AUDIT REPORT FOR THE AUDIT OF THE HFC-6000 PLATFORM
AT DOOSAN HF CONTROLS ON OCTOBER 6-9, 2009

Background

By letter dated March 5, 2008 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML080780169), as supplemented by letters dated November 15, 2007 (ADAM Accession No. ML073390048), and January 16, 2009 (ADAMS Accession No. ML090710918), Doosan HF Controls Corporation (HFC) requested approval by the U.S. Nuclear Regulatory Commission (NRC) for the "HFC-6000 Safety System Topical Report," document number PP901-000-01, Rev. C (ADAMS Accession No. ML080780170). The supplemental documents provided under the November 2007 and January 2009 cover letters, provided additional information that clarified the application and did not expand the scope of the application.

The audit was conducted in accordance with the audit plan, which was provided to HFC prior to the audit, and is included in Enclosure 2.

HFC Audit

NRC staff (Norbert Carte and Jonathan Rowley) and the supporting contractor (Richard Wood of Oak Ridge National Laboratory) visited the HFC facility in Carrolton, Texas, from October 6 through October 9, 2009, to perform a regulatory audit. The purpose of the audit was to obtain clarification of design details of the HFC-6000 platform and observe demonstration of the associated processes and procedures employed to ensure its quality.

During the course of the site visit, the audit team engaged in clarifying technical discussions with HFC staff and conducted thread audits. In addition, the HFC-6000 Test Specimen for the HFC Nuclear Qualification Project ERD-111 served to illustrate the hardware components and configuration of a sample HFC-6000 system and to demonstrate the functional capabilities of the platform.

The following major topics were discussed and included thread audits of pertinent documents to assess claims made by HFC in the submitted Topical Report (TR):

1. Scope of the HFC-6000 platform (i.e., what hardware and software modules are included in base platform): Audit Plan Item Nos. 2 and 14
2. Means of identifying a module or system in the configuration management system and in the field: Audit Plan Item Nos. 2, 3, 6, 9 and 14
3. Origin (i.e., supplier or manufacturer) of HFC-6000 modules: Audit Plan Item Nos. 11 and 14
4. Demonstration of operational performance and fault tolerance characteristics: Audit Plan Item Nos. 4, 5, 6, 7, 8 and 10
5. Software quality assurance: Audit Plan Item Nos. 1, 11, 12, 13, 15
6. Software installation: Audit Plan Item Nos. 9 and 14
7. Cyber security: Audit Plan Item Nos. 9 and 11
8. Qualification testing: Audit Plan Item Nos. 10 and 15
9. Failure modes and effects: Audit Plan Item Nos. 4, 5, 6 and 7

The thread audits gave demonstration of the implementation of HFC quality assurance procedures and provided information to support the evaluation of HFC claims based on sampled traces through the docketed and on-site HFC documentation. Anomalies that were found include:

1. Ambiguous references (e.g., revision identification is not always included in references to HFC documentation and test records that are annotated hard copies of test procedures do not have unique identification),
2. Incomplete reconstituted software requirements developed for the commercial grade dedication of pre-developed software,
3. Omission or erroneous execution of procedural steps for qualification testing,
4. Inconsistencies among multiple layers of documentation for qualification test findings, and
5. Unsupported or ambiguous claims regarding conformance to requirements given in EPRI TR-107330.

HFC is addressing these anomalies through their corrective action processes.

Discussion Summary

Platform Scope - Previous requests for additional information (RAIs #9 and #10, ADAMS Accession No. ML052850063) had requested identification of the modules and components that are within the scope of the HFC-6000 platform under review; however, the response to the RAIs, the list of components in the TR, and comparable lists and descriptions in various supplemental documents are inconsistent. For example, several qualification reports indicate that certain items are outside the scope of the qualification system (i.e., the C-Link and ECS-B232). Additionally, no identification information has been provided for certain components (e.g., power supply modules, 19-inch card rack, and power supply rack). Discussions with HFC clarified that the statements excluding the C-Link from the scope of the qualification testing referred to the network itself and did not apply to the processor and communication components incorporated on a SBC06 controller card or to the C-Link functionality provided by the controller. It was also stated during these discussions that the ECS-B232 should not be considered within the platform scope.

The audit team asked HFC to make available a comprehensive list of modules and components that are within the scope of the base platform covered by the TR. Specifically, HFC was asked to provide the necessary identification (such as model, part, and version numbers) to definitively establish what specific hardware and software elements are covered under the requested review. The Master Configuration List of the HFC-6000 system for the ERD-111 Qualification Project is an Excel spreadsheet so a summary printout was generated by HFC. This listing provided part numbers, revision letters, serial numbers, board types, and software part numbers for the components of the HFC-6000 Test Specimen. However, the list included items that were stated to be outside the scope of the platform (e.g., ECS-B232) and provided only part numbers for the racks and power supply modules. An updated listing of modules and components that are addressed by the topical report, with necessary identification, must be docketed.

The ongoing technical review has found that platform component identification is inconsistent among docketed materials. For example, Table 3.1 of DD0401, Rev. A, has a “Q” appended to

the name of several modules. HFC initiated a condition report (CR) to address this discrepancy (CR No. 2009-0537).

Discussion of the four on-board complex programmable logic devices (CPLDs) also addressed the current controller configuration, in which the CPLD logic has been implemented on a single field programmable gate array (FPGA). Presently, the scope of the base platform (being reviewed by the NRC) does not include the controller module using the FPGA.[1] The FPGA based version was developed after the qualification testing (referenced in the topical report) was performed. HFC stated that it treats FPGAs as software and that the FPGAs are developed in accordance with the same plans and procedures used for platform software development. Since the scope of the topical report did not include FPGAs, the review had not considered the applicability of the plans and procedures to FPGA development. The NRC considers all programmable devices (e.g., CPLDs & FPGAs) to be software and that the development plans and procedures should be reviewed in accordance with the same criteria as is used for all other software development.

Means of Identification – The Bill of Material (BOM) for a project (such as ERD-111 Qualification Project for the HFC-6000) contains identifying information on the hardware and software components of a system. The hardware modules are identified by a module type and part number. The firmware is identified on the BOM by a part number and checksum. The software part number refers to a version number that represents a class (i.e., project grouping) with dedicated versions of each software module. The collection of generation-specific software modules that is included in a software version is maintained in a reference folder in the SourceSafe repository.

Physical identification on a module printed circuit board (PCB) is provided by stickers that are attached during assembly and configuration. A bar code sticker on a card contains the serial number for the specific item, the part number for the module, and the build (i.e., manufacture) date. An additional sticker identifies the module revision by noting the letter assigned to that particular revision. Stickers on the on-board CPLDs and flash memory chips provide software part numbers for CPLD logic and processor firmware, respectively. These firmware items are not intended to be modifiable in the field and must be revised using the development tools maintained at HFC. HFC provides only one version of the software to a module supplier to ensure configuration control. The NRC will request additional information in order to review system and software security aspects of this physical identification convention.

Software identification can only be checked using the development tools maintained by HFC. Direct queries are not supported while a controller is in normal operation mode based on configuration settings (e.g., switches and jumper settings). These memory query capabilities are only intended for use with the module out of service in a separate offline controller bay (e.g., a test and maintenance cabinet). Software identification for firmware consists of a header that identifies the firmware type (i.e., SC, SAP, SEP) and compile date. This identification information can be read using development environment tools included with the HFC Engineering Workstation. An internal checksum is provided in the first byte of the code. However, no direct indication of the software part number is provided in the query display. Cross-checks with the stickers on the card and the BOM are a means for obtaining that

[1] The evaluation report will clearly state that the newer FPGA based version is not included in the scope of the TR and evaluation report.

information. For application software, offline queries yield the date of compilation, loop identification, revision letter, drawing number and revision, and date of drawing revision. Tools on the development workstation permit comparison of the installed software against reference software with identifiers that include the filename, compile data and time, software version, checksum, file size, input/output (I/O) scan table version, and dynamic database request table version.

The audit team performed a trace of identification information through the HFC documentation for a sampled controller module. Starting with the BOM and Receiving reports, information on the module and its software could be traced to find the associated source code. No anomalies were found.

Source of HFC-6000 Modules - HFC-6000 cards are supplied by multiple vendors. Each supplier has been assessed and authorized by HFC based on review of quality assurance processes and demonstrated performance. To fulfill an order, a supplier procures approved parts, assembles and configures the PCBs, and installs the software provided to them by HFC as part of the procurement package. HFC inspects all incoming modules and documents its findings in a Receiving report. The HFC inspection includes a check of the various means of identification described previously. However, HFC did not describe any direct verification that the correct software has been loaded as an action during the inspection process. RAIs will be needed to determine how HFC ensures that the software is not intentionally or unintentionally modified or miss-installed by the PCB vendor(s), consistent with the provisions of Regulatory Guide (RG) 1.152 (Rev 2), Regulatory Position 2.4.2, which addresses tampering with the developed system.

Every module is functionally tested by HFC. Failed modules are returned to the supplier for replacement. Aside from the confirmation of correctness provided by the functional tests, HFC does not review the version of software installed on a module. HFC relies on administrative controls to ensure the correct software version is used for a particular purchase order. Specifically, HFC provides unique software package with each order for installation by the supplier.

HFC has established an approved parts list based on an evaluation of their equivalence. Of the more than seventy items on the Bill of Material for the HFC-6000 Test Specimen assembled for the ERD-111 Qualification Project, approximately thirty parts have multiple suppliers. HFC has established a Parts Interchangeability Evaluation (PIE) procedure (WI-ENG-007, Rev. A) to guide the evaluation of the alternate parts. Attachment 7.1 of this procedure provides an evaluation checklist. In a sample of the interchangeability evaluation (PIE 375, 7/27/09) that was provided for review, it was found that an additional page was included with the PIE checklist. This addendum to the PIE checklist provided a form for assessing the impact of the alternate part on the environmental withstand capability of the assembled module. The supplemental page is not currently included in the evaluation procedure. The audit team and HFC discussed the potential consequences of interchangeable parts in terms of the representative nature of a test type used for qualification. The audit team will determine whether specific guidance on this matter is available. The audit team selected a specific supplier as a sample for review of the HFC approval process. HFC provided the documentation that affirms the approval of the selected supplier to provide assembled printed circuit boards for the HFC-6000 platform. No specific statements regarding the provision of an Appendix B compliant quality assurance program by the supplier were identified.

Operational Performance and Fault Tolerance - HFC demonstrated the performance of the HFC-6000 using the configured Test Specimen. Specifically, HFC illustrated the analog time response of the system, demonstrated the operation of redundant controllers, showed the manual initiation of the maintenance failover capability (i.e., transfer primary control from one controller to the redundant controller), and injected several faults to demonstrate the diagnostic capabilities and fault tolerance characteristics of the platform. Communication interruption and processor failure were simulated to show the failure detection capabilities based on software (i.e., "mailboxes") and hardware watchdog timers. Additionally, fault tolerance of the redundant power supply modules was demonstrated by pulling one module while in service.

In addition to successfully demonstrating the fault tolerance provided by the redundant controller and communication link configuration, HFC showed the means for indicating failed conditions. Operational and faulted conditions drive circuits which illuminate local light-emitting diodes (LEDs). These LEDs give local status indication on the bezel faceplate that can be used by maintenance staff at a plant to determine the status of the controllers. Certain LEDs indicate specific fault conditions based on display of hex code. The dynamic database that is broadcast by each controller node on the C-Link network can be configured to provide status flags to support annunciation/alarm of failures or degradation to the operations staff at a plant. This capability was demonstrated through the test system interface connected to the Test Specimen. Each faulted condition that was injected into the Test Specimen was annunciated on the test display.

HFC pointed out that a controller module will not self recover. Essentially when a faulted or failed condition is detected through self-test or watchdog timeouts, a failover will occur and the controller will halt. The failed controller must be manually reset or replaced. The recommended remediation for failed controllers is replacement. Per terms of their contracts for fielded systems, all failed modules are returned to HFC for evaluation and replacement/repair. HFC maintains a database of all failures. Additional information from HFC regarding their failure history may be useful to help support the conclusion that the operating platform software does not contain intentional or unintentional defects or undesired code per the provisions of RG 1.152 (Rev 2), Regulatory Positions 2.2.2, 2.3.2 and 2.4.2. Calibration of I/O modules occurs at the factory and is an offline activity.

Software Quality Assurance - Discussion of software quality assurance (QA) dealt with commercial dedication of pre-developed software (PDS) and the maintenance of PDS using the HFC change control and configuration management processes under the Quality Assurance Management Plan.

HFC plans and procedures such as QPP 3.1, WI-ENG-003, WI-ENG-812, and WI-ENG-830 were used during a thread audit of a specific software component. It was found that an element of the procedures (specifically in Section 5.3.5 of WI-ENG-830, Rev. B, concerning identification of the location of the software under review or change) was not followed in the documentation on the software module. HFC initiated a CR about the issue (CR No. 2009-0538).

A thread audit tracing the documentation for a software module was conducted on a sampled function block module. The item selected was the XX4QRTO.A10; 4. The thread traced back from the code inspection report to the source code file to the design specification. No requirements for this block were found. A forward trace from the source code inspection report to the test plan and test report was also conducted. It was found that the test summary was

inconsistent with the test record (i.e., annotated test plan), which reported that the block was not working for two of the three test cases. HFC stated that a subsequent, undocumented test during the commercial-grade dedication (CGD) code inspection and testing did not show any anomalies and the failed test cases appeared to be the result of an incorrect test setup. These anomalies challenge the reported findings for the CGD activity in which the software requirements specification was claimed to have been reconstituted for all of the PDS. Additionally, the discrepancy between test summaries and test records require further investigation to more fully assess the adherence of HFC to QA procedures. Since the justification for the quality of PDS depends on the evidence generated through the CGD process, the re-engineered software requirements must address function blocks (i.e., the CQ4 software modules) and other system functions. HFC stated that it will document the requirements for all elements of the PDS. The NRC will request that the completed documentation be docketed.

An additional thread audit was conducted to trace a selected EPRI TR-107300 requirement through the documentation for a Test Specimen Application Program (TSAP). A specific requirement regarding the configuration of the Test Specimen and its representative application code was selected from the Electric Power Research Institute (EPRI) TR-107330 Requirements Compliance Traceability Matrix (RR901-000-10, Rev. A). Using the references in the Requirements Compliance Traceability Matrix, the requirement was traced through the TSAP requirements document (700901-09, Rev A) to the corresponding TSAP design description (ADS0401, Rev. A). Next, the corresponding test setup procedure and test execution procedure/record (TP0408, Rev. A, annotated for pre-qualification test execution on 2/17/04 and TP0402, Rev. E, annotated for seismic retest on 9/22/04 and 9/24/04) were found. No anomalies were found using the document references included in the Requirements Compliance Traceability Matrix. As in other cases, no unique documented identification for test records is provided other than hand-written notes on the scanned hard copy of the test procedure.

A third thread audit was conducted to perform a forward trace of a system firmware requirement using the Traceability Matrix (RR901-000-31, Rev. B). The thread began with a selected requirement regarding write enable/disable functionality for the system processor firmware (i.e., SC firmware). Next, the description of the requirement was found in the Requirement Specification (RS901-000-37). As indicated in the Traceability Matrix, the corresponding design description was found in the Module Specification (MS901-000-01) and Design Specification (DS901-000-01) for the SBC06 controller module. The source code (912038-11 PROM code) and source code review documents (SR001-000-001 through SR001-000-012 and SR001-000-056 through SR001-000-086) were made available and the specific code (WR_ENCHK) was found. This code is called by several software modules. No anomalies were found.

Since the on-going technical review of TR addresses the software quality program to manage PDS software, HFC was asked about the relationship of their software QA processes and procedures to the life cycle processes described in NUREG-0800, Chapter 7, Branch Technical Position (BTP) 7-14. HFC stated that it would generate a mapping of their QA documents to the plans and products described in BTP 7-14. HFC also indicated it would document any deviations from BTP 7-14 in their QA processes and procedures for managing PDS software changes. The docketing of the information regarding the QA mapping to BTP 7-14 guidance would assist the review process.

Software Installation - The development environment for system firmware was demonstrated by HFC. Code management is implemented using Microsoft SourceSafe. Access to the system source code repository is through networked engineering workstations. System software is collected in a local folder for development to support a project. The development software must go through the formal review and approval processes before being released for production and included in the repository as a new software class. HFC developers use Microsoft Visual Studio for editing the assembly language source code. The Intel x86 Assembler, Linker and Locator tools are used to generate binary versions of the source code for implementation. After a class of system software has been released for a project, the system firmware is burned onto a PROM using a dedicated fixture The PROM can then be installed in the PCB for a controller module. A similar development process is used for CPLD logic. Using a testing and configuration management assembly connected to a development workstation, CPLD logic is downloaded into each on-board chip. These implementation capabilities are maintained at the HFC facility and are not provided to utility customers.

Maintenance of system software adheres to the software quality assurance program and follows the configuration management procedures. A System Change Request (SCR) documents changes, including software modification. Each software revision change is associated with a SCR number. The BOM shows progression through revisions by identifying the applicable SCRs documenting the software change history. CPLD changes are denoted by incrementing its part numbering.

The application software development environment was also demonstrated. Application software is represented as control algorithm drawings using AutoCAD software. HFC One-Step macros in the Promis-e software environment extract design information from the drawings. One-Step software compiles the data into binary code for installation in the controller module. It was noted that verification of generated code is based on manual point-by-point comparison of source code against logic diagrams. A development and configuration management assembly (e.g., the equivalent to a hot spare cabinet bay connected to a HFC Engineering Workstation) is used for offline troubleshooting and reprogramming of application software. System configuration for field installation and administrative controls are intended to prevent software downloads to a controller module while it is installed in the field cabinets and in service.

The demonstration of software installation included a discussion of controller modes of operation. HFC stated that software is developed, installed, and updated off line. Essentially, the system firmware is developed by the HFC Engineering Department and installed on the controller module by the supplier prior to assembly of an application system. The application software is developed in a similar manner and downloaded to the dedicated flash memory for the controller prior to system delivery. Field modifications are accomplished with the module removed from service and installed in a maintenance and testing assembly. Thus, for software installation and maintenance, offline means a module is out of service and removed from the field cabinets while online means a module is installed in the field cabinets and in service. The supporting documents that have been docketed identify four modes of operation – Normal, Simulation, Test, and Offline. Dual in-line package (DIP) switches can be configured for an Offline mode in which the system software runs normally, but the equation interpreter task does not run. The Normal or Run mode is the operating mode in which execution of the application software will begin after operating system initialization. In the Test mode, the controller performs different tests based on a request code set up by the DIP switches. The Simulation mode supports simulation of the operation of controller with I/O point changes without the

presence of real field devices. It appears that each mode can be invoked while the module is installed in the field cabinets. Administrative controls would need to be applied to ensure that controller modules are not configured for offline, test, or simulation modes while the module is in service.

Security - The audit team and HFC discussed provisions that contribute to security for the HFC-6000 in the field and for the computer's development and configuration management systems at the HFC facility. The HFC-6000 provides protection against reprogramming/download of application software while it is installed in its cabinets and online for operation. These provisions include a local write protect switch to disable software download to the application flash memory of its controller modules, diagnostics to detect and flag a change in the write protect switch (i.e., indication when downloads are enabled), manual jumper settings to disable write capability to system firmware flash memory, and an one-way communication gateway on the C-Link network (which is not part of platform under review) to prevent access to a HFC-6000 node from non-safety systems. A thread audit of the security features will be performed on the subsequent audit.

An additional measure that is provided occurs during initialization equalization of the redundant controller memories in which the application code in flash memory for the secondary controller is compared with and replaced by the application code in effect for the primary controller. This mechanism ensures that an altered application cannot replace an online application when a controller is returned to service following manual reset or replacement. Finally, flash memory for system firmware can be compared against an installed PROM during startup/reset initialization based on configuration selections.

Security protection in place for software development environments include network firewall protection, server and workstation anti-virus protection, password-based access control, administrative restrictions on write permissions, and control of source code versions and protection of record versions in the SourceSafe repository. The ability to embed an access backdoor or malicious code in system or application software would require not only access but also expert knowledge of the programming conventions and tools to avoid immediate detection through erratic behavior or design measures (e.g., comparison of code against checksums during initialization, failed execution of undefined or erroneous code, or rejection of communication messages based on format nonconformance). In-house measures at the HFC facility to ensure the fidelity of software include manual code reviews and version control measures in SourceSafe. The observed platform capabilities and control of the development environment are intended to address RG 1.152 Revision 2, Regulatory Position 2 for the HFC-6000 software. These aspects will be addressed in an RAI regarding the security features. Further consideration of whether unwanted or undocumented functions may be present is warranted in the evaluation of dedication evidence for PDS. Application specific reviews of security can address system-level security considerations (e.g., confirmation of only one-way communications with external systems across the C-Link or administrative controls on platform configuration to ensure that software download capability is disabled)[2].

Based on what was shown at the audit, the HFC-6000 platform has capabilities and provisions to contribute to security. Much of the RG 1.152 regulatory positions relate to architectures, systems and applications. The provisions for security (write protect switches, jumper settings,

[2] The one-way communication gateway is not within the scope of the TR.

comparison of code, etc) and the described development process and its protection support compliance with the regulatory positions of RG 1.152. However, what nodes are connected to the C-link, the use of an one-way gateway, administrative controls on allowing configuration for software downloads, etc. are application specific items that were not considered during the audit.

Qualification - The documentation of qualification testing was reviewed and the degree to which the evidence that is reported supports the HFC claims about complying with the EPRI TR-107330 qualification requirements was discussed. During the ongoing technical review of the TR, questions have arisen about the characterization of compliance with EPRI TR-107330 given differences between what is required by the EPRI guide and what was achieved by HFC regarding the stress condition envelope and demonstrated performance characteristics of test specimen. Multiple levels of documentation capture the qualification results. These levels of documentation include the overview of the qualification program in the TR, the summary reports for each test phase, the detailed test result reports that are provided as appendices to the test summary reports, and the annotated test plans that are effectively the official test records. Instances of inconsistencies among these documents and examples of deviations from the performance and environmental stress requirements of EPRI TR-107330 were discussed with HFC. To resolve the issues that were discussed during the site visit, HFC stated that it will generate summary information clarifying the environmental compatibility and performance envelopes that are demonstrated by the HFC-6000 qualification tests. In addition, HFC plans to clarify its claims of compliance with EPRI TR-107330 by clearly identifying deviations and providing associated justification. This summary information on the HFC-6000 qualification program and compliance with EPRI TR-107330 qualification and performance requirements should be docketed.

During the discussion of qualification testing, the audit team noted that review of the test procedures and test records had identified instances in which procedural steps do not appear to have been conducted as written. Two specific instances were discussed. First, analog modules (HFC-AI16F) being out of calibration were cited as the reason the HFC-6000 did not satisfy the EPRI TR-107330 requirements for the Analog Accuracy tests. These tests are part of the Operability tests used to establish baseline performance. However, the HFC procedures for test setup (e.g., TP0401, Rev. A) specify verifying that each module has been “tested, calibrated, and/or configured” so this condition should have been detected at the start of testing. Second, a configuration deficiency of the tester system caused performance data records (i.e., the Sequence of Event (SOE) data files) to be overwritten. The test procedure for each test phase contains a step in which the SOE and Historical Archive System (HAS) data files for pre-tests should be stored and used to verify that pre-test conditions remain consistent with the performance baseline. Clearly, this step was not fully accomplished during testing since the tester bug was not discovered until deep into the qualification testing. Another issue that was highlighted during these discussions involves the absence of unique document identification. Test records are hard copies of annotated test plans with no unique identification to differentiate between test record and test plan (e.g., the February 9, 2004, integration test record is hand-written notes on copy of TP0401 Rev A). These quality assurance issues are under review by HFC.

Another point of discussion regarding the execution of the HFC-6000 qualification testing was that a limited number of tests and analyses indicated by the EPRI guide were either not conducted or not documented as part of the qualification program for the HFC-6000 platform.

Specifically, the RS101 electromagnetic susceptibility test, the Failure to Scan test within the Operability test sequence, and a radiation withstand analysis were identified. To address the inadequate documentation issues identified, HFC will review the HFC-6000 qualification documentation as it develops a new qualification summary, generate CRs as appropriate, and then resolve the ambiguities or deficiencies in accordance with their established procedures.

As previously noted, the HFC-6000 qualification reports exclude the C-Link from the scope of the testing while the TR describes successful testing of the C-Link communication function. HFC stated that the statements in the supporting documents refer to the network itself, which was not tested in a multi-node configuration under stress. HFC affirmed that the test data confirming the functionality of the C-Link processor and communication capability of the controller modules was recorded and retained. HFC showed that previous versions of the test summaries included discussions of the C-Link performance under environmental stress. As an example, the initial version (TS901-000-34, Rev. A) of the summary for in-house testing that was conducted prior to shipment for a seismic retest contained the C-Link results whereas those results were not included in the revised version (TS901-000-34, Rev. B) of the report. HFC stated that it would include these results in the qualification summary they plan to generate.

To confirm that the necessary test data are available to support conclusions about the qualification of the C-Link components and functionality, a specific communication test from the test plan (i.e., Serial Communication Operability) was selected to trace the available data for C-Link performance. For the pre-seismic Operability test, the data was traced to the automatic HAS and did show that the C-Link communication operated without error. No anomalies were found in this thread.

Failure Modes and Effects – The failure modes and effects analysis (FMEA) was performed on a single channel as described in the HFC-6000 topical report. This analysis was not performed to demonstrate that a single channel is single failure proof, but rather to identify potential failure mode of a single channel and associated mitigation measures.

Bus arbitration for shared memory and the Dual-Ported Memory (DPM) module is provided by on-board CPLDs (specifically, the SHARB CPLD). Shared memory is provided within the HFC-6000 controller module to enable information exchange among the three on-board processors (the main controller or system processor (SYS) and two subordinate communication processors, the C-Link and ICL processors). The DPM module provides shared memory and failover management for two redundant controller modules to enable primary and secondary (i.e., hot standby) controllers to coordinate status, maintain current data equivalence, and transfer (i.e., failover) primary control in the presence of a failed state or manual demand. During the audit, the HFC analysis of the effects of a bus arbitration failure was discussed (as described in the FMEA Report, RR901-000-01). A random failure of the CPLD was identified as the possible cause of bus access failure. Other possible but less likely causes that were noted in the discussion are power bus burnout, inactive or frozen memory locations, or loss of clock. The subsequent effect of bus arbitration failure was identified as a loss of sanity[3] for the controller due to timeout of the software watchdog timer (loss of memory access prevents maintenance of the “mailbox” for a processor so a timeout would occur). The presupposed mechanisms for the failure involve a high/low latchup of an input or output address line or an inactive logic transition

[3] HFC characterizes the operability (e.g., powered, online operable status) of a controller using the term “sanity.” “Sane” is roughly equivalent to “operable.”

cell. Further assessment identified no credible mechanisms for this failure mode to initiate a cascade of effects that could result in an undetected failure of function. The discussion of the HFC analysis indicated a thorough assessment of the selected failure mode and consequential effects.

A further discussion of the bus arbitration functionality that is provided by the CPLDs addressed arbitration of access to memory resident on the DPM module. Each controller manages access by its processor to the DPM. The memory on the DPM provides two ports so that each of the redundant controller modules can simultaneously access the memory. The only conflict management occurs if the controllers request access to the same memory location. The first controller request is serviced and the second controller receives a "busy" indication. If the first controller stalls, the memory will be released and its faulted state is indicated through the "Sanity" circuit.

For shared memory (on the controller module), the SYS is assigned higher priority for arbitrating bus requests. The subordinate processors (C-Link and ICL) have equal priority.

It is important to recognize that the communication addressed in the HFC-6000 TR is communication within a single channel; therefore, DI&C-ISG-04 is not applied as regulatory guidance in this context.

The ongoing technical review of the TR found that comments included in the EPRI TR-107330 Requirements Compliance Traceability Matrix (RR901-000-10, Rev A) are inconsistent with the content of the Failure Modes and Effects Analysis (RR901-000-01, Rev. B). Specifically, the Requirements Compliance Traceability Matrix identifies a runtime bit failure in memory as a failure condition that might not be detectable or produce an alarm indication. Further, it is stated that a software modification to add a runtime memory test was recommended in the FMEA. However, the TR states that there are no identifiable undetectable failures and the FMEA does not suggest any software change to address runtime bit failures. HFC responded that Revision A of the FMEA had included software failures as separate from system failures and the analysis had determined that no diagnostic functions were provided to directly detect runtime bit errors. Subsequent analysis focused on errors at the system level to adhere to industry practice and, consequently, Revision B of the FMEA document does not contain the suggested software modification. However, the Requirements Compliance Traceability Matrix was not updated to reflect the revised analysis. A condition report to correct this and related discrepancies was generated (CR No. 2009-0540). During the audit, HFC identified a separate analysis that addresses the issue with the runtime memory failures by showing they are indirectly addressed. This analysis will be discussed further with HFC.

A discussion of the Reliability and Availability report included questions about the reliability impact of continued operation after failure of a redundant capability (e.g., controller, communication link). HFC noted that the recommended remediation for alarms and failure indication is replacement of the affected module or component. However, it was observed that operation in a degraded mode (e.g., single controller performing the function with no failover capability or single I/O port functioning for an I/O module) is possible. Since replacement of one controller is possible while the other redundant controller continues to perform the function, the capability for timely remediation is provided. The failure of a non-redundant I/O module would affect execution of the function that is dependent on that data.

Thread Audit Summaries

1) Trace module identification information through HFC documents – Starting with the BOM and Receiving reports for HFC-6000 Test Specimen, the serial number for a specific controller (SBC06 S/N 37030155) was selected. Subsequently, the part number (40041701) and revision identification (B) were found. Also, the corresponding software part number led to the Source Code List (SC100003, 2/14/04). No anomalies were found.

2) Trace documentation of a software module – A specific software component (RTO block) was identified from the source code review report (SR001-000-50) based on the software part number identified from the BOM and Receiving reports for the HFC-6000 Test Specimen. To perform a backward trace to the corresponding requirements, the source code file (XX4QRTO.A10; 4) was located and then the description of the block was found in the Design Specification (DS001-000-03, App. 27 no rev ID). No requirements were found in any Requirements Specification document and, following this discovery, HFC stated it will generate the missing requirements for function blocks to fulfill its CGD activities for the HFC-6000 PDS (CR No. 2009-0539). Subsequently, a forward trace to the test results that verify the performance of the block was conducted. The RTO block was traced to the corresponding test plan (ATP0402, Rev. A). Next, the test report (TR001-000-02) was made available along with the test record (an annotated hard copy of the test procedure). It was found that the test record stated that the module passed for one test case (ratio calculation) but the module was "not working" for the other test cases. This unexpected test behavior not reported in higher level summaries (i.e., no anomaly was reported in test summary report for the test cases and there was no discussion of field test cases for execution of 2 of 3 tests). Anomalies from this thread are 1) document reference uncertainties since the annotated test plans are not uniquely identified and the references to various documents do not provide revision identification, 2) the absence of PDS requirements for function blocks, and 3) inconsistencies among test records and test summary reports. Further assessment of the HFC corrective actions in response to these anomalies will be performed through RAIs.

3) Trace documentation for a TSAP configuration requirement from EPRI TR-107330 – A specific requirement regarding the configuration of the Test Specimen and its representative application code was selected from the EPRI TR-107330 Requirements Traceability Matrix (RR901-000-10, Rev. A). This requirement addressed the configuration of an algorithm and test setup to support automatic response time testing. First, the corresponding requirement for HFC-6000 TSAP (700901-09, Rev A) was identified along with the corresponding TSAP design description (ADS0401, Rev. A). Next, the corresponding test that verifies the requirement is met (TP0402, Rev. E, annotated for seismic retest on 9/22/04 and 9/24/04) was found. Finally, the test setup that verifies correct configuration (TP0408, Rev. A, annotated for pre-qualification test execution on 2/17/04) was located. No anomalies were found using the document references included in the Requirements Compliance Traceability Matrix. However, as in other cases, there is no unique documented identification for test records other than hand-written notes on the scanned hard copy of the test procedure. This condition suggests the potential for errors in document management through ambiguous references.

Note: The absence of unique identification of test records introduced some challenges in specifying which documents were needed to conduct this thread audit. This condition makes it complicated to cite the test records and makes the trace of information through the document

system more difficult since the records are not uniquely identified. However, HFC was able to retrieve the documents when requested (except that they initially retrieved the test data for the Operability tests prior to the first seismic testing rather than the requested test data for the in-house operability tests prior to the seismic retests). If the test records were uniquely identified, then perhaps they would have gotten the right data.

5) Trace documentation for system controller firmware requirement – A requirement on a write enable switch for software downloads was randomly selected from the Traceability Matrix (RR901-000-31, Rev. B). The selected requirement is listed in RS901-000-37, Rev. A, Section 4.1.1 as requirement 12 for the SC firmware. For this requirement, the Traceability Matrix shows MS901-000-01, Rev. C, Sections 3.1 and 4.1 and DS901-000-01, Rev. B, Section 2.4.1.1 as design phase references, 912038-11 PROM code as the source code reference, SR001-000-001 through SR001-000-012 and SR001-000-056 through SR001-000-086 as the source code review references, and TS901-000-02 Sections 5.8 and 5.11 as the prototype test references. The requirement was traced through the design phase documents, source code, and source code review (specifically, SR001-000-014, Rev. 11 for the Equation Interpreter module BC_CRCHA.A10). The sampled code is contained in the software element WR_ENCHK, which implements a write enable check and stops the Equation Interpreter if the switch is set to enable writing. This code is called by several software modules. No anomalies were found.

6) Trace of test records and supporting data for qualification testing – A specific test was selected from the qualification test plan to confirm that data on the performance of the C-Link communication function under stress was available and to assess the traceability of test records. The Serial Communication Operability test from the collection of Operability tests was chosen. The specific example was the execution of this test as part of the pre-test baseline assessment for the seismic testing phase (TP0405, Rev. C). The data points that were logged in a file by the automatic HAS were identified from the annotated Operability Test procedure (TP0402, Rev B). Manual data records were observed and the time entry for the conduct of the test was noted in the annotated test plan from the pre-seismic testing. The HAS data was displayed and showed no errors occurred during this test. No anomalies were found.

Conclusions

The final session of the regulatory audit consisted of an overview of future interactions and HFC's plans to generate additional clarifying information to resolve issues identified during this visit.

It was agreed that the next two NRC-HFC teleconferences will be held on October 20 and November 17. The audit team stated that the draft Audit report will be provided to HFC by November 17 for review to confirm that no proprietary information is disclosed. It was noted that the technical evaluation report should be completed by December 2009, to support release of a safety evaluation in June 2010.

It is anticipated that the NRC will seek, formally, clarification on the qualification testing program, the relationship between HFC quality processes and regulatory guidance, and the definitive identification of hardware and software modules within the scope of the HFC-6000 platform. In addition, technical questions about the response time characteristics of platform and the terminology for offline versus online as well as the modes of operation for the controller will be addressed later.

Finally, HFC will generate additional clarifying information that includes a qualification testing summary, a mapping of the HFC QA plans and procedures to BTP 7-14 guidance, and requirements specification for the functions of the pre-developed software (e.g., function block modules) for which documentation was omitted. NRC and HFC will consider a second site audit on November 23-24, 2009, to allow follow up on the HFC actions regarding the CRs initiated during the visit and to allow discussion of the additional information that HFC is generating.

List of Documents Reviewed

In addition to the previously docketed materials that were made available as a comprehensive set at HFC facilities, the following documents were provided for review during the conduct of the audit:

ATP0402, Rev. A
DS001-000-03, Rev A
Master Configuration List ERD-111 (Excel Spreadsheet)
Parts Interchangeability Evaluation 375, 7/27/09
PO 005040-00, 10/7/09
SC100003 2/14/04
SR001-000-014, Rev. A
SR001-000-50, Rev. A
TR001-000-02, Rev. A
Bill of Materials for ERD-111
WI-VV-101, Rev. A, Att. 7.5
WI-VV-006, Rev. B
WI-ENG-812, Rev. C
WI-ENG-204, Rev. A
WI-ENG-007, Rev. A
TS901-000-37, Rev. C
TS901-000-34, Rev. A & B

HFC Audit Team:

Allen Hsu	Ed Herchenrader	Charles McKinney	Terry Gerardis
Ivan Chow	Jon Taylor	Greg Morton	James Hall
Gregory Rochford	William Luo	David Briner	

Items not closed during the audit

Clarification of online versus offline status for HFC-6000 modules (TR pp. 7-3 and 8-42, RAI 69c) and modes of operation (Run, Offline, Simulation, and Test) (MS901-000-01 p. 37).

Updated list of the modules and components with all necessary identification information to uniquely specify the scope of the HFC-6000 platform covered by the TR.

In contrast to stated conformance with EPRI TR-107330 requirements, the qualification results do not demonstrate comprehensive environmental stress withstand capability and PLC performance in compliance with the specified acceptance criteria. Explanation of how deviations from the requirements of EPRI TR-107330 were justified and an explanation of how quality issues with the execution of the test program have been addressed. Docketing of the performance and environmental stress envelopes as supported by test results. Justification for the omission of tests and analyses (specifically, the RS101 electromagnetic susceptibility test, the Failure to Scan test within the Operability test sequence, and a radiation withstand analysis).

Clarification regarding the relationship between the HFC software quality assurance plans and procedures for maintaining pre-developed software and the BTP 7-14 acceptance criteria for

software life cycle documentation. Explanation of the equivalence (e.g., provide a mapping) between the HFC QA program and BTP 7-14.

The “defined maximum response time characteristics” and the means for establishing a “predetermined maximum response time” as identified in Section 8.1 (pp. 8-1 and 8-6) of the TR.