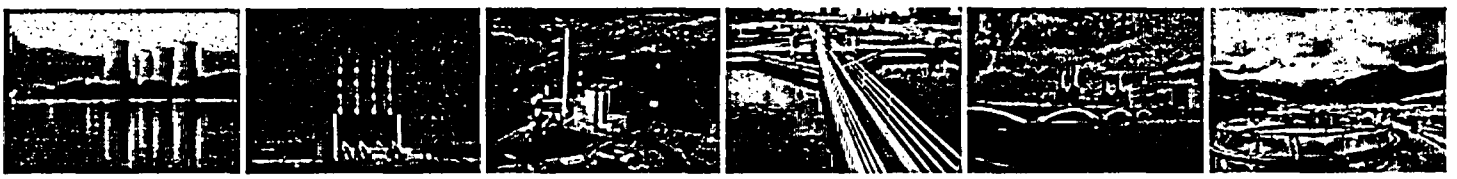

HFC

Leadership • Innovation • Service

HFC-6000 Safety System
Topical Report

www.hfcontrols.com

HF Controls Corporation • 16650 Westgrove Drive • Suite 500 • Addison, TX 75001 • Phone 972.367.4600 • Fax 972.367.4699 • www.hfcontrols.com

November 19, 2004

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

Attention: Document Control Desk

Subject: HF Controls Submittal of Topical Report for Safety Evaluation

Reference: HFC-6000 Safety Control System

Ladies and Gentlemen:

In August of this year HF Controls Corp. alerted the NRC of our intention to submit our topical report for NRC evaluation leading to the issuance of an SER on the HFC-6000 Safety Control System. Enclosed with this letter is that report. You will find attached hereto a hard copy of both the proprietary and non-proprietary versions of our submittal. Our guiding philosophy in the preparation of this document has been to keep the scope and purpose well-defined and presentation very clear to allow a smooth and efficient review.

As indicated in my previous letter, we are looking forward to a productive technical exchange with your staff in the coming months. We re-issue our invitation to your staff to come to our facilities in Addison, TX, in order to evaluate our quality processes, to review any other pertinent supporting technical detail that is deemed necessary, and to meet with our technical team.

At any time during this process if I can provide assistance, answers or any other type of help that will further the process, please do not hesitate to contact me.

Yours truly,

Timothy J. McCreary
President and Chief Executive Officer

Cc: Drew Holland, Bill Macon, NRC
Project Directorate IV-1
Mail Stop 07D1

A. Hsu, J. Stevens, T. Gerardis, HFC

1007

ABSTRACT

This report describes and provides qualification information for the HF Controls Corp. (HFC) HFC-6000 nuclear safety related instrumentation and control platform. The purpose of this report is to seek review and gain approval from the US Nuclear Regulatory Commission for the use of the HFC-6000 in safety related applications in US nuclear power plants.

The HFC-6000 is primarily oriented to meet all safety related I&C requirements in nuclear power plants. Typical applications include:

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

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

The scope of this report addresses both the hardware and software associated with the HFC-6000 platform describing the design, qualification, reliability and the HFC commercial dedication process. The qualification of the HFC-6000 system is in accordance with the guidance presented by EPRI TR-107330. High-level design descriptions, design processes for software and the verification and validation of software quality are discussed. Pre-development software quality was verified and validated through methods outlined in EPRI TR-106439. Hardware was qualified through type testing in accordance with applicable regulatory guidance and the requirements of IEEE Std 603-1991. Defense-in-depth and diversity is discussed in a summary fashion with acknowledgement of the concern and the proposed solution. A detailed defense-in-depth and diversity analysis will be addressed during the plant specific licensing process. The main body of this report describes the HFC-6000 controller, communication devices and input/output modules with detailed discussions of the key issues cited in numerous reports and in the Standard Review Plan (NUREG-0800). An appendix addresses the document control map developed to provide reviewer assistance in locating HFC design documents. A matrix is being developed to show design attributes associated with the EPRI TR-107330 standard. This report also refers to pertinent regulations and other industry standards such those developed by IEEE and other agencies. In addition, a Failure Modes and Effects Analysis (FMEA) report is in review process and very near completion. A summary of the current and projected FMEA findings is provided in Section 8. The report shows that the HFC-6000 system design meets the single failure requirements of IEEE Std 603-1991 and IEEE Std 379-2000.

This report is a summary of detailed design documents, test procedures, and qualification reports.

TABLE OF CONTENTS

INDEX OF FIGURES

INDEX OF TABLES

1 Introduction

1.1 Introduction to HFC

HFC, which is located in Addison, Texas, was established in 1961 as Forney Engineering Company and commissioned by Foster Wheeler to develop fossil plant control systems. HFC currently has the following three product lines: AFS-1000 (Boiler Safety and Nuclear Safety I&C Systems); ECS-1200 (Distributed Control System); and HFC-6000 (Nuclear Safety I&C Systems). In 1979 HFC entered the nuclear plant safety systems industry with contracts for the Duke Cherokee 1&2 and Perkins 1&2 nuclear power plants. These contracts included the safety related control systems. The Duke systems were 90% complete prior to cancellation of plant construction. HFC was contracted by KEPCO in Korea to provide both safety related and non-safety digital control systems for the Yongwang 3 & 4 plants. These control systems were delivered in 1994 and have experienced very reliable operation. Subsequently HFC was contracted by KEPCO to supply the Ulchin 5 & 6 non-safety and safety related control systems. These systems were delivered in 2002 and 2003, and are undergoing various stages of the plant commissioning process. HFC has also been contracted by KEPCO to provide the KEDO plant safety related control systems. In addition HFC has supplied a number of upgrades to operating plants in Korea and over 450 fossil power and industrial plants throughout the world.

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

The HFC control systems provided for the Yongwang 3 & 4 and the Ulchin 5 & 6 nuclear plants in Korea include non-safety and safety controls, I/O and data communications, and control room HMI devices for the NSSS and BOP field components. To date HFC has provided the Korean plants with over 4,000 individual controllers, with between 10,000 and 17,000 I/O per plant in a highly functionally segregated and partitioned design. All systems were delivered on schedule and have operated reliably.

HFC is requesting NRC review of the HFC-6000 product line for suitability in safety related nuclear applications in the USA. The HFC-6000 is a successor of the earlier ECS-1200 and AFS-1000 product lines which have an extensive fossil and nuclear power plant operating base. Both HFC-6000 and ECS-1200 systems use essentially identical software. The changes to develop the HFC-6000 hardware from the ECS-1200 hardware are associated with changes to the ECS-1200 form factor.

It is the HFC intent to employ this report as the vehicle by which HFC will receive the NRC sanction to use the HFC-6000 hardware, basic software operating system, communication software, specified application software, the appropriate software tools and I/O software on

safety system installations throughout the US domestic market. Review and approvals for specific plant applications will be addressed on a plant- specific basis.

2 Documents and Definitions

2.1 *Documents*

Appendix A defines the document structure used in the development and qualification of the HFC-6000 safety system. It lists and describes the documents that were used in the development of this report providing the status and revision number of each document. The documents in this structure include the following categories of interest:

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

This structure constitutes a document mapping system that describes the hierarchy of documents related to this report providing a concise map to guide the reviewer to the detailed design data and qualification material used to generate this report.

2.2 *Definitions*

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

Acceptance Testing. Formal testing conducted to determine if a system satisfies its acceptance criteria and to enable a customer to determine whether or not to accept the system.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Remote. A controller unit and it also act as a node of communication links.

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

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

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

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

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

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

3 Acronyms

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

EPROM	Erasable Programmable Read Only Memory
ESD	Electrostatic Discharge
ESFAS	Engineered Safety Features Actuation System
EWS	Engineering Workstation
F	Fahrenheit
FL	Flags
FMEA	Failure Modes and Effects Analysis
FO	Fiber Optic
FOT	Fiber Optic Transmitter
FPC	Flat Panel Controller
FPCB	Flat Panel Controller Board
FPD	Flat Panel Display
FPDM	FPD Module
GDC	General Design Criteria
H	Hertz
HAS	Historical Archiving System
HFC	HF Controls
HMI	Human Machine Interface
HPAT	HFC Plant Automated Tester
Hz	Hertz
I&C	Instrumentation and Control
ICL	Intercommunication Link
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers
I/O	Input/Output
IOM	Input/Output Module
KEDO	Korean Peninsula Energy Development Organization
KEPCO	Korean Electric Power Company
KHz	Kilo Hertz
LED	Light Emitting Diode
mA	milli Ampere
M/A	Manual/Automatic
MCL	Master Configuration List
MFM	Master for a Moment
MHz	Mega Hertz
μ	Micron
μV	Micro Volt
MMI	Man Machine Interface
MMS	Module Management System
MS	Microsoft
MSS	Maintenance Subsystem
MTBF	Mean Time Between Failures
MUX	Multiplex
NACK	Negative Acknowledge
NIC	Network Interface Chip

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

SRS	System Requirements Specification
SSE	Safe Shutdown Earthquake
SSP	System Safety Plan
Std	Standard
STP	System Test Plan
SVVP	System Verification and Validation Plan
SVVR	System Verification and Validation Report
SY	System
TCB	Task Control Block
TRS	Test Response Spectrum
TSAP	Test System Application Program
TCP/IP	Transmission Control Protocol/Internet Protocol
UCN	Ulchin
UCP	Universal Communication Packet
UDP	Universal Data Packet
UFSAR	Updated Final Safety Analysis Report
UPS	Uninterruptable Power Source
v	Volts
vac	Volts Alternating Current
VAX	Digital Computer
vdc	Volts Direct Current
YGN	Yongwang

4 Overview of HFC-6000 Qualification Project

The HFC-6000 system design requirements were established using the design requirements established for the earlier AFS and ECS product lines. Functional, environmental, module interface and performance requirements were established for the HFC-6000 system to be compatible with the USA nuclear installations and the associated plant digital control systems upgrade requirements. These requirements form the bases for the design of the system and with their specification defines the key areas for design reviews including audits and verification and validation processes. HFC used the guidance provided by EPRI TR-107330 and TR-106439 to qualify the HFC-6000 system.

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

A. An architecture overview of the HFC-6000 system and its suitability for the intended application was performed. Input/Output modules, communication, and controller modules were defined so as to encompass the broad range of nuclear applications. This review also included the performance of a single failure analysis considering redundancy incorporated by the plant design. Using the architecture, a Failure Modes and Effects Analysis (FMEA) for the HFC-6000 system was performed. This is to be used in the future as an input to the more detailed plant specific application. This overview includes an analysis of the deterministic features of the system.

B. Evaluate the HFC-6000 system's hardware and software QA programs that are applied to determine if they are adequate to support nuclear safety-related applications with a reasonable set of supplementary activities. The evaluation includes factors relating both to generic qualification and future applications of the qualified products.

C. Select a set of modules, supporting devices and software from the HFC-6000 system to be used as the qualification test specimen.

D. Define and produce a Test System Application Program (TSAP). The TSAP serves as a synthetic application that is designed to aid in the qualification tests and demonstrate the acceptability of the system being qualified.

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

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

G. Perform the hardware qualification tests, perform the data analyses, and document the results. Results documentation includes definition of the qualification envelope, identification of the specific products that were qualified, and guidance for using the qualified control system in a specific application.

H. Perform a suitability analysis for HFC-6000 requirements including such features as accuracy, response times and physical characteristics. Identify all I/O points, scan rates and software features.

I. Demonstrate that the operating software of HFC-6000 is adequate for use in Nuclear Power Plant Safety Systems. This proof of adequacy follows the guidance presented in EPRI TR-106439. This TR calls for a blend of original design documentation, additional proof processes by HFC and a review of operating history to determine past quality. Testing is only one aspect of the HFC acceptance process. HFC has considered the allocation of HFC-6000 system requirements to the main controller and other supporting modules, established a software test program which included both the hardware and software, established a mature and stable software development process, and has collectively reviewed operating history data for the applicable Pre-Developed Software.

J. Develop the test application software using the HFC quality standards. The HFC development process is mature and stable and provides safety related application software that meets all appropriate guidelines and regulations.

K. Ensure that the configuration identification and management program for the HFC-6000 hardware and software is maintained using the guidelines contained in the applicable standards and regulations.

L. Ensure that all specifications of the HFC-6000 system are consistent with the requirements of 10 CFR 50 Appendix B, IEEE Std 603-1991 and the applicable GDCs. Ensure that all applicable RGs and industry standards have been followed to the external practical.

The controller software, I/O software, communication software, development and maintenance tool software and test and diagnostic software are primarily Pre-Developed Software (PDS) and, as a result, the guidance provided in EPRI TR-106439 was used as the basis for its qualification. The software qualification follows the guidance presented in EPRI TR-106439. HFC credits supplemental testing, operating history, design and documentation and life-cycle processes to prove that the HFC-6000 software is qualified for safety related applications. The plant specific application software will be developed in accordance with the provisions of BTP HICB-14 to qualify this software on plant specific basis.

The following sections of this report will provide both design and qualification details that will demonstrate compliance with all applicable regulations for a programmable safety related instrumentation and control system.

5 HFC-6000 System Overview

HF Controls provides integrated digital systems to support nuclear power plant safety, control, and information functions. The HFC-6000 digital safety systems meet regulatory requirements for safety system quality, qualification, redundancy, fault tolerance, deterministic performance, isolation and independence. The overall architecture of HF Controls distributed safety, control, and information systems form the bases to meet the requirements for nuclear power plant applications.

The HFC-6000 safety system is designed to operate with either single or multiple control remote units in each channel. The primary CPU Module (CPUM) in a remote unit is the system controller (HFC-SBC06), which supports the execution of control logic programs, I/Os scan, and C-Link communication. [

] The Communication Module (COMM) consists of HFC-PCC06 peripheral interface board in the same rack. [

]

The Figure 5-1 illustrates a typical system arrangement and modules of HFC-6000 system. The Input/Output Module (IOM) provide the hardware interface to controlled field devices and are implemented by different types of I/O printed circuit boards. [

]

The dedicated Flat Panel Display Module (FPDM) can be used as an HMI interface composed of a qualified HFC-FPD06 flat panel display and an HFC-FPC06 FPD controller. [

]

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

Figure 5-1 - HFC-6000 System Arrangement Diagram

6 HFC Safety I&C Platform Hardware Description

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

6.1 System Controller Module

The HFC-6000 safety system provides plant monitoring and control functions, with monitoring and control capabilities from one to multiple remote control units. The HFC-SBC06 System Controller is the primary module used for implementing plant safety functions. [

]

Figure 6-1 - HFC-SBC06 application in quadruple channels configuration

Descriptions of the functional requirements of the HFC-SBC06 System Controller module and HFC-DPM06 Dual Ported Memory module, from an external perspective, are provided in the HFC-6000 Product Line Requirements Specification, RS901-000-01. Detail level descriptions of the HFC-SBC06 and HFC-DPM06 are contained in the HFC-SBC06-DPM06 System Controller Module Detailed Design Specification, DS901-000-01.

The principal functions supervised by the HFC-SBC06 System Controller are:[

•

]

The HFC-SBC06 System Controller module is designed to operate in a redundant controller configuration consisting of two HFC-SBC06 modules and one HFC-DPM06 module. The primary HFC-SBC06 performs the main functions of the system controller while the secondary HFC-SBC06 operates as a "hot spare" for the primary HFC-SBC06. [

.]

The Maintenance Failover function permits manual verification of the working status of both the primary and the Secondary controller to make sure it will be able to take over control in the event that the Primary controller fails.

The HFC-6000 safety system provides three communication interfaces to support transfer of data and status between system components. [

]

The HFC-SBC06 module contains three separate microprocessor sections: the SYS microprocessor section, the ICL microprocessor section, and the C-Link microprocessor section. Each microprocessor section is dedicated to a specific set of functional responsibilities, with the SYS processor being the main processor for the whole controller and the other two acting as subordinate processors. [

]

[

]

In addition to common access to Public Memory, each microprocessor is configured with a Private Memory composed of separate PROM, Flash, and RAM sections. A set of system firmware is installed in the PROM or flash memory. Private Memory is accessible only to the microprocessor in that circuit section.

There is an onboard Sanity circuit for detection of controller failure. The SANE status and PRI (Primary) status signals from the Sanity circuit are routed to the Failover circuit on the HFC-DPM06 module. The Failover circuit supports controller switchover on failure of the primary controller as well as maintenance failover.

[

]

6.2 Input /Output Modules

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

- Measuring input signals or setting output signals

- Communication with HFC-SBC06 system controller through the ICL
- Self-diagnostic functions

An I/O module having output channels receives digital images for its output channels from an HFC-SBC06 system controller at regular intervals and uses this data to control each output point. An I/O module with input channels converts the input signal for each channel into a digital image, and sends these images to the HFC-SBC06 system controller at regular intervals.

[

•

]

Each HFC-6000 I/O module supports communication with the HFC-SBC06 controller via the ICL as shown in Figure 6-3. Each I/O module has two transceivers that are connected to the redundant ICL channels. [

] Throughout normal operation of the HFC-6000 control system, one HFC-SBC06 controller functions as primary and polls the I/O modules. The messages carried over the ICL network are either normal data update or diagnostics messages.

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

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

Name	I/O Channels
DO8J	8 channel digital relay output
DI16I	16 channel digital input

DC33	2 channel 120-vac digital output and 12 digital input
DC34	2 channel 125-vdc digital output and 12 digital input
AI16F	16 channel analog input
AO8F	8 channel analog output
AI8M	8 channel 100Ω RTD input
AI4K	4 channel pulse input

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

6.2.1 Relay Output Module

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

]

6.2.2 Digital Input Module

The HFC-DI16I assembly is a 16-channel digital input module. The assembly operates as a standard DI module in a HFC-6000 control system. [

]

6.2.3 Digital Controller Module

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

[

]

6.2.4 Digital Control of Breakers Module

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

Typical applications include monitoring Electrically Operated Breakers (EOB) for overloads. This module is designed to provide the specific combination of digital I/O channels needed to control motor starters or switchgear field equipment.

[

]

6.2.5 Analog Input Module

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

] It samples the AI readings, performs analog to digital conversion for each channel at regular intervals, and stores the resulting digital images in onboard RAM prior to data transfers to the controller.

6.2.6 Analog Output Module

The HFC-AO8F module operates as the standard AO module in a HFC-6000 control system. It receives digital images from the system controller and performs digital to analog conversion for each channel at regular intervals. [

]

6.2.7 RTD Input Module

The HFC-AI8M Resistance Temperature Detector (RTD) printed circuit module (PCB) is an input-conditioning device for a HFC-6000 control system. This module receives the voltage images of its isolated analog inputs from an external RTD and presents it for conversion into a digital count value image for each channel at regular time intervals.

6.2.8 Pulse Input Module

The HFC-AI4K module provides four input channels for processing pulse signals from field equipment. The four channels are organized as two pairs, and configuration parameters for each pair can be entered by switches that are accessible at the front bezel. These configuration parameters permit selection of rate or accumulate mode. When the rate mode is selected for a particular pair of channels, hardware counters produce a count value that represents the frequency of the input signal. When the accumulate mode is selected, the counter increments with each input pulse, and the microprocessor scales the input based on the pre-scaled value.[

]

6.3 Communication Modules

In an HFC-6000 System, there are (1) C-Link Communication Link, (2) ICL communication, and (3) four safety channel communication networks. Communication support is integrated in the system controller modules and I/O modules. [

]

6.3.1 Communication Link (C-Link)

The C-Link Processor and ECS-B232 Fiber-Optic Transmitter (FOT repeater) module serves as the interface between the HFC-SBC06 system controller module and the redundant C-Link. Each node of this safety train C-Link has the following features:

[

•

]

6.3.2 Inter-Communication Link (ICL)

The ICL links handle communication between HFC-SBC06 system controller module and its local and remote I/O modules, HFC FPC-06 Flat Panel Device controller module and HFC-PCC06 Peripheral Communication Controller module.

6.3.2.1 I/O Communication

The HFC-SBC06 system controller module accesses local I/O module through RS-485 serial communication links. [

]

6.3.2.2 HFC-PCC06 Module & RS-485 Serial Links

The HFC-PCC06 module provides communication interface between the system controller and human interface control modules, such as CSM and M/A stations. The PCC06 module is installed in an HC-6000 I/O chassis. [

]

6.3.2.3 HFC-FPC06 Module & 4 Safety Channels Communication Links

The HFC-FPC06 Flat Panel Controller assembly provides the electrical interface with the HFC-FPD06 Flat Panel Display and one or more user interfaces such as keyboard, mouse or trackball and touch screen. [

]

6.4 Human Machine Interface (HMI)

The HFC-6000 product line provides two types of HMIs: 1) FPD operator interfaces and 2) control module interface.

6.4.1 FPD Operator Interfaces

FPD operator interfaces provide the human-machine interface to the HFC-6000 safety system. The FPD operator interface is an HFC-FPD06 flat panel display that has been packaged to withstand class 1E seismic stress testing. The operator interface can also include display navigation device such as a mouse, touch screen or a trackball and a keyboard. FPD operator interfaces can also be configured with a second display for enhanced display capability or without a keyboard for situations where operator data entry is not required. The FPD operator interface has the capability for process diagram displays, trends, alarms and text displays.

6.4.2 Control Switch Modules and M/A Stations

The control modules provide optional interface hardware. They are control switch modules for ON/OFF status and M/A stations for analog control. Control switch modules include from one to four pushbutton switches with integral switch lamps to indicate switch status. M/A stations include manual/auto stations and manual only stations. Each M/A station provides up to three bar graphs and a digital readout to display analog values associated with its control loop.

6.5 Power Supplies and Chassis

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

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

There are three types of backplanes in the HFC-6000 product line: the HFC-BPC01-19, the HFC-BPE01-19, and the HFC-BPC01-08.

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

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

The HFC-BPC01-08 is a SLC backplane which serves as a controller chassis backplane for an 8-inch card rack assembly. It provides two slots for HFC-SBC06 controllers, one slot for an HFC-DPM06, and the remaining slots for I/O modules. The backplane can receive operating power from redundant power cables that attach to a connector at the rear of the chassis. The loop controller(s) plugged into this backplane communicates with I/O cards via redundant serial Intercommunication Link (ICL) traces on the backplane. Redundant ICL connectors at the rear of the backplane card enable connection of the ICL with an expansion card chassis.

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

7 HFC Safety Platform Software Description

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

- Platform Software
- Application Software (Plant Specific)
- Engineering Workstation Software (Non-Safety)

Platform software consists of firmware programs that provide the generic capability of the HFC-6000 product line. This generic firmware is written in Assembly language stored in non-volatile memory and is not alterable by the user. The platform software for the HFC-6000 is discussed in detail below.

Applications software consists of plant specific programs that provide the unique functionality required for a safety related application. Applications software is stored in non-volatile memory and cannot be altered while the controller is operating in the on-line mode.

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

This section consists of the following platform software topics:

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

7.1 Controller Software

7.1.1 HFC-SBC06 Controller

[

] The major functions of the three processors are as follows:

- The Pentium system processor monitors overall system status, coordinates overall operation of the controller, and runs the equation interpreter (application program) task.

- The Inter-Communication Link (ICL) processor controls the ICL interface and runs the ICL scan cycles. [

]

- The C-Link processor controls the redundant C-Link interface for the controller. [

]

The application program for the HFC-SBC06 controller consists of an equations file, an I/O configuration list, a Block Request (BLRQ) table, a blocks list and a block data file. These program components consist of the following:

[

•

]

The four structures associated with the application program are generated using utilities installed on an offline PC engineering workstation. After the files have been created, they are compiled into a binary format file. The successful compiled object file can be burned into a PROM or downloaded into Flash memory of the HFC-SBC06 system controller module during offline mode operation.

7.1.1.1 The System (SYS) Processor

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

from the application program to generate digital and analog output values using input values currently in memory.

[

]

Each subordinate processor has a "Mailbox" in the Public Memory. During normal operation, the subordinate processor periodically updates its mailbox by loading a preset value. The SYS processor monitors subordinate processors running status by decrementing the value in the mailbox at preprogrammed intervals. The setting of mailbox preset value and mailbox decrementing amount and intervals determine how soon a failure of the subordinate processor can be detected.

[

]

7.1.1.2 SYS Processor Software Architecture

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

The tasks running on the SYS processor are:

[

•

]

During initialization, the SYS processor configures several Mailbox utility functions for the OS Utility Task. These mailbox functions are essential to determine the System Controller's Sanity (operating status of processor). During every OS task scan cycle, these functions will be executed by the Utility Task based on the primary or secondary status of the controller.

[

]

The following figure illustrates the tasks execution sequence:

7.2 Communication Software

Figure 7-2 gives an overview of the HFC-6000 control system communication paths. The C-Link processor enables the HFC-SBC06 to broadcast data and exchange information among safety I &C systems within the same channel/train. Through isolation hardware, the non-safety equipment can receive the broadcast dynamic data and display at the same time. Internally, the HFC-SBC06 system controller uses the ICL to access I/O, panel mounted devices and controllers of other safety channels.

7.2.1 Communication Link (C-Link) Software

The C-Link consists of IEEE Std 802.3 hardware with the redundant 10BaseT cables that connect to a FOT assembly. The fiber optic connection provides both physical and electrical isolation for C-link communication. A node on the C-link is called a "remote".

[

]

7.2.1.1 Token Passing Scheme

[

]

7.2.1.2 Synchronization on Dual-Channels

[

]

7.2.1.3 Message Types

[

]

7.2.1.4 C-Link Processor Software Architecture

The C-Link Processor software is also software designed based on the operating system component common to all processors on the HFC-SBC06 module and a set of configurable tasks that will be run by the operating system.

7.2.2 Inter-Communication Link (ICL) Software

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

7.2.2.1 I/O module communication

[

]

7.2.2.2 Redundant Serial Link

Each HFC-6000 controller includes a hardware interface for one or more ICL channels to provide the hardware link with configured I/O modules. [

]

7.2.2.3 Polling

The ICL employs a poll-response communication protocol to control message exchanges between the controller and its configured I/O modules. The controller initiates scan cycles at regular intervals throughout normal operation. [

]

7.2.2.4 Secondary Loopback Test

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

]

7.2.2.5 Secondary Polling Function

[

]

7.2.2.6 ICL Software Architecture

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

The tasks running on the ICL Processor are:[

]

The descriptions of Initialization Process are provided in the DS901-000-001, HFC-SBC06 Module Detailed Design Specification.

7.2.3 Input/Output Module Software

[

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

[

]

All I/O modules are configured as slave stations on the ICL. After ICL initialization is complete, the ICL communication routine remains inactive until the first byte of a new message has been received from the controller. [

]

When a receive interrupt occurs, indicating that a message is received from the ICL, the Receive Interrupt Service Routine will validate the message and call a Process Command Routine to process the message and to store any output images contained in the message in the I/O image buffer in RAM. [

]

7.2.4 HFC-PCC06 Peripheral Communication Software

The HFC-PCC06 is designed to be installed in a HFC-6000 I/O rack. This peripheral Communication Controller (PCC) allows the HFC-SBC06 controller to communicate with Control Switch Modules (CSMs) and/or Manual/Automatic (M/A) stations. [

]

7.2.4.1 Communication with the HFC-SBC06

Each HFC-PCC06 module supports communication with the HFC-SBC06 controller via the ICL. The mechanism for transferring data between the HFC-SBC06 and the HFC-PCC06 is identical to that for any other station on the ICL. The structure of the data of received from the HFC-

SBC06 or transferred to the HFC-SBC06 is determined by the specific combination of input modules configured for the system.

7.2.4.2 Communication with the CSMs or M/A stations

[

] The CSMs are used as an operator interface device for ON/OFF control. Each CSM includes from one to four pushbutton switches with integral switch lamps to indicate switch status. M/A stations are used as the operator interface device for analog control. It includes a combination of pushbutton switches, alphanumeric display, LEDs and bar graph displays to enable analog control and to indicate analog status.

At regular intervals the HFC-PCC06 scans each configured CSM or M/A station in sequence.

]The CSMs and M/A stations are Class1E devices and, as a result, isolation is not required for the communication interfaces.

7.2.5 HFC-FPC06 FPD Controller Software

The HFC-FPC06 consists of a Single Board Computer (SBC) and a separate FPD controller module, which have separate and independent programs. Nonvolatile memory on the SBC assembly contains the real time OS for the controller. The OS runs hardware diagnostics and initialization functions following power-up or reset. During subsequent operation, the OS functions as a task scheduler for the entire assembly. The FPD controller portion of the assembly provides the software for the ICL interface, graphics driver, and safety channels interface utilities. These programs and utilities are installed during fabrication of the hardware assembly and are not accessible to the user.

[

] Static data consists of text and graphic representations of control system equipment. Dynamic data consist of digital status and analog values obtained from the dynamic database of the HFC-6000 controller(s). The dynamic data may simply be displayed on a pre-fabricated graphic page, or they may be used to control the appearance of selected graphic features in a dynamic display page. [

]

[

]

7.3 *HMI Software*

The HFC-6000 safety platform can use a local FPD HFC-FPD06 and its controller HFC-FPC06 as the human machine interface (HMI) device. [

]
In addition, the HMI Software includes graphic and hardware drivers for the display and for the interface hardware. The range of functional operations available with the flat panel display and its user interfaces includes the following:

- Display current alarm status.
- Acknowledge alarms.
- Select a graphics display page from a menu.
- Enter a command for a selected discrete control function.
- Control manual/auto mode selection for an analog control function.
- Increase/decrease control inputs for analog control functions.
- Display video trends for selected variables of the application.
- Direct process control with interactive graphic displays.

7.4 *The Development and Maintenance Tools*

The firmware for the controllers and I/Os of HFC-6000 safety platform software were written in Intel Assembly language. They were developed under Intel x86 Cross Assembler, Linker and Locater on Digital VAX computer. HFC uses either the VAX monitor or PC workstation as terminals.

The configuration management of source codes and configuration files are under the VAX Code Management System (CMS) and Module Management System (MMS) control. [

]

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

]

8 Safety System Design Topics

8.1 Deterministic and Time Response

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

This description will define all aspects of deterministic performance including:[

-]

8.1.1 System Controller

An HFC safety system can be configured with either single or redundant System Controllers. With a redundant System Controller configuration, a second System Controller and a Dual Ported Memory Board are added to the configuration. In a redundant configuration, one controller is in secondary mode, monitoring the primary System Controller and updating its database through the DPM. If the primary controller fails, the secondary controller takes over the operation. This section describes both configuration options.

[

-]

8.1.2 SYS Processor Characteristics

[

]

8.1.2.1 Applications Tasks

[

]

8.1.2.2 Supervisory Tasks

[

]

8.1.3 ICL Processor Characteristics

The ICL processor operation differs depending on whether it is configured with a single SC controller or with a redundant SC controller.

8.1.3.1 Operation in a Non-Redundant Configuration

[

]

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

8.1.3.2 Operation in a Redundant Configuration

[

]

8.1.4 C-Link Processor Characteristics

The C-Link processor controls redundant IEEE Std 802.3 -compliant 10BaseT Ethernet links.
[

]

8.1.5 I/O Module Characteristics

An I/O module is an independent card in the chassis. Each I/O module has a microprocessor. All I/O cards utilize a common series of operations for communication with the ICL processor in the SC.

The I/O station begins initialization on power up or after the local reset switch is depressed. [

]

8.1.6 Flat Panel Display HMI Operation

The HFC Flat Panel Display Controller (FPC) is a module in the chassis that contains a single board computer for communication with the HFC-SBC06 System Controllers. [

]

The FPC initializes on power-up and performs diagnostics that validate the FPC hardware and the code stored in non-volatile memory. [

]

8.1.7 Deterministic Performance Conclusion

The HFC system is designed to have deterministic performance with a predetermined maximum response time to changing input signals and messages communicated locally and over the C-Link.

8.2 Failure Mode Effects Analysis (FMEA)

The HFC-6000 FMEA covers the existing system design for the HFC-6000 product line. The FMEA presented in Tables A-1 through A-17 of the preliminary FMEA report was performed in accordance with EPRI TR-107330, Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants, Section 6.4.1, and qualitative guidance in IEEE Std 352-1987, IEEE Guidance for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems. The analysis covers a total of 232 postulated failure modes for the generic system architecture that are incorporated into the HFC-6000 control system product line. A summary of the impact on system performance is presented in Section 4.2 of the preliminary FMEA report. The existing system design provides confidence that a detectable failure condition can be detected and alarmed; at the mean time the redundant components permit continued operation of critical system functions in the presence of a single failure condition.

The evaluation of postulated system failures provides assurance that no latent design errors are present in the legacy components derived from previous HFC control system designs. Any detectable HFC-6000 hardware failure after the initialization will be resolved by scheduled on-line diagnostic software and the operator surveillance of system performance. All detected failures will be reported as alarms. Operator surveillance of system status and alarms with the availability of redundancy provides confidence in overall system integrity. Consequently, the overall preliminary assessment of the system failure modes and their effects are as follows:

- The probability that a single common mode failure or an undetected failure mode condition exists in the HFC-6000 system is negligible.
- The redundant architecture of the controllers and communication links provide adequate assurance that any single failure in the controller section does not disrupt the capability to maintain control of the application process. In addition, the redundant architecture provides a mechanism for generating an alarm to notify the user that a failure exists.
- The architecture of the HFC-6000 control system includes redundant I/O channels as an option. Any single failure of the non redundant elements is detected by the controller

generating an alarm to notify the user that a failure exists. Redundant I/O modules for particular systems may be included as part of the design for a specific plant application but are not necessary for reliable system operation.

These features provide confidence that the HFC-6000 control system architecture will satisfy the single failure requirements of IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and IEEE Std 379-2000, "IEEE Standard Application of the Single-Failure Criteria to Nuclear Power Generating Station Safety Systems."

These conclusions are based upon the preliminary FMEA. As the FMEA is finalized, if any change or new conclusions are developed, they will be reported in the FMEA report.

8.3 Reliability and Availability

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

]

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

Some modules of the HFC-6000 safety system have a redundant configuration, which means that one module can be lost without degrading functional operation of the HFC-6000 as a whole. The calculation of availability of redundant modules was based on the guidelines described in IEEE Std 352-1975.

For this analysis, the duty cycle was assumed to be 100 percent. The temperature profile is set at 26.40 degree C. It is assumed that the plant control system is in daily use, and failures will be detected within one day of occurrence. It is also assumed that spare parts are on hand to affect timely repair.

Mean Time to Repair has a strong influence on the availability that the equipment can achieve, but it is only partially under the control of the manufacturer. The best the manufacturer can do is

to make the equipment easy to diagnose and repair. The owner has the responsibility to aggressively monitor the equipment for failure and expeditiously replace any part that fails. The owner also has the responsibility to maintain the system according to HFC's maintenance manual and replace modules according to the recommended replacement schedule.

Each system can have a different configuration and architecture. The reliability of the overall system is highly influenced by the choice of configuration and architecture design. From the system design side, there are two ways to improve availability of overall system: one is to select high reliability parts and products for the product line design, and the other is to utilize redundancy in system design and configuration. Availability is improved significantly when redundancy is applied. HFC-6000 products provide redundancy support at different levels of the system. They can be used to build safety related control system with different configurations. The owner's decision on selecting the system configuration will decide the final availability of the overall system.

8.4 Quality Assurance Programs

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

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

Software quality was verified per the guidance of ANS/IEEE Std 7-4.3.2-1993, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations which incorporates guidance from ASME NQA-2a-1990 Part 2.7.

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

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

Pre-developed software quality was verified using the guidance of ANS/IEEE Std 7-4.3.2 and EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Equipment for Nuclear Safety Applications" and TR-107330, "Generic Requirements Specification for

Qualifying a Commercially Available PLC for Safety Related Applications in Nuclear Power Plants."

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

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

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

The HFC QA Program covers the design, implementation and commissioning of the HFC-6000 system. Requirements of this program apply to all activities (systematic and planned actions) affecting the quality of products and services provided and performed by HFC. [

-]

The QA Program includes procedures for managing the multidisciplinary interfaces within the HFC design effort and clearly delineates the responsibilities for quality functions in the respective organizations. To assure that the documentation reflects current design, the QA Program, includes procedures and methods that ensured the correctness and completeness of the documentation at the end of each phase of the HFC-6000 design project. The ultimate objective was to eliminate all design errors as early as possible and ensure that the design basis, safety, operational and maintenance requirements were properly considered. This ensured that the resulting HFC-6000 product met the highest standards of technical quality while eliminating the time-consuming "redo's" that might otherwise plague the design effort.

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

The HFC Quality Assurance Manager has the responsibility for establishing the Quality Assurance Program and verifying that activities affecting the quality of deliverables are

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

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

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

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

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

]

Design verification includes design reviews, alternate calculations, qualification tests or a combination of methods executed in accordance with approved procedures. Design verifications

are performed in accordance with approved procedures, performed prior to release for procurement, manufacturing, or to another organization for use to ensure that the design output meets the design input requirements. Independent design validations ensure that developed products conform to the specified requirements.

Design Analyses are performed in a planned, controlled and documented manner. They are sufficiently detailed as to purpose, method, assumptions, design input, references and units. Methods such as computer programs and calculations are described and controlled. Qualification testing demonstrates adequacy of performance under conditions that simulate the most adverse design conditions.

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

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

8.5.1 General

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

8.5.2 Compliance with Nuclear Regulatory Commission (NRC) Documents

RG 1.22 "Periodic Testing System Actuation Functions"

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

RG 1.29 "Seismic Design Classification"

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

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

The HFC-6000 provides outputs to indicate the bypassing of the channel where the channel performs a function associated with the maintenance of safety. Plant specific designs will have the capability to follow this RG's guidelines when using the HFC-6000.

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

Single failures of the HFC-6000 system have been evaluated in the earlier discussed FMEA. That assessment led to the conclusion that the system meets the single failure criterion of IEEE-603. There were no undectable failures within the HFC-6000 platform. All failures are immediately known and are found during testing functions performed at the required intervals. Due to system redundancies, all credible single failures within the HFC-6000 system will not interrupt the operation of the plant system.

RG 1.62 "Manual Initiation of Protective Actions"

All HFC-6000 actuation functions can be initiated manually. Provisions for this are maintained at the system level. However, provision for component level manual actuations will also be retained through past control system designs. The amount of equipment common to both manual and automatic, isolation is kept to a minimum. The manual initiation path remains a relatively simple design. Plant-specific designs will not allow a credible single failure to prevent system level manual actuation.

RG 1.75 "Physical Independence of Electrical Systems"

The design of the HFC-6000 system conforms to this RG. The field-implementation of the HFC-6000 (e.g., the connecting wires, cables, switches and relays) will also conform to the physical, mechanical and electrical separation standards provided by the guide. The primary means of separation between channels and safety classes is through the use of fiber optics. Additional barriers and conduits will also be used as required.

RG 1.89 "Qualification for Class 1E Equipment for Nuclear Power Plants"

The HFC-6000 system has been tested to verify its conformance with this RG and IEEE Std 323. The environmental qualification tests employed both type-testing and analysis which were followed per the provisions of EPRI TR-102323. This is described in more detail later in this report (Section 9).

RG 1.97 "Instrumentation for Light-Water Cooled Nuclear Power Plants to Assess Plant an Environs Conditions During and Following Accident"

The HFC-6000, when installed in any post-accident monitoring system will conform to all provisions of this RG.

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

The HFC-6000 platform conforms to this RG, IEEE Std 338 and HICB-17 as discussed in RG 1.22.

RG 1.152 "Criteria for Programmable Digital Computer System Software in Safety-Related Systems of Nuclear Power Plants"

The HFC-6000 system design follows the guidance of this RG by meeting the applicable provisions of IEEE-ANS-Std 7-4.3.2. The software for the HFC-6000 is segregated into both pre-developed and new software. For the new safety related software, HFC has described acceptable methods employed for designing, verifying, validating and implementing software to be used in safety related systems. The HFC software quality plan is consistent with ASME NQA-2a; this plan addresses all of the runtime resident computer software. The verification and validation processes are in accordance with all applicable guidance. Those processes provide adequate confidence that the safety requirements and the requirements defined at each phase of the development process are implemented. The pre-developed software is qualified based on the provisions of Section 5.3.2 and Appendix D of the IEEE Std standard. Where the legacy qualification process did not compare favorably with this standard, compensating factors were used. These compensating factors were developed per the guidance of EPRI's TR-106439 and TR-107330.

RG 1.153 "Criteria for Safety Systems"

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

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

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

All of the verification and validation activities associated with this effort were carried out in conjunction with a structured software development process. In addition, overall V&V plans were developed while considering the planned implementation for system applications. Verification was performed throughout the Software Life Cycle. This provided a check of the

translation of information between phases of the Life Cycle as discussed in HICB BTP-14. The resulting information provided for each phase was determined to be both unambiguous and complete. The testing requirements for the verification activity were all attainable and documented. HFC ensured that the V&V program addressed the integration of the hardware with the software for the HFC-6000 platform. The HFC V&V plan was structured to confirm the completeness and correctness of system design. All necessary activities and tests were witnessed, performed and reviewed by competent individuals and using independent review processes.

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

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

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

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

The HFC-6000 test plan includes the following items:

- the items to be tested,
- the features of the system under test,
- the overall test approach,
- the test environment,
- the test group and staffing,
- test sequencing,
- test equipment,
- the acceptance criteria.

The final area addressed by the documentation is the subject of test reporting. For the HFC-6000 platform the report includes:

- a description of the test hardware configuration,
- input listing,
- output listing,
- data regarding timing and sequencing,
- conformance with acceptance criteria,
- an error log with corrective actions noted.

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

Employing HFC's software test methods and procedures, tests were performed. The results met all test objectives within pre-established criteria. The software performed as specified by the design document, all of the interfaces executed as anticipated.

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

The SRS has been written to follow both the guidance contained in this RG and in the endorsed IEEE Std 830. HFC has ensured that the characteristics discussed in Section 2 of this RG are addressed. HFC has developed its SRS to address the criteria and guidance of Section 2 of the RG. Particular emphasis was given to ensure that the SRS are traceable, accurate, complete, consistent, ranked for importance or stability, verifiable, and modifiable. Equal emphasis was given to the interfaces between control systems and the Human-Machine-Interface (HMI). The SRS contains a complete specification for all system functions including their data structures and all relationships between those structures. No requirements within the SRS were found to contradict or conflict with each other. All of the SRS are verifiable. An independent verification process was used to show that each SRS implementation fulfills the software requirement. An SRS change control program has been implemented by HFC as part of the overall HFC-6000 configuration management program.

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

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

The RG and the IEEE Std 1074 provide a structured approach for the development of a software life cycle program consistent with regulatory guidance. HFC recognizes that, for development and maintenance of high functional reliability and high quality safety software, there has to be an orderly structure to the entire software design and implementation process. HFC's Software Life Cycle addresses the issues and concerns of the standard although its organization differs. The Software Life Cycle process that HFC used successfully provided the necessary framework for the HFC-6000 software project so that activities could be mapped. With this mapping, a

concurrent execution of related activities can occur and staged checkpoints are available at which characteristics of certain activities can be verified. .

HFC's life cycle plan insures that all necessary development and V&V activities are performed and that the required inputs, outputs, activities, pre-conditions and post-conditions are described or has been accounted for in the HFC-6000 platform life cycle model. While the RG and Std do not specify the completion of specific documents, SRP BTP-14 places a great degree of emphasis on the output documents as a manner to judge successful completion of a life cycle process. The activities for the HFC-6000 software life cycle model were deemed successfully completed when sufficient input information has been processed and sufficient output information has been generated.

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

The HFC-6000 platform has been qualified to EMI/RFI guidance in accordance with this RG and the EPRI TR. Details regarding this qualification are discussed in Section 9 of this report.

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

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

NUREG-0737 "Requirements for Emergency Response Capability"

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

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

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

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

All isolation devices used in the HFC-6000 are qualified in accordance with this BTP. The design of isolation devices conform to the requirements of RG 1.75 and 1.153. The basis for the qualification of these devices is consistent with accepted industry standards. The testing has demonstrated that the devices meet the acceptance criteria of IEEE Std 603-1991.

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

The HFC software development life cycle shares certain characteristics with this BTP model. The HFC new safety related software was developed using acceptable software development plans. The results produced acceptable design outputs. Management, implementation and resource planning procedures were established for new software. The functional characteristics and software development characteristics noted in the BTP were established and met by the HFC process.

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

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

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

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

NUREG-0800 BTP HICB-21 "Guidance on Digital Computer Real-Time Performance"

HFC-6000 system timing requirements are such that their allocation to events within a plant's safety analyses should support the timing requirements for each event. This is evident with the use of either small scale or large scale digital system modifications using the HFC-6000. A time analysis for each event will be part of the plant specific implementation process. The software design does not contain any non-deterministic time delays.

8.5.3 Institute of Electrical and Electronic Engineers (IEEE) Standards

IEEE Std 7-4.3.2-1993 "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations"

See RG 1.152 above.

IEEE Std 323-1974/83 "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations

The HFC-6000 was environmentally qualified using the guidance contained in EPRI TR-102323. This qualification effort is discussed in more detail within Section 8 of this report.

IEEE Std 344-1975 "IEEE Standard for Seismic Qualification of Class I Electric Equipment for Nuclear Power Generating Stations"

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

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

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

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

The HFC-6000 system meets the functional requirements of IEEE Std 603 in addition to the guidance contained in this IEEE. Considering the single failure criterion in association with all potential HFC-6000 applications, all requisite safety functions can be maintained without impeding the execution of other safety functions. This is valid for all functions where redundancy is maintained. Interconnections between redundant channels were reviewed and determined not to cause a cascade of the failure such that the safety function is lost.

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

The HFC-6000 system conforms to this IEEE Std as endorsed by RG 1.75 and discussed in HICB BTP-11. This conformance is discussed to response to RG 1.75 and BTP-11.

IEEE. 472-1974 "Guide for Surge Withstand Capability Tests"

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

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

See the response to IEEE Std 352-1987

IEEE Std 603-1991/1998 "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"

See RG 1.153 above.

IEEE Std 730-1989 "Software Quality Assurance Plans"

The HFC-6000 system quality assurance plans conform to the guidance of this Std. A discussion of the QA process is presented in Section 8 of this report. Supporting information is provided in HFC Quality Process Procedures.

HFC's HFC-6000 software quality assurance plan is compliant with this standard.

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

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

IEEE Std 829-1983 "IEEE Standard for Software Test Documentation"

See RG 1.170 discussion above.

IEEE Std 830-1984 "IEEE Standard Guide for Software Requirements Specification"

See RG 1.172 discussion above.

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

See RG 1.171 discussion above.

IEEE Std 1012-1986 "IEEE Standard for Software Verification and Validation Plans"

The HFC-6000 system verification and validation plans conform to this standard as described in the HFC software design descriptions and noted in the RG 1.168 discussion above.

IEEE Std 1016-1987 "Recommended Practice for Software Design Description"

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

IEEE Std 1028-1988 "Standard for Software Reviews and Audits"

HFC complies with this Std. The HFC-6000 Quality Assurance Program assures that the requisite software reviews and audits are performed. See RG 1.168 discussion above.

IEEE Std 1042 "IEEE Guide to Software Configuration Management"

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

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

A life cycle was established for the design of the software for the HFC-6000 system. See RG 1.173 discussion above.

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

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

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

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

8.5.4 Other Documents

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

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

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

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

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

The HFC-6000 system was tested for EMI/RFI in accordance with EPRI-TR102323-R1. This testing and the test results demonstrated that per this standard, the HFC-6000 is qualified for safety related applications. Testing details are provided in Section 9 of this report.

MIL-STD-462D "Measurement of Electromagnetic Interference Characteristics"

The HFC-6000 system was tested for EMI/RFI in accordance with EPRI-TR102323-R1. This testing and the test results show that it is qualified for safety related applications. Test procedures were established that follow the guidance of this MIL-STD.

ASME NQA-1/NQA-2 "QA of Design Software"

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

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

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

EPRI TR-102348 "Guideline on Licensing Digital Upgrades, December 1993"

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

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

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

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

Per this standard, a matrix was developed that demonstrates that the HFC-6000 system design complies with the individual specifications of this guidance document.

8.5.5 CFR and General Design Criteria (GDC)

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

The HFC-6000 QA procedures and record-keeping both conform to this requirement.

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

The HFC-6000 system has been tested and found to conform to the requisite design criteria

c) GDC 4 - Environmental And Missile Design Bases

The design basis for this requirement has been met and proven via testing of the HFC- 6000 system.

d) GDC 13 - Instrumentation And Control

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

e) GDC 19 - Control Room

The control requirements are met by the HFC-6000 and in particular the Flat Panel Module. The requirements for an auxiliary shutdown location will be met during the plant specific implementation.

f) GDC 20 - Protection System Functions

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

g) GDC 21 - Protection System Reliability And Testability

The reliability and testability of the HFC-6000 digital platform meets the requirements of this GDC.

h) GDC 22 - Protection System Independence

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

i) GDC 23 - Protection System Failure Modes

HFC-6000 plant specific protection systems are designed (and verified) to fail to a fail-safe or acceptable state. Plant specific applications of the HFC-6000 system responsible for protections will assume the proper failure modes.

j) GDC 24 - Separation of Protection And Control Systems

The HFC-6000 system design ensures that there is adequate separation of protection and control systems per this criterion.

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

The HFC-6000 reactivity control systems will meet the requirements of this GDC. Fuel design limits will not be exceeded for any single malfunction of the digital platform.

l) GDC 29 - Protection Against Anticipated Operational Occurrences

HFC-6000 protection and reactivity control systems will continue to meet the requirements of this GDC. Failure to accomplish the safety function has been determined to be unlikely.

m) GDC 37 - Testing of Emergency Core Cooling System

ESFAS HFC-6000 system applications will support this requirement with its configurations for periodic and functional testing

n) GDC 40 - Testing of Containment Heat Removal System

o) GDC 43 - Testing of Containment Atmosphere Cleanup Systems

p) GDC 46 - Testing of Cooling Water System

q) GDC 54 - Systems Penetrating Containment

These GDC's are all supported by the HFC-6000 system design when it is used in plant specific applications as called for by the individual criterion

r) 10 CFR Part 50, Appendix B

All activities affecting the safety related functions of the HFC-6000 system meet the requirements of this Appendix. The requirements of Appendix B are rigorously adhered to during the design control process, purchasing, fabricating, handling, shipping, storing, building, inspecting, testing, operating, maintaining, repairing and modifying of the HFC-6000 system. Quality assurance for the HFC-6000 system consisted of the proper planned and systematic actions necessary to provide adequate confidence that that the HFC-6000 system will perform as

required. Additional details regarding quality assurance activities for the HFC-6000 system are discussed in this section.

s) 10 CFR Part 21

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

t) 10 CFR Part 50.36

The HFC-6000 will maintain all limiting safety system settings The HFC-6000 system setpoint methodology will readily replace existing analog system setpoint methodologies with an accuracy and drift control rate superior to that previously reported with analog systems. With these improvements, the surveillance interval for the HFC-6000 can readily support a 24 month fuel cycle (30 months maximum).

u) 10 CFR Part 50.49

The HFC-6000 is environmentally qualified in accordance with the requirements of 50.49. The qualification process is described in more detail in association with the discussion of the system's compliance with the qualification criteria presented in EPRI TR-102323. This discussion can be found in Section 9 of this report.

v) 10 CFR Part 50.62

The ATWS equipment will remain diverse from the RTS and ESFAS equipment. Hardware and/or a software common mode failure will not be able to render the RTS, ESFAS and ATWS inoperable at the same time.

8.6 Defense-in-Depth and Diversity Evaluation Process

8.6.1 NRC Position 1

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

8.6.1.1 Compliance to Position 1

A plant specific diversity and defense-in depth analysis will be performed utilizing the guidelines provided in NUREG/CR 6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems, "December 1994.

The analysis will demonstrate that diverse plant equipment and operator action can be utilized to cope with the plant's design basis anticipated operational occurrences concurrent with a

common-mode failure in the HFC-6000 software-based equipment, such that the acceptance criteria stated in BTP HICB-19 will be met. The defense-in-depth and diversity analysis will utilize best-estimate analytical methods and realistic assumptions, including crediting operator action where adequate displays and controls remain that are not affected by the common-mode failure and sufficient time exists to perform the operator action.

8.6.2 NRC Position 2

In performing the assessment, the vendor or applicant/licensee shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate methods. The vendor or applicant/licensee shall demonstrate adequate diversity within the design for each of these events.

8.6.2.1 Compliance to Position 2

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

8.6.3 NRC Position 3

If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, should be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.

8.6.3.1 Compliance to Position 3

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

8.6.4 Critical Analog Signals

Critical analog signals are defined as those signals that are utilized as input signals to the HFC-6000 safety system and that are also required to be utilized for display and/or control functions that support the defense-in depth and diversity analysis. For these signals, a separate analog signal(s) will be developed prior to the utilization of the signal in the HFC-6000 safety system as shown in the example in Figure 8-1 below. The separate analog signal will be isolated with a class 1E qualified isolator and sent to the existing non-safety-related diverse display and/or control system. In the event that only an indication is required to support an operator action, an existing safety-related indicator could be used without requiring isolation. In either case, the diverse control system or operator action based on either the non-safety display or the Class 1E indicator could be credited in the defense-in-depth and diversity analysis to assist in coping with the anticipated operation occurrence.

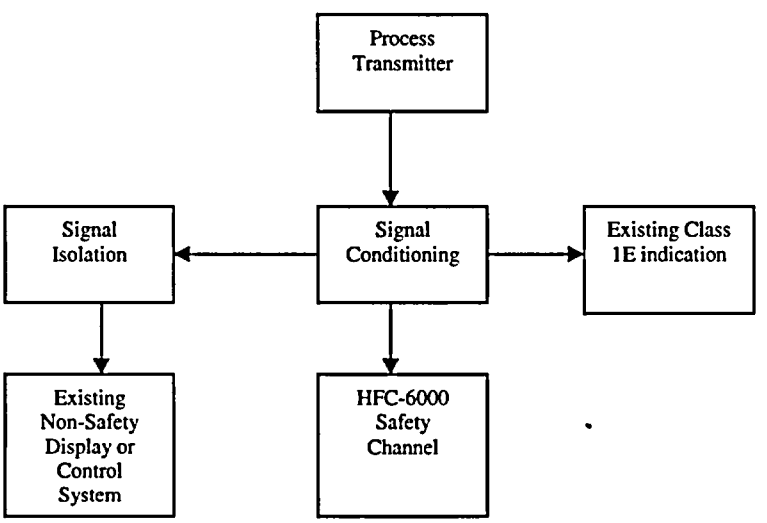

Figure 8-1 - Configuration for Critical Analog Signals

8.6.5 Critical Manual Signals

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

8.6.6 Implementation of Critical Manual Signals

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

8.6.7 Conclusion

The HFC concept for safety is based upon a simple system approach. Quality is designed and built into the HFC-6000 system such that any type of failure both hardware and software is highly unlikely. The design, qualification, and in-service testing afforded by the HFC-6000 system are implemented to minimize the probability of failures of all types. However, additional safety is achieved by employing the concepts of defense-in-depth and diversity. HFC's strategy for Diversity and Defense-In-Depth techniques has been devised to satisfy NRC acceptance criteria contained in BTP-19. The HFC goal is to meet the requirements with the following implementation goals:

- New diverse instrumentation and manual controls are not necessary because of the manner in which the HFC-6000 is designed and implemented at plant sites. The existing information available will be retained such that the plant can be placed in a hot-shutdown condition concurrent with a postulated SWCMF to the HFC-6000.
- Engineering assessments will be acceptable for most of FSAR Chapter 15 accident analysis. A detailed quantitative assessment will not be necessary. Where possible, risk-based assessments will be used to determine the significance of the event concurrent with the postulated SWCMF. This risk-based effort will follow the guidance offered by EPRI and the NRC.
- It is not anticipated that diverse systems will need to be added or existing systems will need to be modified to accommodate the results of the postulated SWCMF. Existing systems including those required by the ATWS rule will be sufficient.

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

HFC has demonstrated and will be able to demonstrate for future plant specific applications that the HFC-6000 design addresses Diversity and Defense-in-Depth consistent with NRC requirements and satisfy NRC acceptance criteria for this topic. Furthermore, HFC and future plant specific customers are expected to follow the risk-based Defense-in-Depth and Diversity assessment guidance and will use it when NRC approval is granted. Implementation of plant specific HFC-6000 Instrumentation and Control system upgrades in accordance with guidance

offered in NUREG/CR-6303 and HICB BTP-19 assures that adequate diversity and defense-in-depth is provided in HFC's design approach.

8.7 Cyber Security

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

[

]

Since the HFC-6000 is a closed system, there is no opportunity for outside cyber security threats such as a virus causing on-line modifications to an operating system or to any software. The safety related portion of the HFC-6000 is not accessible by outside communication means as there are no outside communication links that can alter any programming functions including the

logic gate arrays. The development and the final design for the controllers are inaccessible to outside cyber security threats. For maintenance, calibration and other test activities a security plan, training, work permits, and user authentication are extended to the HFC-6000 to prevent unauthorized changes to hardware or configuration to limit cyber security threats for this area.

[

]

The HFC cyber security design demonstrates protection from the four classes of cyber security attacks. [

]

The four types of postulated cyber security threats to the HFC-6000 have been considered and judged not to be credible due to the impediments established by the HFC-6000 design and varied plant administrative procedures. The HFC cyber security design and the plant specific procedures adequately demonstrate protection from the four pertinent classes of cyber security attacks. The combination of these features demonstrates that the HFC-6000 system is not vulnerable to any analyzed cyber security attacks either from internal sources or through network connections.

8.8 Isolation and Independence

The HFC-6000 platform is qualified as a safety related device without any non-safety related components. In addition, its qualified isolation capabilities are guaranteed by the use of isolation devices (Fiber Optics Transmitters, B232 FOT) and fiber-optics cables as the communication medium in order to provide both physical and electrical isolation. This isolation scheme is applied to three communication paths:

A) Interface among all four (4) safety channel controllers

B) Communication among safety controllers within the Safety Train

C) Communication to non-safety devices and network

8.8.1 Interface among all four safety channels

[

]

8.8.2 Communication among safety controllers within a train

The communication scheme among safety controllers within a train employs an architecture design identical to Figure G2 of IEEE Std 7-4.3.2 Annex G.

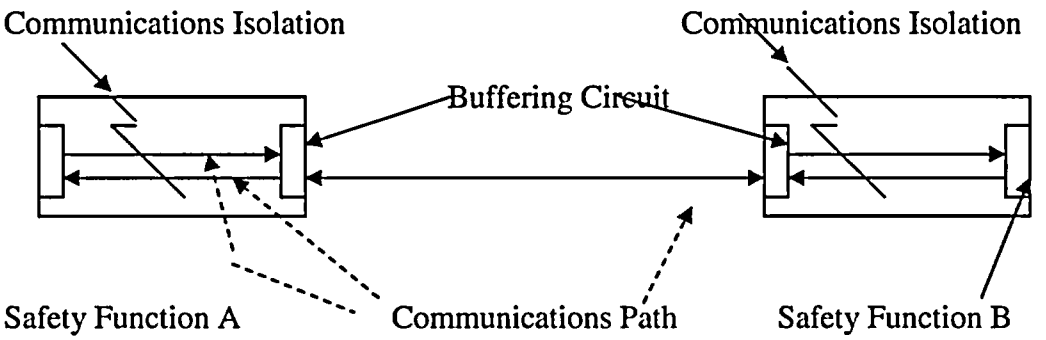

Figure 8-2 - Isolation between safety devices

The physical link of the fiber- optic network provides electrical isolation between one safety controller and another safety controller within the same train. This isolation is accomplished optically through dual fiber optic cables and circuits (Fiber- optic C-Links).

[

]

8.8.3 Communication to non-safety devices and network

The communication scheme from safety controllers to non-safety devices employs an architecture design identical to Figure G5 – "Communications between safety and non-safety computers" in IEEE Std 7-4.3.2 Annex G.

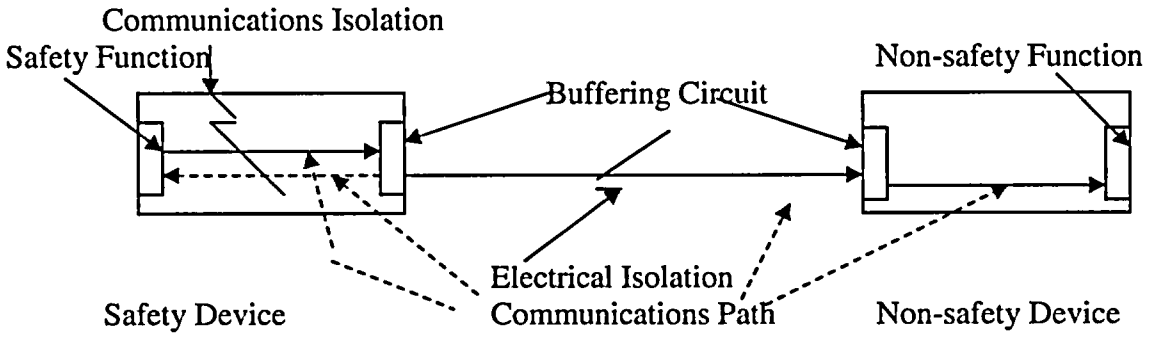

Figure 8-3 - Communication between safety and non-safety devices

The physical links of the fiber optic network also provide electrical isolation between the safety and the non-safety devices. This isolation is accomplished by means of optical transmission of data through fiber optic cables and isolation devices from the safety controller to the non-safety devices as shown in the above figure.

[

]

9 Equipment Qualification

9.1 Introduction

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

9.2 System Qualification Test Plan

9.2.1 Scope

The technical scope, focus, and content of EPRI TR-107330 define the basis for the steps involved in completing a generic qualification program. Accomplishing the qualification requires creation of a synthetic application, so the steps are similar to those in qualifying any device for safety-related service. These steps are:

A. The HFC-6000 product line was selected by HFC for qualification for nuclear safety applications.

B. An evaluation of the HFC-6000 and related third party sub-tier suppliers systems was performed. It was concluded that the HFC-6000 system and related third party systems, when fully and successfully tested in accordance with the EPRI TR-107330 were suitable to support nuclear safety-related applications.

C. A set of hardware test modules and supporting software was defined and used as the HFC-6000 qualification Test Specimen.

D. A Test System Application Program (TSAP) was defined and the software developed. The TSAP serves as a synthetic application that is designed to aid in the qualification and Operability tests.

E. The Test Specimen and the TSAP were combined into a suitable test configuration and a set of acceptance tests were performed. This activity constitutes the system integration testing for the Test Specimen.

F. A set of qualification tests to be performed on the Test Specimen were specified, including a defined set of Operability and Prudency tests to be conducted at suitable times in the qualification process.

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

Items A and B were addressed in prior sections of this topical report. This section addresses items C through G.

9.2.2 Equipment Tested

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

]

A small number of modules did not have acceptable test results. The modules will not be used in nuclear safety applications. Alternate modules which had acceptable test results will be used.

System layout drawings, wiring and power distribution diagrams, and assembly diagrams defined specific details of the hardware design for the Test Specimen. Test plans and procedures provided detailed requirements and instructions for equipment mounting and interfaces to be used for equipment testing. A TSAP was developed and installed in the master controller and the single-loop controller of the Test Specimen. Detailed requirements for the individual components of the Test Specimen and the TSAP were defined in a Requirements Specification. Detailed configuration information, such as module serial numbers and software versions, were recorded in the Master Configuration List (MCL), which is included as part of the qualification documentation.

9.2.3 Safety Functions Tested

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

1. The capability of the Test Specimen to perform design functions within specified tolerances under normal environmental and operating conditions.

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

   - Function during and after exposure to abnormal temperature and humidity
   - Function during and after operational basis and safety shutdown seismic events

- Function during and after application of EMI/RFI waveform exposures. Function during and after application of ESD test discharges
- Function during and after exposure to surge test waveforms
- Function under varying conditions of source power quality
- Demonstrate specified levels of Class 1E to non-Class 1E isolation and continue functioning after application of the test voltage levels.

9.2.4 Test Requirements

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

- Tests conducted prior to the start of qualification testing confirmed that the synthetic TSAP created for qualification testing purposes operated as intended.

- Operability and Prudency tests established a performance baseline for the Test Specimen. These tests were repeated at various points before, during and after the qualification test to demonstrate that the system performance remained within acceptable limits.

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

9.2.4.1 Test Plans and Procedures

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

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

The master test plan provides a link between the requirements of the EPRI TR-107330 standard and the procedures that were used to conduct the tests. The test plan addresses the general

approach for the test program, and it included a separate test plan for each qualification test to be performed. Individual test plans for each test are included as attachments to the Master Test Plan, and each one identifies references to requirements and defines requirements, testing criteria, acceptance criteria, and documentation for a particular test.

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

Three application programs were associated with the testing effort defined by these test plans:

- Redundant Controller TSAP
- Single Loop Controller TSAP
- HFC Plant Automated Tester (HPAT) program for the test workstation

HFC used both a Sequence of Events (SOE) utility and a Historical Archiving System (HAS) utility to log data generated during the test program. Both the SOE and the HAS are HFC proprietary utilities that were developed to operate with HFC control systems. [

]

Figure 9-1 illustrates the process flow used to extract data logged during the various tests for subsequent analysis and evaluation.

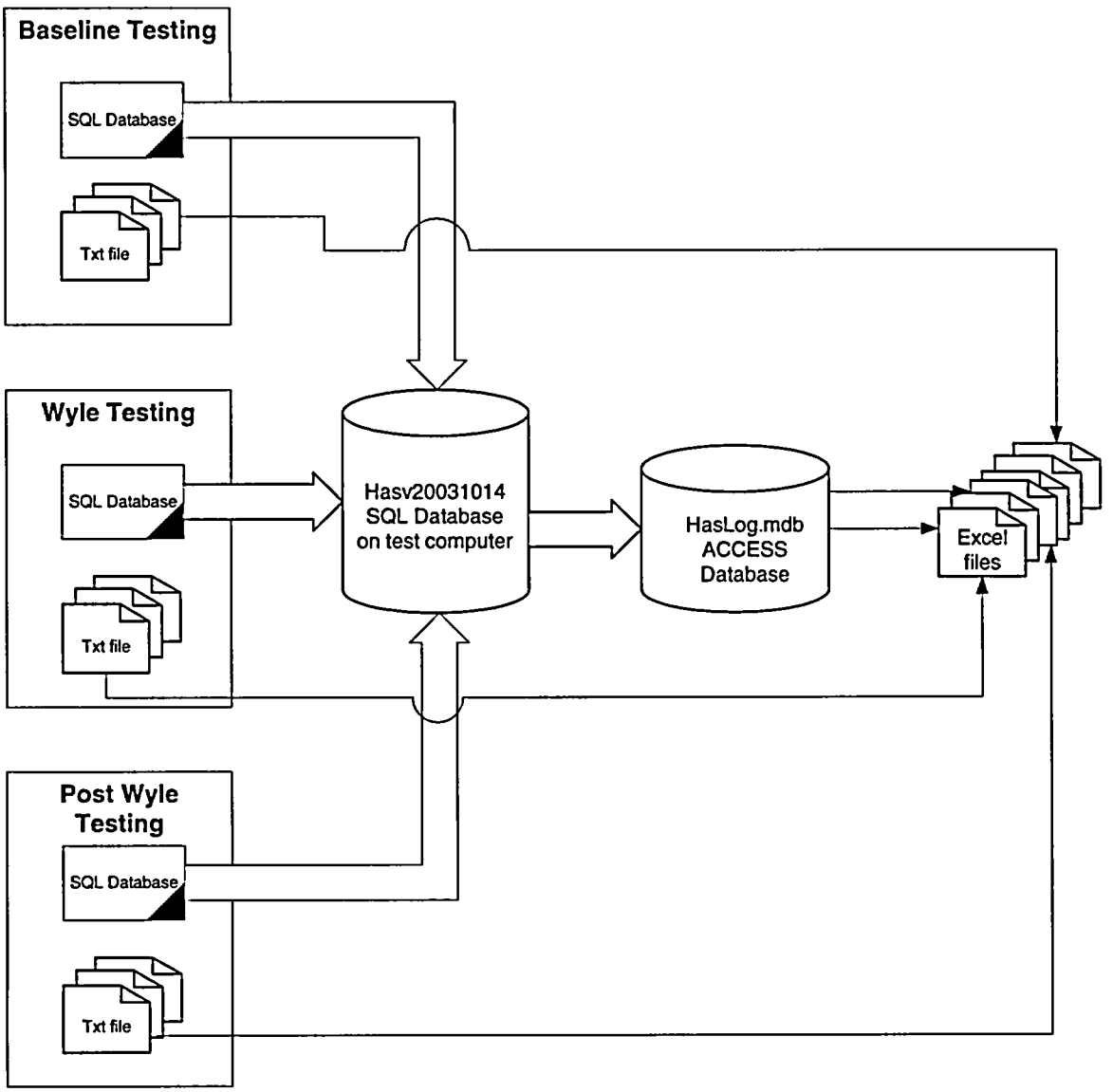

Figure 9-1 - Test Data Flow Chart

9.2.4.2 Test Sequence

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

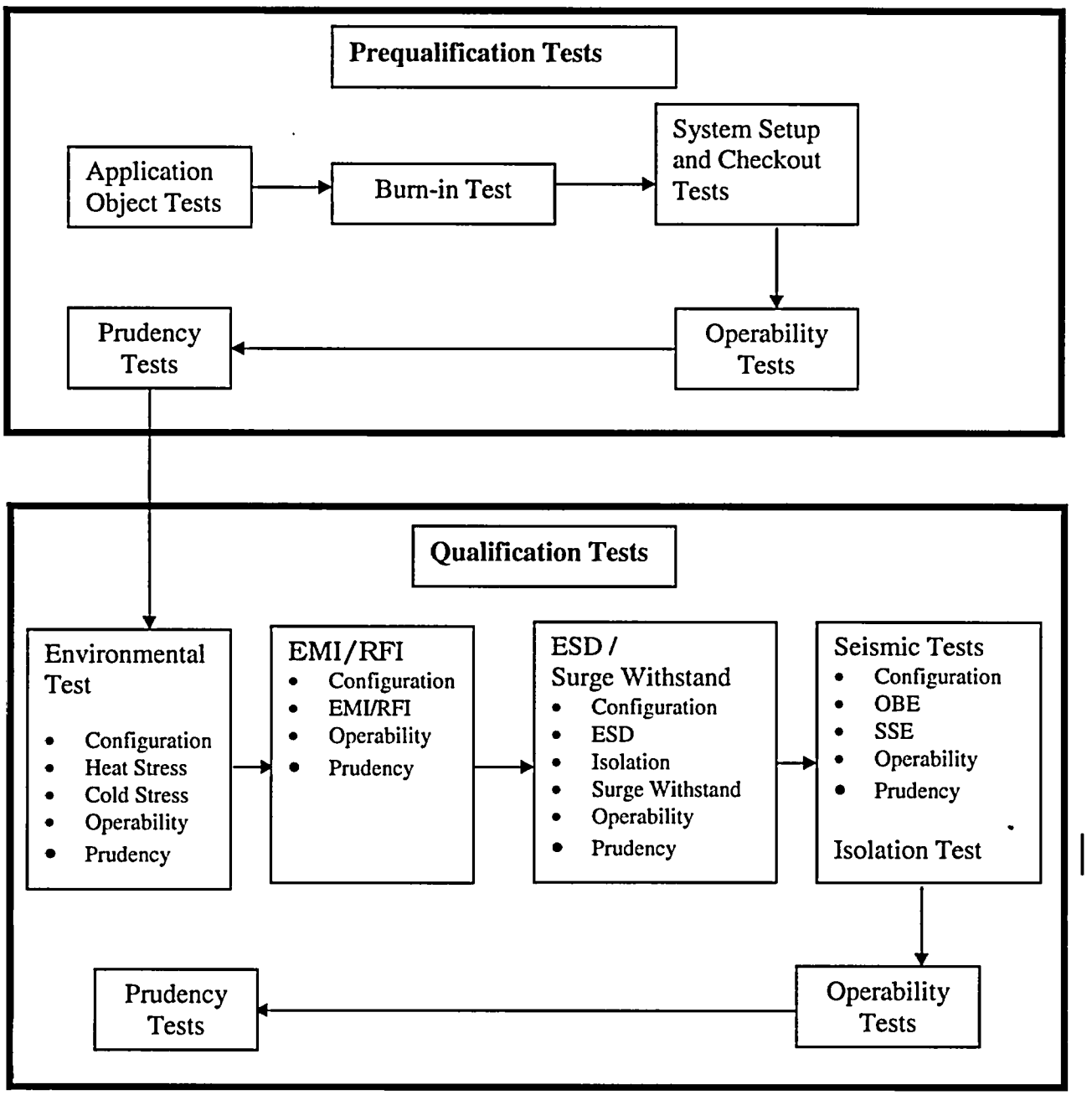

Figure 9-2 - Overall Test Sequence

NOTE

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

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

1. Configured Test Specimen components in accordance with applicable engineering drawings and HFC procedures at the HFC facility.

2. Validated Test Specimen configuration in accordance with the Integration (Setup and Checkout) Procedure.

3. Conducted prequalification tests at HFC facility.

4. Disassembled Test Specimen and shipped it to Wyle Laboratories for qualification tests.

5. Reassembled Test Specimen at Wyle Laboratories and verified its functional operation. The test procedure for each of the qualification tests defined the required functional verification of the Test Specimen before the start of the actual qualification test.

6. Performed environmental stress test.

7. Configured the Test Specimen for EMI/RFI testing and verified correct operation of the Test Specimen prior to the start of testing.

8. Conducted EMI/RFI testing.

9. Conducted ESD testing.

10. Conducted Surge Withstand testing.

11. Configured Test Specimen for seismic testing, and verified correct operation of the Test Specimen prior to the start of testing in accordance with the seismic test procedure.

12. Conducted Seismic tests.

13. Disassembled the Test Specimen and returned it to the HFC facility, and verified correct operation prior to the start of isolation testing.

14. Returned Test Specimen to HFC facility, reassembled, and verified correct assembly and interconnection of all components in accordance with TP0401.

15. Performed Class 1E isolation testing and non Class 1E isolation testing.

16. Conducted Operability and Prudency tests after completion of initial qualification stress testing.

17. During evaluation of test results, HFC concluded that the seismic test needed to be repeated. The Test Specimen was repaired and reconfigured in preparation for this retest.

18. Conducted TASP Verification (TP0408B), Operability (TP0402), and Prudency (TP0403) test prior to return to Wyle for seismic retest.

19. Reassembled the Test Specimen at Wyle Laboratories, validated functional operation in accordance with TP0408B, and conducted seismic retest in accordance TP0405, and ran the post tests required by TP0405.

20. Performed a complete seismic retest.

Detailed requirements for each test were presented in the individual test plans included within the Master Test Plan. Detailed instructions for conducting the specific tests were contained in separate test procedures.

9.2.4.3 Test Methodology

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

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

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

During the qualification tests, the Test Specimen was subjected to stress conditions to simulate various stress factors. While each test was in progress, the TSAP was processing test signal waveforms supplied by the HPAT. Responses of the Test Specimen during each qualification

test were logged and compared to the performance baseline established during prequalification testing to detect any deviation in performance. After all of the qualification stress tests were completed, Operability and Prudency tests were repeated, and all responses were recorded and compared with the performance baseline to identify any degradation in performance. In each case, the logged responses of the Test Specimen provided the objective basis for evaluating the performance of the generic modular control system design.

9.2.4.4 Test Personnel

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

9.2.4.5 System Operational Stress Conditions

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

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

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

Paragraph 4.3.6.3 of the EPRI standard identifies radiation exposure below 10^3 RAD which envelopes the environment in most nuclear plant control rooms. EPRI states that this is an insignificant factor for aging of the safety system. [

]

9.3 System Qualification Test Results

9.3.1 Prequalification Tests

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

9.3.1.1 Burn-in Test (TP0410)

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

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

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

9.3.1.1.1 Burn-in Test Results

All assemblies to be utilized in the qualification test program passed the burn-in test by successfully achieving the minimum cumulative 352 hours of burn-in operation. No anomalies were recorded for the modules that passed the burn-in test.

9.3.1.2 System Setup and Checkout (TP0401)

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

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

- Verified that all specified components of the Test Specimen had been received, installed, and functionally tested in accordance project document requirements.
- Verified that the correct software had been installed in Test Specimen, HPAT, and HPAT computer. This was done as part of the TSAP Validation Test Procedure.
- Performed Continuity Testing, which confirmed that all interconnection wiring was correctly installed.
- Verified that C-Link communication had been established.
- Verified that all HFC-6000 PCBs (Printed Circuit Boards) I/Os were functional and communicating with SBC06 controller.

9.3.1.2.1 System Setup and Checkout

All assemblies met the acceptance criteria for the setup and checkout test upon completion of the procedure.

9.3.1.3 TSAP Validation Test Procedure (TP0408)

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

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

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

9.3.2 TSAP Validation Test Procedures Test Results

At completion of the of the TSAP tests all TSAP software met the acceptance criteria.

9.3.2.1 Operability Tests (TP0402)

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

- **Accuracy Test** - This test developed a baseline to compare against the accuracy and linearity of the analog I/O modules observed during the qualification tests.
- **Response Time Test** – This test measured the response time for discrete and analog inputs.
- **Discrete Input Operability Test** - This test verified the capability of discrete input channels to detect a transition in the input signal being monitored.
- **Discrete Output Operability Test** - This test verified the capability of discrete output channels to operate reliably within its specified loading conditions.
- **Communication Operability Test** – This test verified reliable data transfer over the ICL, C-Link, and serial interfaces with Control Switch Module (CSM) and M/A stations.
- **Timer Test** – This test developed the baseline for the timer function accessible to the TSAP.
- **Failover Operability Test** – This test demonstrated correct operation of the failover function.
- **Loss of Power Test** – This test demonstrated correct response of all I/O channels to a loss of source power followed by reapplication of power to the system.
- **Power Interruption Test** – This test demonstrated the capability of the power modules to sustain system operation during a temporary (40-ms transient) power interruption.
- **Power Quality Tolerance Test** – This test was developed to demonstrate the capability of the Test Specimen to continue normal operation over a range of source power voltages and frequencies.

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

9.3.2.1.1 Operability Test Results

The acceptance criteria defined for the operability tests were met with the exception of deviations for a limited number of test cases. These include:

SOE Test Data

During the initial baseline tests, some of the SOE test data for the Operability Test and Prudency Test was overwritten during the test period. The digital input (DI) modules that provided the SOE function contained a circular buffer for logging SOE data as it was received.

Due to the circular nature of the buffer, when its storage capacity is exceeded, the earliest recorded data is overwritten. This problem was detected and corrected prior to the final Operability Test and Prudency Test. Subsequent Operability and Prudency test results were used to supplement the lost data.

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

[

]

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

Analog I/O Modules Out of Calibration

The analog I/O modules have a design accuracy of 0.1% over their entire operating range. Several of the modules had individual channels whose performance was outside of this accuracy range during the initial performance of the Operability and Prudency tests. This was not detected prior to completion of the stress testing. [

]

When the decision was made to rerun the seismic test, all of the analog modules were recalibrated and retested before returning to Wyle. During this test, the calibrated analog I/O cards all performed within the specified acceptance criteria.

HFC concluded that the out of calibration analog I/O cards had no impact on the performance of the qualification tests and had no impact on the ability to reach conclusions on the acceptance of the qualification test program.

Tolerance of Automated Test Records

The acceptance criteria for the analog I/O cards are 0.1% over their entire operating range. The HAS was inadvertently configured to log analog data points with a deadband of 0.5% prior to the initial execution of the Operability Test and Prudency tests.

[

]

EPRI Performance Limits

The timer function and response time did not perform within the limits indicated by EPRI TR-107330. The timer function of the HFC-6000 consistently operated within the theoretical limits for its design throughout system testing, and response time characteristics for this system are dependent on size of the application program. In each of these cases, the tests successfully established baseline characteristics that provided the basis for evaluation of the Test Specimen throughout qualification testing.

9.3.2.1.2 Conclusion

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

9.3.2.2 Power Interruption Test

The power interruption test required that half of the redundant power supplies be disabled during the 40-ms ac power interruption. When this condition was fulfilled and all spare slots were filled with operating modules, the remaining power supplies did not consistently prevent one or more of the modules from resetting. The system was designed to operate with two sets of power supplies connected to different power sources. Based on the single failure criterion, only one power source will experience a power interruption at any time, ensuring that the system will successfully maintain control without resetting during that interruption.

9.3.2.2.1 Conclusion

[

]

9.3.2.3 Prudency Tests (TP0403)

The initial execution of the Prudency Tests was performed during the same time period as that of the Operability tests. These tests, as defined by the EPRI standard, do not address any

specific requirement but exercise the Test Specimen in various ways to simulate potential in-service stresses. Throughout the period that the Prudency tests were running the Test Specimen power source was set to 90 vac and 57 Hz. The following specific tests were defined:

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

The Prudency tests were executed during the prequalification phase of testing to establish a performance baseline for the Test Specimen. The BOE test was repeated at various points during the qualification tests to identify any performance degradation from the performance baseline, and the entire test was repeated following return from Wyle. The test data was captured and recorded by both the SOE and the HAS. The SOE system has a 1 ms response time; but it is only capable of processing digital data, and has a smaller data storage capacity than the HAS. The HAS can log both analog and digital records, but it is limited to a maximum update rate of once per second.

9.3.2.3.1 Prudency BOE Test Results

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

SOE Test Data

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

Analog I/O Modules Out of Calibration

This matter was covered in the earlier Section on Operability Tests

Automated Test Result Tolerance

This matter was covered in the earlier Section on Operability Tests

Conclusion

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

9.3.2.3.2 Prudency Serial Port Failure Test Results

The Serial Port Failure test section of the Prudency test is configured to test the three different types of serial communication port employed by the HFC-6000 system. These are 1) the redundant communication link (C-Link) between all controllers within a system and between all controllers within a system and external workstations, 2) the redundant Intercommunication Link (ICL) that enables communication between the HFC-SBC06 and all other modules associated with a particular remote, and 3) a separate serial link to each control switch module (CSM) or M/A station.

The objective of the Serial Port Failure Test is to demonstrate that a hardware failure on a single serial link will have no adverse impact on the steady-state operation of the controller.

The Serial Port Failure test was run on the C-Link and the ICL during the prequalification phase of the program, and the acceptance criteria were met.

[

] The complete Serial Port Failure test was then run during execution of the Operability and Prudency tests before returning to Wyle for repetition of the seismic test. The acceptance criteria for all three links were met during that execution of the test.

Conclusion

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

9.3.2.3.3 Prudency Serial Port Noise Test Results

The Test Specimen includes two redundant serial links and a set of non redundant serial links to operator interface modules. The Serial Port Noise test was designed to superimpose a white

noise signal on either the transmit or the receive signal line of each serial link (one channel of the redundant pair) one at a time. The EPRI specification did not require execution of this test before, during, or after any of the qualification tests to be conducted at Wyle Laboratories.

[

]

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

Conclusion

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

All three links met the acceptance criterion except for one minor deviation:

[

]

9.3.3 Qualification Tests

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

9.3.3.1 Environmental Stress Test (TP0404)

The environmental stress test is one of the tests described by EPRI TR-107330 to qualify a commercially available PLC for safety-related applications in a nuclear power plant. This test exposes a specially configured HFC-6000 Test Specimen to extremes of temperature and humidity in order to induce accelerated aging of functional components. This testing was accomplished by enclosing the Test Specimen in an environmental test chamber in accordance with Wyle Laboratories test procedure 50043-1. The Test Specimen was running a TSAP throughout the test period, and its operation was monitored continuously by SOE and HAS data loggers located outside the test chamber. In addition, comprehensive functional tests were conducted before, after, and at specified points during the stress testing. The results of these tests were used to identify any deterioration in functional performance of the Test Specimen due to adverse environmental conditions.

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

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

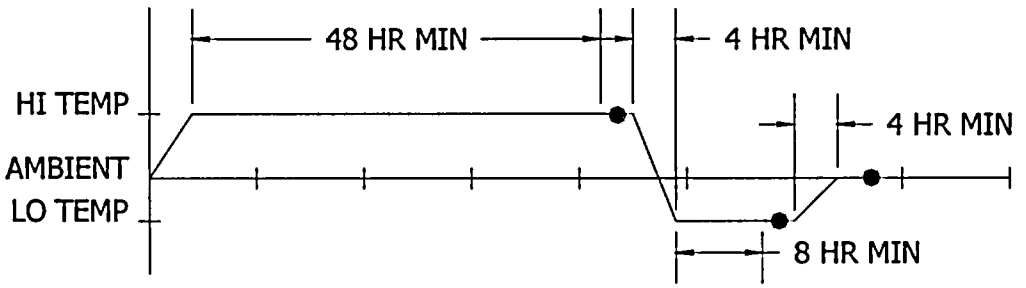

Figure 9.3 Environmental Stress Temperature Profile

9.3.3.1.1 Environmental Test Results

The environmental test results met all acceptance criteria.

Four areas exist for detailed evaluation of test results. The following conclusions were reached concerning these four matters.

Power Drop to Test Specimen

Certain of the test results during the temperature ramp down phase were complicated by intermittent failures in the Wyle power drop due to incompatibilities with the HFC variable voltage test equipment.

The variable power source upstream from the Test Specimen power supplies was set to 90 vac and 57 H as specified in EPRI TR-107330 prior to execution of the high temperature phase of testing. After the high temperature test was completed, the power source was left at these stress levels. During the ramp down phase of the temperature tests, the Wyle power drop experienced several intermittent failures that resulted in loss of supply power to the Test Specimen. The cause of the power trips was identified prior to the start of the low temperature period, and it was resolved by obtaining an additional power drop to eliminate the overload condition. Once power

was restored, the Test Specimen returned to normal operation. All trips of the Test Specimen were directly correlated to overload of the power drop from Wyle.

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

]

RTD Module

The Test Specimen included one HFC-AI8M module with four channels configured for data monitoring. The indicated temperature for each of these channels changed during the course of the environmental test and did not return to the original value after return to ambient conditions.

Physical resistors were used to simulate RTD elements, and these resistors were mounted on a terminal strip that was inside the environmental chamber. These resistors had been selected and matched within ±0.25 ohm prior to the initial execution of the Operability test. The values of the simulation resistors were found to have changed during the environmental test, and non of these resistors returned to their original value. These resistors are not part of the qualified products, and their change in value had no adverse impact on the qualification results and conclusions.

Conclusions

The power feed trips imposed additional stress on the system but was unrelated to the performance of the Test Specimen.

The intermittent failure of the HFC-SBC06 was evidently caused by the repeated trips of the power feed, but this had no impact on the functional performance of the safety system.

The apparent deviation of the RTD module was caused by the simulation devices. The RTD module continued to process the input signals it received correctly.

9.3.3.2 EMI\RFI Test (TP0407)

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

Overall test requirements are defined by EPRI TR-107330-R1; the levels of EMI/RFI susceptibility and radiation limits are defined in EPRI TR-102323-R1. It is the understanding of HFC that these values will be modified in the near future to reduce conservatism. The test was conducted at Wyle Laboratories based on Wyle Test Procedure 50044-10. Specific tests conducted were as follows:

- Radiated Susceptibility Test – RS-103 (Reference EPRI TR-102323-R1 Appendix B Paragraph 3.1)
- Low Frequency and High Frequency Conducted Susceptibility Test – CS101 and CS114 (Reference EPRI TR-102323-R1 Appendix B Paragraph 3.2)
- Conducted Emissions Test – CE101 and CE102 (Reference EPRI TR-102323-R1 Section 7)
- Radiated Emissions Test – RE101 and RE102 (Reference EPRI TR-102323-R1 Section 7)

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

The radiated susceptibility test was divided into several frequency ranges with a different signal source and antenna for each frequency range. Each test was executed twice: once with the antenna positioned at front center of the Test Specimen and once with the antenna at rear center.

The low frequency conducted susceptibility test was run at 30 Hz and 50 kHz. These test signals were injected directly into power leads of the Test Specimen. Two tests were executed: one for power module A of the redundant power supply (Model Jasper HML 601-5) and one for the non-redundant power supply of the single-loop rack (Model HFC-1039).

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

Wyle test personnel executed conducted emissions tests in accordance with Wyle Test Procedure 50044-10 Appendices B and C. The tests were performed in accordance with EPRI TR-102323-R1 Chapter 7, which covers power plant emissions limits and acceptable methods to be used for measuring these emissions levels. In addition, MIL-STD-461D CE101 was used to define the test method employed for measuring emissions between 30 Hz and 50 kHz, and MIL-STD-461D CE102 was used to define the method for measuring emissions between 50 kHz and 400 MHz. Specified portions of the Operability and Prudency tests were run during the test to ensure that an adequate level of controller activity was present while the measurements were being run. Separate tests were run for power supply group A of the redundant power supply (Model Jasper HML 601-5) and for the non-redundant power supply (Model HFC-1309) of the single-loop controller.

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

- Radiated Magnetic Field Emissions – a loop antenna was positioned at a distance of 7 cm from the test specimen. Separate readings were taken for up to 10 different loop locations.
- Radiated Electric Field Emissions – Separate readings were taken with the antenna positioned at the front center and rear center of the Test Specimen. The antenna type varied with frequency range as indicated in the Wyle test procedure.

9.3.3.2.1 EMI/RFI Tests Results

During the test, the HFC-6000 Test Specimen was mounted in open instrument racks. No additional cabinet or cable shielding was installed, and no additional noise filters or suppression devices were used on the input/output interfaces. Therefore, the test specimen was fully exposed to radiation from an external source or open to emit radiation generated internally. In any real

application, the HFC-6000 equipment will be installed in cabinets qualified for Class 1E applications. Such cabinets will provide shielding against external radiation, improving the overall radiation withstand capacity of the system. For example, HFC had EMI/RFI tests conducted for the Ulchin Nuclear Plant Control System (PCS) project. The test specimen for this system was composed of assemblies similar to those of the HFC-6000 Test Specimen, except they were installed in a safety cabinet assembly designed for Class 1E qualification. The results for that test were satisfactory for all frequency ranges included in the test.

[

]

9.3.3.3 ESD Test (TP0409)

Components of a HFC-6000 control system may be installed in an electrical equipment room as well as at various locations near the field equipment under control. In either case, the potential

exists for exposure of sensitive electronic components to high voltage electrostatic discharges (ESD). This test subjects each major component of the HFC-6000 Test Specimen to simulated ESD pulses to establish its capability to withstand such discharges without disabling or disrupting normal operation.

Detailed requirements for ESD immunity are defined by EPRI TR-102323-R1; the specific level of ESD immunity required is defined in EPRI TR-102323-R1 Appendix B Paragraph 3.5. ESD testing was conducted by Wyle Laboratories based on Wyle Test procedure 50044-10 Appendix I. The test methods used to apply the ESD pulses are defined by IEC 1000-4-2 (equivalent to IEC 801-2).

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

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

9.3.3.3.1 ESD Test Results

The HFC-6000 Control System did not exhibit any failure condition resulting from the ESD testing. [

]

9.3.3.4 Surge Withstand Test (TP0406)

Power, electrical I/O signal lines, and hardwired communication cables may be exposed to high amplitude transient signals in the locations where control system hardware may be installed. These locations include an electrical equipment room and various other locations near the equipment under control. The test covered by this document injected a large amplitude surge waveform at specified points of the Test Specimen. The purpose of this test was to demonstrate that Test Specimen performance characteristics remained within acceptable limits during and after exposure to such discharges. The Test Specimen was powered on and running the TSAP while the test pulses were being applied to specific circuits in accordance with EPRI TR-107330.

9.3.3.4.1 Surge Withstand Test Results

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

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

9.3.3.4.2 Surge Test Results

In no case did application of the test surge waveforms result in failure of the Test Specimen as a whole, and in no case did the test pulses result in failure or disruption of any module other than

the one specifically under test. [

•

]

Conclusion

The HFC-6000 Test Specimen satisfactorily met all of the performance and acceptance criteria for surge testing. Some components were damaged as the result of the test pulses; but that damage was limited to the specific components under test, and the remainder of the system continued operating normally.

[

]

9.3.3.5 Seismic Tests (TP0405)

Seismic testing exposed the HFC-6000 Test Specimen to a set of dynamic spectra designed to simulate an Operating Basis Earthquake (OBE) and a Safety Shutdown Earthquake (SSE). This test spectrum defined by EPRI TR-107330 is shown in Figure 9.4. The dynamic spectra consisted of tri-axial, random, multi frequency waveforms that were transmitted to the Test Specimen by means of hydraulic actuators attached to a Seismic Simulator Table. The overall scope of testing consisted of the following phases:

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

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

- 24 accelerometers,
- The SOE logger with a total capacity of 48 digital points, and
- The HAS that has the capacity to log any point available from C-link DDB

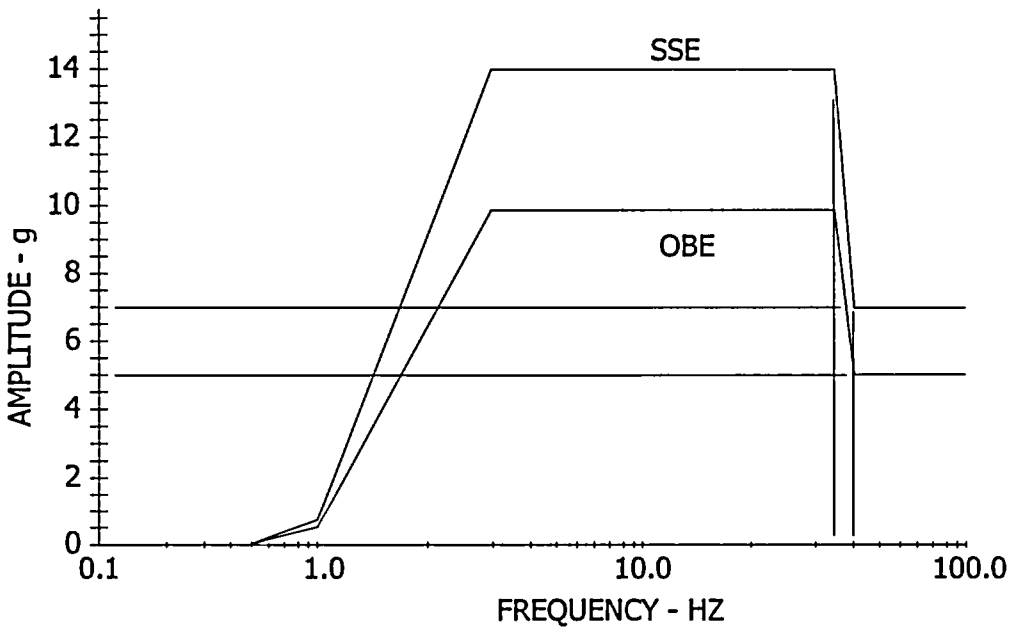

Figure 9-3 - RRS Test Spectrum

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

Wyle personnel conducted the dynamic seismic tests using the TRS established as the result of the resonance sweep test in accordance with Wyle Test Procedure 50043. Wyle personnel

performed five tests based on the OBE RRS and one test based on the SSE RRS. The response spectrum of the Test Specimen was reported for 0.5%, 1.0%, 2.0%, 3.0%, and 5.0% damping factors. While any particular dynamic test was in progress, an HFC test engineer ran the specified combination of automated tests to verify overall system performance. Following each dynamic test, the entire Test Specimen was examined for mechanical damage. Any mechanical damage sustained during testing was recorded and reported in detail in the seismic test report.

9.3.3.5.1 Seismic Test Sequence

The seismic test was initially run after completion of surge withstand testing. According to the HFC qualification master test plan, the seismic test was scheduled to be conducted right after environmental test so that any components damaged by the destructive Surge Withstand test will not complicate the Seismic test results. However, the Seismic test was performed after Surge Withstand test due to Wyle lab's scheduling conflict. During the analysis of the test data, the SLC was found to have passed all five OBE test runs and the SSE test run without any fault. HFC decided to repeat the entire seismic test mainly because of the incomplete logging data. The following summarizes the overall sequence for the repeat of the seismic test:

1. Repair or replace any electronic assemblies that had been damaged by the surge withstand and isolation tests.

2. Ensure that all replacement electrical hardware had successfully passed the required 352-hour burn in period.

3. Repair and redesign mechanical structures that had not withstood the initial seismic test.

4. Perform the TSAP Validation Test (TP0408B) to verify that the reconfigured Test Specimen was fully operational.

5. Repeat the entire Operability and Prudency tests prior to shipping the Test Specimen to Wyle Laboratories.

6. Repeat the entire seismic test as defined by TP0405 in Wyle.

Results of TSAP Validation Test (TP0408B)

The Test Specimen was reconfigured to repair all hardware failures that occurred during the previous testing and to correct any errors that had been detected. After this reconfiguration was completed, a functional test was performed to verify that all configured I/O points operated correctly and to verify overall operation of all TSAP functions.

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

Results of Operability Test (TP0402)

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

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

Results of Prudency Tests (TP0403)

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

- In a few instances, the value of logged HAS data for the analog BOE points exceeded the 0.3% deviation from the expected value.
- Two abnormal transitions were detected during the serial link noise test for the ICL.

HFC considers neither of these deviations significant because they are limited in scope and did not affect the system as a whole.

Results of Seismic Test 2

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

]

Conclusion

The Test Specimen was subjected to OBE and SSE test spectra up to the limit of the Wyle seismic simulator table (10 g maximum acceleration). The Test Specimen passed through the second execution of the seismic test with three minor anomalies, all of which have satisfactory resolution:[

•

]

9.3.3.6 Isolation Test

As noted previously, the HFC-6000 hardware may be installed both in an electrical equipment room and at various other locations near the equipment under control. When I/O chassis are physically located in a remote location with respect to the controller hardware, they will be connected to the controller by means of a dedicated fiber-optic communication link. This link will provide the mechanism for ensuring physical and electrical isolation between a Class 1E controller and non-Class 1E equipment in an installation. This test covered specific testing to demonstrate two categories of isolation:

- Channel-to-channel isolation of I/O ports under ordinary operation.
- Class 1E to Non-Class 1E (channel to channel and module to module) isolation.

The following tests covered channel-to-channel isolation testing for both Class 1E to Non-Class 1E and channel to channel isolation applicable to each of the individual I/O card types. The primary purpose of these tests was to demonstrate immunity to channel-to-channel interference during a design basis event. The test signals were applied to I/O channels both in the Class 1E portion of the Test Specimen and to I/O channels in the expansion rack. The general approach to testing consisted of two phases:

- First, selected channels were subjected to the Class 1E/Non-Class 1E isolation test signal. If the component under test exhibited acceptable isolation from other components within the system, application of additional test signals to that channel type was deemed unnecessary.
- If the component under test did not exhibit acceptable isolation in response to the initial Class 1E test signal, additional testing was conducted to determine the maximum test

signal that could be applied to that type of channel without affecting performance of other portions of the Test Specimen (channel to channel isolation).

The minimum acceptable level of channel-to-channel isolation for normal operation differs for each card type. The following list presents the minimum acceptable level of isolation as defined by EPRI-TR-107330 for modules of the HFC-6000 Test Specimen on a channel-to-channel or module-to-module basis.

- ±30 v peak for AI channels on a group basis
- 100 v peak for 48-vdc discrete inputs on a group basis
- 40-vdc for pulse input channels on a group basis
- 600 v peak applied for 30 seconds for 120-vac discrete output channels on a group basis
- 600 v peak applied for 30 seconds for 125-vdc discrete output channels on a group basis
- 600 vac and 250 vdc applied for 30 seconds for AO channels
- Twice the nominal output voltage for discrete output channels and serial I/O channels on a group basis

The Class 1E to Non-Class 1E isolation test refers to demonstration of electrical isolation of Class 1E control equipment from Non-Class 1E equipment as well as isolation between different Class 1E channels. The minimum signal levels used for this test were as follows:

- 600 vac applied for 30 seconds
- 250 vdc applied for 30 seconds

9.3.3.6.1 Isolation Test Results

Acceptance criteria for channel to channel testing are:

- No channel other than the one under test is affected by the test signal.
- Operation of no module other than the one under test is disrupted by the test signal.

Acceptance criteria for Class 1E to Non-Class 1E is discussed EPRI-TR-107330 (4.6.4), IEEE Std 603, IEEE Std 384 and RG 1.75. The test was applied to each of the I/O channel types except the HFC-PCC06 serial channels, which are connected to the CSMs and M/A stations. Overall test results were as follows:

In no instance did the test signal affect operation of the overall system.[

•

]

Conclusions

All channels tested satisfied EPRI guidelines for channel-to-channel isolation and module-to-module isolation.

[

]

9.3.4 Post-Qualification Tests

The Post-Qualification Tests consisted of re-running the System Setup and Checkout, Operability, and Prudency Tests at HFC following the return of the equipment from Wyle labs after completion of the first seismic test. The purpose of Post-Qualification Tests is to prove that

the HFC-6000 control system continued to operate properly after being subjected to the complete set of qualification tests.

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

Data from the Operability and Prudency tests was used to supplement or, in some cases, substitute for the corresponding test run during the prequalification period. This data was used to define the baseline for comparison to the results of the Operability and Prudency tests run during the various qualification Tests at Wyle labs.

9.3.4.1 Setup and Check-Out Test Results

All assemblies met the acceptance criteria for the set-up and check-out test prior to completion of the test.

9.3.4.1.1 Operability Test Results

[

-]

[

]

9.3.4.1.2 Prudency Test Results

The acceptance criteria defined for the Prudency tests were met with the exception of minor deviations for a limited number of test cases. [

-]

[

]

Conclusions

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

9.4 Conclusion

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

[

]

10 Software Qualification

For more than 25 years HFC has provided commercial grade digital control systems to industrial customers for critical applications where system reliability and availability are key considerations. The digital platforms for these applications have a significant documented history of successful operation in these applications. HFC-6000 is the dedicated product line for the safety I &C platform application.

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

1. The dedication of Pre-Developed Software (PDS)
2. The development of system software/firmware
3. The development of application software

Items 2 & 3 have the same development process in accordance with the existing HFC quality procedures and work instructions with the exception of coding phase for the PDS software. The actual application software development process will be handled by future plant specified requirements and qualification and will follow the same qualification process as Item 2 which is discussed in Section 10.2. The quality control process of application software is in accordance with the life cycle guidance presented in HICB BTP-14 and as outlined in Section 10.2.

The common practice of software operation and maintenance process is applied to all HFC-6000 safety related software.

10.1 The Dedication of Pre-Developed Software (PDS)

10.1.1 Software Commercial Grade Dedication Overview

[

] HFC has performed a commercial-grade dedication of the PDS, consistent with the guidance provided in EPRI report TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Application." Figure 3-2, "Equivalent Level of Assurance for Nuclear Grade and Commercial Grade Digital Equipment" was used to provide the integrated solution for the HFC dedication process. Relevant software characteristics were extracted from the TR and used for the establishment of the PDS overall quality and functionality. The necessary steps consisted of HFC dedication efforts, a review of the existing documentation and the operating experience. These efforts are discussed below.

The following diagram illustrates the entire scope of the commercial grade dedication process of HFC-6000 PDS.

10.1.1.1 Verification of Software Documentation

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

- The platform design is appropriate for deterministic operation. An external watchdog timer has been added to nuclear safety configurations for assuring fail-safe operation.
- The communication capability of the HFC-6000 equipment can be configured to accomplish communication between redundant channels or trains in a manner that complies with the electrical and communication isolation requirements of IEEE Std 603-1991 and IEEE Std 7-4.3.2 along with the NUREG-0800 guidance to assure independence of redundant elements.
- The records of the original design and QA process were not sufficient to support dedication without an examination of the product operating history and the performance of supplemental testing. Supplemental activities that were performed include the items in Figure 10-1.

10.1.1.2 Documentation Evaluation

[

]

10.1.1.3 Software and Validation Testing Program

HFC determined that supplemental testing needed to be performed to provide further evidence of product quality and suitability for dedication for safety-grade application. The following testing programs were conducted for the HFC-6000 platform:

- Application Object Testing
- Software Component Testing
- Prototype Testing
- Functional testing
- Stress Testing.

Please refer to section 10.1.3 for a detailed description.

10.1.1.4 Operating History Evaluation

The software components to be utilized in the HFC product were identified and their operating history was defined. The evaluation of the operating history demonstrated that the software has significant experience in critical application, including Korean nuclear power plants. The software has been stable for a long duration with very few defects, supporting the conclusion that its inherent quality makes it suitable for dedication for use in nuclear safety applications. Furthermore, it was concluded that the operating conditions in Korean plants were either similar or even identical to the condition that will be seen in US nuclear plants. This is discussed further in section 10.1.4.

10.1.2 Verification of Software Documentation

HFC-6000 software components include a combination of HFC's field-proven commercial grade PDS and software products that have been modified or developed anew. In either case, software is defined as software components and is used by related hardware modules. Please refer to the Appendix A for a detailed description of the HFC-6000 documentation map.

10.1.2.1 Software Requirements

The requirements of the PDS software components were documented in the requirement specification of HFC-6000 modules during the software dedication process of the HFC-6000 product line. Since the HFC-6000 is essentially a re-packaged product line, it has the same

hardware circuitry when compared with the existing ECS-1200 product line but with a form factor change. This form factor change includes rack size, connectors and packaging of field wires termination.

10.1.2.2 Software Design Specification

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

10.1.2.3 Software Dedication Process

[

] HFC evaluated the PDS and provided a re-engineering process that proves adequate reliability in accordance with nuclear safety related software standards. With this qualification process, the technical and regulatory issues associated with the use of commercial grade item (software) dedication have been addressed. A level of assurance comparable to the level of the 10 CFR 50 Appendix B requirements has been accomplished with the HFC dedication process. The safety functions and critical characteristics of the digital platform have been defined and an evaluation consisting of several testing methods has been completed. The guidance of EPRI TR-106439 and IEEE Std 7-4.3.2, Appendix D was used as a means for the qualification of the PDS.

[

]

For PDS, HFC has established a two-fold process which adapts the guidance in EPRI TR-106439. This dedication process consists of operational history, additional testing and documents reconstruction. The testing performed on the pre-developed software was directed at measuring the quality of the software. It was used to validate the functional characteristics of the software. This included accuracy, acceptability, clarity, completeness, correctness, interface consistency, interoperability, performance (efficiency and timing), preciseness, robustness, security, simplicity, understandability, and usability. In addition to these, the internal engineering

characteristics were validated. These included integrity, internal consistency, testability, and validity. The inspection and test process for the software consisted of source code inspections, software component testing, application object testing, prototype testing, and stress testing.

10.1.2.4 Source Code Inspection

[

]

10.1.3 Software Validation and Testing Program

Software Testing was performed in the following series of five (5) tests. The static testing that was performed in the HFC-6000 software was application object testing and software component testing.

10.1.3.1 Application Software Object Tests

In Accordance with EPRI TR-107330, a comprehensive Application Object Test (AOT) was conducted on HFC-6000 product line. This included all software components that have a direct impact on the application code or that can be accessed by application code while it is running on the system processor of the HFC-SBC06 controller module. Such software components are designated as Application Software Objects (ASO). [

]

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

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

10.1.3.2 Software Component Tests

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

Software component tests were conducted on the software components that are used in the HFC-6000 product line. Software component testing activities included determining the features to be tested, designing test cases, designing the test set up and the test environment, identifying acceptance and rejection criteria, executing the tasks, analyzing test results and reporting. A test design is based on the software functions described in the PDS documentation or the HFC-6000 product requirement specification. Test inputs were defined during design of the test cases and the expected outputs were determined. Since most of the software components are part of the printed circuit board firmware, software component testing is mostly low level code testing using an emulator to create a simulation testing environment. Test software including one or more software components were run on a representative hardware platform.

[

]

All major software components were tested and test reports were reviewed and documented. There was no critical defect found during these tests.

10.1.3.3 Prototype Testing

A prototype test is a selected test set that engineers use to prove a design. The purpose of prototype testing is to test the feasibility of the design and operability of the hardware and software module. [

]

All prototype tests of the HFC-6000 required by the test procedure were completed and all acceptance criteria have been met. The prototype test reports were reviewed and documented.

10.1.3.4 Functional Tests

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

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

]

All functional tests of the qualification test set were completed and all acceptance criteria have been met. Test reports were reviewed and documented.

10.1.3.5 Stress Tests

The purpose of stress tests is to prove that the software modules' functionality and performance do not degrade under stress conditions. In addition to the qualification tests, the HFC in house laboratory has the capability to perform various software stress tests, such as extra CPU load, overload data access rate, heavier communication traffics, memory access integrity with extra length of bus extension, etc. The measurement criteria include errors count of memory read/write, communication link status, dynamic data equalization between the redundant controllers, and failover mechanism. Stress test was performed on HFC-6000 software components as a part of software validation and dedication process.

This stress test was completed and all acceptance criteria have been met. Test report was reviewed and documented.

10.1.4 HFC-6000 Operating History

10.1.4.1 Operating History Background and Evaluation Approach

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

[

]

The operating history evaluation is directed primarily at the basic system software. Critical defects, if any, are also evaluated for the hardware design.

The Operating History evaluation process included:

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

10.1.4.2 HFC Product Lines

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

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

The HFC-6000 product line incorporates many of the hardware and software features of the AFS-1000 and ECS-1200 product lines. The HFC-6000 includes form factor changes but still uses the basic hardware and software components from the earlier product lines to produce a new product line for nuclear safety I &C systems. [

]The software for the I/O modules for HFC-6000 is identical to the predecessor systems. HFC-6000 has a subset of software components from the ECS-1200 product line and the later model AFS-1000 product line (from 1995). Therefore the operating history of the AFS-1000 and ECS-1200 are applicable to the HFC-6000.

10.1.4.3 Product line History

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

10.1.4.3.1 AFS-1000 Product line History

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

Table 10-1 – AFS-1000 Product line history

10.1.4.3.2 ECS-1200 Product line History

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

Table 10-2 – ECS-1200 Product line history

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

Table 10-1 shows the relationship of the HFC-6000 to the AFS-1000 product line. The software of the two product lines is essentially the same design with the exceptions of different coding for the earlier versions of the microprocessors. However, the HFC-6000 inherited not only the special I/O circuitry for nuclear safety I &C system but also the control system logics were merged into HFC control algorithms as the base of critical mission control algorithms. The consideration of the AFS-1000 in the operating history analyses is due to the fact that the AFS-1000 basic systems software including the operating system and I/O interface software have operated in the Korean Yongwang 3 and Yongwang 4 plants since 1994 with no software design defects. No defects were detected and no changes to the basic software were made since delivery in 1994. This is used in part to validate the quality control measures of the HFC software design and test processes. The Yongwang 3&4 systems software was developed using software quality processes typical in the fossil power plant industry period prior to the 1990 Yongwang 3&4 development period. The current HFC software quality processes have continued to advance to

meet the more demanding codes and standards for nuclear power plant safety applications. [

]

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

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

[

]

10.1.4.6 ECS-1200 Operating History

As discussed above, the HFC-6000 is a technology extension of the ECS-1200 using the same basic hardware components with form factor changes and with no changes in the basic system software modules. The software operating history for the ECS-1200 is therefore directly applicable to the HFC-6000.

The ECS-1200 product line has been used in fossil power plants and industrial applications for nearly 25 years and recently in a nuclear plant in Korea. Table 10-3 provides a list of the key installations for the ECS-1200 systems, date of initial operation and, the specific application.

Table 10-3 - Key ECS-1200 Installations

10.1.4.7 Module Operating Years (TMOY) calculation

The total module operating years (TMOY) for each module type has been calculated. This TMOY calculation applies to hardware modules and associated software modules. Associated software module is the software contained in, and required to support a given hardware module.

For each module, the total module operating years (TMOY) is calculated by summing the plant module operating years (PMOY) and then summing these to reach the TMOY.

The PMOY is

> PMOY = Number of type x modules in the system multiplied by the number of plant operating years

This calculation is performed for each module type for each plant.

The total module operating years is defined as

> TMOY = Sum of the PMOY for each module

10.1.4.7.1 The assumption of TMOY calculation

[

]

Table 10-4 - TMOY Calculation

10.1.4.8 Determination on Critical/Non-critical Software Defects

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

[

]

10.1.4.9 Conclusions of defect analysis

[

]

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

10.1.4.10 Summary of Operating History

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

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

  The excellent operating history of AFS-1000 systems provides the qualitative proof of the HFC design and application engineering process. They are used in the boiler safety and nuclear safety related control and non-safety application. The typical project is the Korean Yongwang 3 & 4 nuclear plant control system (Total 1900 loop controllers) which had no software change since its commission in 1994. This AFS-1000 prior SBC-05 system also provides qualitative results but it is not used in the table 10-5 quantitative results.

- AFS-1000 SBC-05 control systems

  The AFS-1000 SBC-05 had been used as the upgrade path for older AFS-1000 product line. Since it has the same set of software modules as the ECS-1200 control system, it can be used as quantitative proof to validate the integrity of HFC-6000 software components.

- ECS-1200 Control System

  The HFC-6000 software components are a subset of the ECS-1200 product line software. The operating history of the ECS-1200 control system has been used in the calculation of the TMOY. Based upon the above evaluation process and calculation, it proves the excellent reliability of these software components [
  ]

10.1.5 Software Operation and Maintenance

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

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

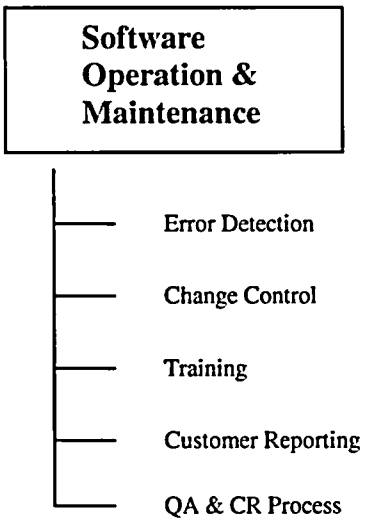

Figure 10-2 - Software Operation and Maintenance

[

]

10.1.5.1 Error Detection

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

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

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

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

10.1.5.2 Error Correction Change Control

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

10.1.5.2.1 Change Management Levels of Authority

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

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

10.1.5.2.2 Software Change Request (SCR)

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

Table 10-6 - Software Change Process

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

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

10.1.5.2.3 Audits and Reviews

[

]

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

10.1.5.3 Training

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

10.1.5.4 Customer Reporting

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

10.1.5.5 QA & CR Process

HFC Quality Assurance Program Manual (QAPM) describes the Quality Assurance Program at HFC. The program is designed to provide administrative measures and procedures necessary for assuring that all HFC hardware and software products as well as any services meet or exceed customer requirements and applicable industry codes and standards. This Quality Program is designed to comply with ANSI/ASME NQA-1&1a-1994; *Quality Assurance Requirements for Nuclear Facilities*, (Basic Requirements) ANSI/ASME NQA-1a-1995 Addenda, 10 CFR 50

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

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

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

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

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

10.2 Safety Related Software Development

[

]

10.2.1 Software Development Life Cycle

[

]The following table lists the cross reference chart among the Software Verification & Validation Program (QPP 3.2 SVVP) and Product Development Plan (WI-ENG-011) and IEEE Std 1012.

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

Phase			Description
SVVP	Product Development Plan	IEEE Std 1012	
Project Planning	Project Planning	Concept	The period of the system life cycle during which project plans, schedules, and staff organization are initially developed.
Requirements	Requirement Specification	Requirements	The period of the system life cycle during which functional and nonfunctional performance capabilities are defined.
Design	Design	Design	The period during the system life cycle during which designs for architecture, software components, interfaces, and data are created.
Implementation	Production	Implementation	The period of the system life cycle during which hardware and software components are created from design documentation.
Component Integration	Production	Implementation	The period of the system life cycle during which hardware and software components are progressively combined into their operating environment and tested...
Acceptance Testing	Testing	Test	Formal testing conducted to determine if a system satisfies its acceptance criteria.
Post Installation Testing	Deployment	Installation and Checkout	Required testing to verify that no damage occurred during shipping and installation and that the system performs all required functions.
Operation and Maintenance		Operation and Maintenance	The period of the system life cycle during which the system is employed in its operational environment.

10.2.2 Life-Cycle Verification and Validation

This section defines the processes for new software development in accordance with HICB BTP-14 and IEEE Std 1228. The SVVP provides a detailed plan for each of the HFC-6000 system life-cycle phases. The following major topics apply to each phase of the life cycle.

- **V&V Tasks.** The V&V tasks constitute the activities of the V&V function throughout the hardware and software development life cycle. Depending on the particular life-cycle phase, these tasks may consist of generating plans, test procedures, and test cases or of using the previously generated plans and tests to evaluate particular components. The definition of V & V tasks are based on the tasks defined by IEEE Std 1012-1986 and Regulatory Guide 1.168 for safety system software.
- **Methods and Criteria.** These topics relate to the means by which particular components are evaluated and the basis for pass/fail judgments. General methods include inspections, direct operation of the component in a real or simulated environment, specific tests, technical reviews, design reviews, and component analyses. Specific methods and pass/fail criteria for individual components are provided by test plan(s) and test procedure(s) that apply to those components.
- **Inputs/Outputs.** The term 'inputs' refers to the source material required to perform a particular V&V task; the term 'outputs' refers to the specific product of that task. In general, the inputs for one phase are supplied by the outputs from the previous phase. Tables in the V&V reports supply listings of inputs and outputs required for the planned V&V tasks to be accomplished during each life-cycle phase.

The HFC V&V activities continue throughout the duration of product development project and nuclear system application project. For product development projects, V&V activities essentially end when the product is released for production. [

]

10.2.2.1 Project Planning Phase

The primary guiding document for product development projects is the Product Development Plan (WI-ENG-11); a Project Quality Plan (QPP 2.1) provides the corresponding function for application projects. However, both product development and application projects begin with the existing HFC product lines as the starting design basis. External requirements from a customer specification or from management strategic planning may provide the basis for a change to an existing component. The V&V tasks accomplished during this phase are as follows:

- **Proposal Generation** - This task includes the following:

Proposal engineer processes a customer's specification. The resulting output is a proposal based on existing product line components to the maximum extent possible. If necessary, HFC management generates a strategic plan for a new product line or product line component.

Task Inputs	Task Outputs
Customer Request for Quote	HFC Project Proposal
HFC Strategic Planning	Internal Product Development Proposal

- **Design Evaluation** - This task includes the following:
  - Determine if the project will require new product line development.
  - Identify constraints imposed by interfacing systems.
  - Evaluate allocation of functions to hardware and software.
  - Assess criticality of each major component to identify those that are safety-related.

Task Inputs	Task Outputs
• Existing HFC product designs • Performance characteristics • Customer specification • HFC Proposal • Product Development Proposal	Project Quality Plan (QPP 2.1) Project Development Plan (WI-ENG-011)

10.2.2.2 Requirement Phase

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

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

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

Task Inputs	Task Outputs
• Project Development Plan or Project Quality Plan • HFC V&V Program • Customer Specification • HFC Work Instructions • Qualification requirements defined by regulatory or industry standards	Requirements Specifications Document Reviews Traceability Analysis ACE List

10.2.2.3 Design Phase

During the design phase, component requirements are converted into the detailed design for individual components, for a product line, or for a specific control system composed of standard components. Before a hardware or software component design is released for implementation, that design must be reviewed for conformity with its requirement specification, traceability, completeness, accuracy, readability, and testability. Depending on the complexity of the component, the various V&V task to be accomplished during this phase may be accomplished as different aspects of a single review.

There are separate procedures for product development and application development.

10.2.2.3.1 Product Development Project

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

QPP 5.2, "Preparation of Procedures"
WI-ENG-001, "Design Verification and Reviews"

- WI-ENG-106, "Development of Hardware Design Specifications"
- WI-ENG-203, "Development of Software/Firmware Design Specification"

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

Task Inputs	Task Outputs
• Project Development Plan • Requirements Specification • Customer Specification • HFC Work Instructions • ACE List	Requirements Specifications Hardware Schematic Diagrams Traceability Analysis Design Review FMEA (if required) Qualification Test Plan (if required) Qualification Test Procedures (if required)

10.2.2.3.2 Application Development Project

During this phase of an application development project, plant specific functional requirements are used to develop the application software. The application software design is treated the same as the operating software developed as safety related software. All of the guidance and requirements used in its development are used for the application software. The applicable regulations and guidance are followed. Detailed guidance for activities during this phase is provided by the following:

- QPP 5.2, "Preparation of Procedures"
- WI-ENG-001, "Design Verification and Reviews"
- WI-ENG-802, "Application Engineering Design Process"
- WI-ENG-803, "Design Arrangement Drawings"
- WI-ENG-804, "Design Power Distribution"
- WI-ENG-805, "Define I/O"
- WI-ENG-806, "Design Control Logic Procedure"
- WI-ENG-807, "Design Graphics"
- WI-ENG-809, "Define Field Hardware,"

Task Inputs	Task Outputs
• Project Quality Plan • Requirements Specification • Customer Specification • HFC Work Instructions • ACE List (if required)	Design Arrangement Drawings Schematic Diagrams Component Design and Assembly Drawings Logic Diagrams User Interface Design Traceability Analysis Design Review FMEA (if required)

10.2.2.4 Implementation Phase

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

10.2.2.4.1 Product Development Project

Implementation for a product development project consists of: 1) Building the prototype based on the defined design for its hardware and software. 2) Testing the prototype both informally and formally to verify that the design functions as intended. 3) If new or additional qualification testing and or analyses are required, they typically will be accomplished during this phase.

Once all tests are satisfactorily completed for a particular product, it can be released for production, completing the development project for that product. Detailed coverage for activities during this phase is provided by the following:

- QPP 5.2, "Preparation of Procedures"
- WI-ENG-001, "Design Verification and Reviews"
- WI-ENG-004, "Release for Production"
- WI-ENG-815, "Red Line Procedure"
- WI-ENG-008, "Software Verification and Validation Test Procedure"

Task Inputs	Task Outputs
• Project Development Plan • Design Specification • HFC Work Instructions • Engineering Drawings • Prototype Validation Test • ACE List (if required)	Traceability Analysis Design Review Prototype Test Report CR for nonconformance Qualification Test Report(s) FMEA Report (if required)

10.2.2.4.2 Application Project

Implementation for an application project consists of building the hardware designs and coding the software/firmware for that design. HFC work instructions presuppose no new standard products will be created under an application product. (If a new standard product is required for a particular application, a separate product development project will be executed for that purpose.) Consequently, V&V oversight consists primarily of QC monitoring for activities on the shop floor. When an application includes application firmware, specific code-level qualification testing may be required. Detailed coverage for activities during this phase is provided by the following work instructions:

- QPP 5.2, "Preparation of Procedures"
- QPP 10.1, "Receipt, In-Process, and Final Inspections"
- WI-QA-003, "Crimp and Pull Test"
- WI-QA-009, "Certificate of Conformance"
- WI-ENG-815, "Red Line Procedure"
- Later, "Design Validation Test Procedure"
- WI-TST-002, "Performing Cabinet Power up Tests"
- WI-TST-003, "Performing Fuse Tests"
- Individual Component Test Procedures

Task Inputs	Task Outputs
• Project Quality Plan • Design Specification (if required) • Engineering Drawings • HFC Work Instructions • Engineering Drawings • Process Control Sheets	Traceability Analysis Test Reports CR for nonconformance FMEA Report (if required)

10.2.2.5 Integration and Testing Phase

This is the phase of an application project during which a complete control system is integrated together and tested as a unit. QC inspection of shop floor activities continues throughout this period, and generic integration/acceptance testing verifies system functional characteristics. If the system application program is included as part of the project, comprehensive validation testing of all application functions are included at this point. Implementation for an application project consists of building the hardware designs and coding the software/firmware for that design. Specific contract requirements for system-level testing and documentation will be addressed at this point. Detailed coverage for activities during this phase is provided by the following work instructions:

- QPP 5.2, "Preparation of Procedures"
- QPP 10.1, "Receipt, In-Process, and Final Inspections"
- WI-ENG-815, "Red Line Procedure"
- WI-ENG-810, "Control System Application Test"
- Later, "System Acceptance Test Procedure"
- Project-Specific Test Procedures

Task Inputs	Task Outputs
• Project Quality Plan • HFC Work Instructions • Engineering Drawings • Process Control Sheets • System Acceptance Test Procedure • Test Procedures	Traceability Analysis Test Reports CR for nonconformance

10.2.2.6 Deployment

After completion of acceptance testing, the product (individual hardware or software components or a completely integrated control system) is shipped for onsite installation. When HFC is supplying equipment to a separate OEM, HFC obligations during this phase may be limited to delivery of equipment documentation. When HFC is the OEM for the final project, detailed requirements are defined by the customer's PO but generally include field support for installation and onsite testing.

Task Inputs	Task Outputs
• Project Quality Plan • Customer PO • Engineering Drawings • Project-Specific Test Procedure	System and Component Documentation Installation Test Report (if required)

10.2.2.7 Operation and Maintenance

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

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

10.2.3 V&V REPORTING

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

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

10.2.3.1 V&V Task Report

V&V tasks include reviews, tests, and analyses covering the product under development. Each review and each formal test includes a report form that provides a mechanism for recording results and any discrepancies. Both review documents and test result forms are designated as QA records and will be retained by Document Control. In addition, the person conducting a review meeting or performing a test will write a report covering that activity. This V&V task report will be supplied to the V&V Team Leader and will provide the basis for generating the System V&V Report, if required. HFC has assured that the V&V responsibility is independent. The organization members that have this responsibility are personnel that are not part of the design team and report to a different supervisor than members of the design team.

10.2.3.2 V&V Analysis Report

A separate report is generated to cover each analysis conducted during the course of a project. Such analyses may cover any combination of the following:

- Successful completion of each phase of the software lifecycle
- Failure Modes and Effects
- Abnormal Conditions and Effects
- System Availability
- Qualification Test Results
- Final Validation Report

Any condition or finding that is adverse to quality or safety is reported in a CR.

10.2.3.3 System V&V Report

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

10.2.3.4 Condition Reports

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

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

10.2.3.5 Final V&V Report

When a project requires formal V&V reporting as a deliverable item, the final V&V Report shall constitute the final submittal of the SVVR. The content of this report shall cover the following:

- Summarize all V&V activities performed
- Summarize task results for each life cycle phase
- Summarize CRs issued during the project and indicate how they were resolved
- Assess overall system quality and reliability

Appendix –

HF Controls Corporation

HFC-6000 Product Line

Document Map

PP901-000-02

Rev A

Author/Title _____Angela Han_____

Reviewer/Title _____Terry Gerardis_____

Approval/Title _____Allen Hsu_____

HFC Proprietary

Revision History

Table of Contents

1 Purpose and Scope

This document defines the required documentation for the HFC-6000 product line and the documentation layer that is used. This document also provides guidance on how to go through HFC-6000 product line documentation.

The documents mentioned in this document include documentation specific to HFC-6000 product line as well as documentation for standard products or software modules, which are referred as components.

2 Conventions

[

]

Figure 1 - HFC-6000 Documentation Layers

Appendix A. List of Documents for HFC-6000 Product Line

