Regulatory Audit Plan HF Controls HFC-6000 Topical Report
Carrolton, Texas, December 16-18, 2009

Background

By letter dated March 5, 2008, as supplemented by letters dated November 15, 2007 and January 16, 2009, Doosan HF Controls Corporation (HFC) requested approval for the "HFC-6000 Safety System Topical Report," document number PP901-000-01, Rev. C. The supplemental documents provided under cover letters dated November 15, 2007 and January 16, 2009, provided additional information that clarified the application and did not expand the scope of the application.

The topical report was accepted for review by letter dated September 16, 2008. In support of this review effort, the NRC staff and its contractor have conducted a regulatory audit at the HFC facility in Carrolton, Texas, on October 6-9, 2009; documented by audit report dated January 27, 2010 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML093580044). During that audit, the hardware configuration of the HFC-6000 qualification test specimen was observed, performance characteristics and functional capabilities (e.g., response time, failover, diagnostics, etc.) were demonstrated, and thread audits were performed. This audit will supplement the previous audit by providing confirmation of docketed information and close out of open items from the last audit.

The purpose of the audit is to verify that the implementation activities are executed in accordance with their plans.

Regulatory Audit Bases

An audit is necessary to identify and confirm design and process information that supports evaluation of information submitted by HFC in the Topical Report PP901-000-01, "HFC-6000 Safety System Topical Report," Revision C. The topical report was submitted for review in anticipation of future licensing submittals under Title 10 of the Code of Federal Regulations (CFR) Part 50 and Part 52 that would involve safety application of the HFC-6000.

Regulatory Audit Scope

HFC has been requested to provide information and supportive documentation at their Carrolton, Texas office for the NRC staff to facilitate a timely review of the topical report. This information should contribute to verification of the information submitted made in Topical Report PP901-000-01 that the platform components are dedicated under an acceptable qualification program and maintained under the current quality assurance program will be acceptable for use in U.S. nuclear applications.

High priority objectives for the on-site audit by NRC staff are to discuss the implementation and execution of the HFC-6000 Qualification Program, confirm evidence of conformance to cited guidance and criteria, and assess corrective actions for condition reports generated during the previous audit. Of particular significance for the NRC staff's review of the HFC topical report are follow up investigations regarding the execution of qualification testing and the associated quality assurance processes, the evidence of commercial-grade dedication of previously developed software (PDS), the processes for maintaining PDS quality through the remaining product life cycle, and resolution of issues cited in condition reports.

ENCLOSURE 1

Additionally, the NRC staff would like to review evidence of security features development in the HFC platform – i.e., requirements, design documentation and test reports – that HFC wishes to have credited in the NRC review (per the regulatory criteria of Regulatory Guide (RG) 1.152 (Rev. 2), Regulatory Positions 2.1, 2.2.1, 2.3.1, 2.4.1 and 2.5.1). Also, the staff would like to review the protections in place within the development environment that HFC credits for preventing tampering and/or introduction of unwanted code into the developed product (per the regulatory criteria of RG 1.152 (Rev. 2), Regulatory Positions 2.1, 2.2.2, 2.3.2, 2.4.2 and 2.5.2).

Each objective of this audit supports clarification of technical evidence necessary to enable resolution of whether the HFC-6000 platform and its life cycle processes are of a quality suitable for use in US nuclear safety system applications.

The on-site audit permits inspections and clarifying discussions. The audit includes test facilities, record keeping facilities, PDS dedication records and testing/maintenance tools, and other components that require access to HFC's physical plant for inspection.

Information and Other Material Necessary for the Regulatory Audit

HFC-6000 software code inspection reports for all PDS software modules (SR###-###-##)
HFC-6000 code listings for all PDS software modules
HFC Quality Assurance procedures, QPP-##.##
User Manuals, UG004-000-##
TS002-000-01 ICL Functional Test
TS002-000-03 C-Link Functional Test
TR002-000-14 ICL Operation, Baseline Performance, Component Functional Test Report
TR002-000-15 C-Link Operation, Baseline Performance, Component Functional Test Report

Regulatory Audit Team

Norbert Carte, Team Leader
Tim Mossman, Engineer
Richard Wood, Nuclear Engineer (Contractor)
Jonathan Rowley, Project Manager

Regulatory Audit Activities

1. Confirm that implementation of security features was appropriately controlled throughout the development process

2. Confirm that appropriate security measures have been and are currently implemented for the various developmental life cycle phases of the HFC-6000 to minimize/mitigate the potential for tampering and the introduction of unwanted code. Confirm that adequate software quality assurance processes are implemented for maintaining system software (i.e., pre-developed software).

3. Confirm that the equipment qualification documentation clearly identifies environmental stress and performance envelopes while fully addressing anomalies and that quality processes and procedures are implemented.

4. Confirm that the configuration management processes are implemented.

5. Perform thread audits for selected set of requirements, specifically addressing completeness as well as forward and backward traceability.

   (a) Starting with security related functionality (e.g., online/offline switch) and tracing forward to test documentation and backwards to requirements
   (b) Starting with operating system functionality and tracing backwards to requirements and tracing forwards to test documentation
   (c) Starting with application function blocks and tracing forwards to test documentation and backwards to requirements

6. Close out remaining open items identified during initial audit (e.g., status of condition reports).

<u>Logistics</u>

The audit is to be performed at HFC's Carrolton, Texas, office. The audit will be conducted over three days from December 16-18, 2009.

<u>Deliverables</u>

At the conclusion of the audit, the NRC staff will conduct an exit briefing and will provide a summary of audit results. A final Regulatory Audit Summary will be provided to HFC within four weeks of the completion date of the audit. The Regulatory Audit Summary will contain the following information:

- Identification of any specific materials that require docketing in support of a safety determination.

- Identification of specific materials for reference (procedures/processes/documentation) that provide support of the determination of whether:
  1) the HFC-6000 Qualification Program is commensurate with the requirements for NRC safety system applications;
  2) the methods and execution of the commercial dedication approach and qualification testing support the conclusions drawn about critical characteristics for the HFC-6000 base platform; and
  3) the corrective actions resolve identified conditions and demonstrate implementation of quality processes.

- Review report of items specifically reviewed.

REPORT FOR THE AUDIT OF THE HFC-6000 PLATFORM AT DOOSAN HF CONTROLS ON DECEMBER 16-18, 2009

HFC Audit

U.S. Nuclear Regulatory Commission (NRC) staff [Timothy Mossman and Jonathan Rowley] and the supporting contractor [Richard Wood of Oak Ridge National Laboratory] visited the Doosan HF Controls (HFC) facility in Carrolton, Texas, from December 16 through December 18, 2009, to perform a second regulatory audit. The purpose of the audit was to supplement the previous audit by providing resolution of outstanding technical issues and evaluation of progress in resolving open items.

During the course of the site visit, the audit team engaged in technical discussions with HFC staff and conducted thread audits. In particular, the visit permitted the application of the HFC Corrective Action process to be reviewed, allowed more detailed discussion of actions underway to address open items that were identified in the previous audit, and enabled confirmation of the security features associated with the HFC-6000 as well as the HFC corporate approach to enforcing a secure development and implementation environment.

Seven activities were specified in the audit plan (Enclosure 1) that was provided to HFC prior to the site visit. These activities support assessment of claims made by HFC in the submitted topical report. The findings from these audit activities are summarized below.

Regulatory Audit Activities (Summary of Findings)

1. Security features for the HFC-6000 platform – During the audit, HFC made available two security documents. These documents are RR901-000-23 Rev. A, “HFC-6000 Security Concept,” and RR901-000-38 Rev. A, “HFC-6000 Product Line Security Overview.” These documents should be submitted to the docket, with appropriate protection invoked for sensitive information.

As part of the review of the security provisions included in the design of the HFC-6000 platform, the audit team examined five security-related function “threads”. The thread audits indicated that the source code reviews conducted by HFC were sufficiently thorough to enable findings relevant to the quality of the source code and, in one case, identified potentially unneeded code (which is an area of emphasis in the security Regulatory Positions in Regulatory Guide (RG) 1.152, Rev. 2, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants”). However, a Condition Report (CR) was generated by HFC to examine the source code review findings and ensure that appropriate follow-up action is taken to resolve the perceived discrepancies.

Based on the findings of the thread audits, two of the functions of the system firmware (i.e., the Programmable Read Only Memory (PROM) to FLASH synchronization and application software mirroring between Primary and Secondary controllers) have the potential to be security features. However, based upon the finding that these features may be turned on or off depending on jumper/switch settings, HFC will need to determine (and docket) the rules for these capabilities. Alternately, if HFC determines that the settings of these features may have relevance to nuclear safety applications that may be developed in the future, these items may need to be addressed on an application-specific basis.

ENCLOSURE 2

2. Life-cycle security measures – The audit team toured the HFC facility to confirm the measures that contribute to security for the development and configuration management systems at the HFC facility. Aspects of physical security, computing environment security, configuration management and version control, and security for the assembly and testing of components and integrated products were observed. Additionally, relevant security information contained in RR901-000-23 Rev. A and RR901-000-38 Rev. A was made available for review on site.

The HFC-6000 topical report and supporting documentation notes that other vendors may manufacture printed circuit boards and that those vendors would be provided the approved software and instructions for those installations. Per a project-unique Project Quality Plan, a firmware checkout procedure is developed which involves 100 percent inspection/testing of all boards and software used on the HFC-6000 platform. The audit team was able to inspect the Firmware Checkout procedure (A-702331-36Q) and final report for a recently completed project. The inspection/test documentation contained a printout of all the cyclic redundancy check (CRC) data and software revision dates for each component. Any discrepancies would be identified and corrected. Since the Project Quality Plan (and its Firmware Checkout procedure) is produced on a project-unique basis, this item should be reviewed as part of a specific application, and will be documented accordingly in the platform safety evaluation report (SER).

3. Quality assurance for maintaining system software – Discussion of software quality assurance (QA) dealt with commercial-grade dedication (CGD) 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 made available to the audit team a draft unnumbered document evaluating their QA processes and procedures for managing PDS software changes. Specifically, this document describes a mapping of their planning documents to the software life cycle documentation identified in NUREG-0800, Chapter 7, Branch Technical Position (BTP) 7-14, “Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems.” It was noted that BTP 7-14 addresses several planning documents that are application specific in nature. As part of the mapping effort, HFC is also identifying deviations from BTP 7-14 acceptance criteria and providing the rationale to address those deviations (e.g., identifying application-specific items). In discussions with HFC staff regarding the mapping, the audit team provided high-level comments. In particular, the significance of the software maintenance plan, the configuration management plan, and the software verification and validation (V&V) plan were discussed. For the software maintenance plan, it was noted that development tools should be covered as well as the PDS itself. When completed, the mapping analysis will support HFC in their response to the Request for Additional Information (RAI) Part 3 (ADAMS Accession No. ML100271720) questions on software dedication.

In addition to the five thread audits of security-related system functionality, four additional thread audits of system functions were conducted to further verify the “built-in” quality of HFC-6000 PDS. To support the tread audits of system functionality, HFC made available the revised documentation of the software requirements for HFC-6000 PDS as well as expanded requirements traceability documentation. Relevant documents include RS901-000-37 Rev. E, “HFC-6000 Controller and HFC-DPM06 SC, SAP, SEP Firmware, VHDL Program Code

Requirement Specification," and its associated appendices; RR901-000-31 Rev. E, "HFC-6000 Product Line Traceability Matrix;" RR901-000-31, Attachment A Rev. A, "CQ4 Traceability Matrix;" RR901-000-31, Attachment B, Rev. A, "Equation Interpreter Traceability Matrix;" and RR901-000-31, Attachment C Rev. A, "I/O Card Traceability Matrix." These documents represent an update of the software requirements specification for the HFC-6000 PDS and will contribute to the HFC response to the RAI Part 3 questions, in particular those questions related to software dedication.

The thread audit findings indicate that the documentation of software requirements has improved with the HFC revision effort. Specifically, requirements for CQ4 function blocks are now documented and traceability matrices have been generated. While several thread audits for the CQ4 function block requirements validation were found to be satisfactory, there were a few traces of system functionality through HFC documentation that did indicate some instances of ambiguous requirements or requirements only addressed implicitly within more general requirements. In some instances, a direct link between requirements and cited test procedures was not always clear (i.e., test procedures did not clearly test the firmware implementation of system functionality that corresponded to selected requirements). The presence of these conditions makes it difficult to assess claims of completeness, lack of ambiguity, traceability, and testability for the software requirements specification. RAI Part 3 contains questions on software dedication that are intended to provide information to resolve these concerns.

4. Equipment qualification of the HFC-6000 – The audit activity regarding quality assurance for the qualification of the HFC-6000 addressed documentation of the HFC-6000 qualification results and the quality processes and procedures in place for the qualification program. To resolve the issues identified in the first regulatory audit concerning the HFC-6000 qualification program and its documentation, HFC had generated summary information clarifying the environmental compatibility and performance envelopes that are demonstrated by the HFC-6000 qualification tests. This summary document (RR901-000-37 Rev. B, "ERD111 Performance Envelope") was made available to the audit team. In addition to describing the environmental test profile employed and observed performance for the Test Specimen, the summary document also describes performance deviations and provides associated justification to clarify HFC claims of compliance with NRC endorsed Electric Power Research Institute (EPRI) Topical Report (TR)-107330, "Generic Requirements Specification for Qualifying a Commercially Available Programmable Logic Controller for Safety-Related Applications in Nuclear Power Plants." The information contained in this document is intended to clearly establish the extent to which the HFC-6000 has been generically qualified. Based on the findings of the high-level review of this document, it was recommended that the demonstrated performance profile be expressed for each environmental factor where demonstrated performance differences occur. Furthermore, it was recommended that a more complete comparison of EPRI TR-107330 requirements versus actual performance should be documented. When completed, the summary document on the HFC-6000 qualification will support the HFC response to the RAI Part 3 questions on qualification.

Specific discussions concerning the qualification of the HFC-6000 addressed quality issues with the execution of the qualification program were conducted. These discussions focused on whether adequate procedures are in place to avoid deficiencies in future qualification testing such as those reported for the generic qualification of the HFC-6000 (i.e., the ERD111 project).

CR No. 2009-0624 was opened to ensure that procedures and processes are in place to address conditions that led to out-of-calibration modules being used for qualification testing. CR No. 2009-0630 was opened to review the qualification test procedures that are the baseline for future testing so that unnecessary or impractical steps are eliminated. Apparent omissions or deficiencies in the qualification program that had been identified during the audit in October were also discussed. In response to these findings, HFC has developed supporting documentation such as RR901-000-36 Rev. A, “Radiation Exposure Evaluation”. This report and other qualification documents that provide relevant information or supporting rationales were made available to the audit team.

As part of the confirmation of quality assurance for the qualification program, a thread audit (Thread #10) was conducted tracing test records and supporting data files from HFC-6000 qualification testing. No anomalies were found.

5. Configuration management processes – Confirmation that configuration management processes are in place at HFC involved audit of the control and configuration processes for the HFC-6000 product line and observation of the implementation and execution of HFC corrective action processes. During the site visit, the audit team investigated the document storage records and control provision. The control of documents was observed and procedures to manage document access were demonstrated. For example, the forms for obtaining copies of controlled documents (WI-DOC-001 Rev. E, Attachment 7.1, “Document Control Print Request Form”) were observed. HFC staff pointed out that WI-ENG-812 Rev. D was revised in response to a condition report to require explicit notation of the revision identification for all documents and citations. During the thread audits that were conducted, it was observed that document and citation examples consistently gave complete identification (e.g., revision) information.

The audit team reviewed the software configuration management and version control / protection provisions at the HFC facility. Topics investigated included the means for verification of the software installed and used for HFC-6000 modules and the use of software librarian tools to maintain control of software versions. As observed in the first audit and addressed as part of audit Item 2 above, there is a need to ensure that installed software is verified before system delivery. Confirmation of this verification should be included as a plant specific review item.

During the previous audit, HFC was asked to make available a comprehensive list of modules and components that are within the scope of the base platform covered by the Topical Report. 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 qualification summary document (RR901-000-37 Rev. B) contains a listing of this information and, thus, it can support the HFC response to RAI Part 3 questions on the platform scope.

The status of HFC corrective actions arising from the regulatory audit conducted in October was reviewed. Four CRs were cited in the Audit Report (ADAMS Accession No. ML093580044) for the initial audit. It was determined that resolution of these CRs had either been completed or was in progress with final disposition planned as part of the response to RAI Part 3.

New CRs were generated as a result of the thread audits conducted during this site visit. CR No. 2009-0623 and CR No. 2009-0625 were opened to address anomalies in the demonstration of key characteristics for software requirements (i.e., unambiguity and testability, respectively). CR No. 2009-0624 and CR No. 2009-0630 were opened to address quality issues for the qualification program; specifically, the CRs address issues related to the definition and implementation of qualification procedures. CR No. 2009-0626 was initiated to ensure that corrective actions are taken to completion. In particular, instances of System Change Requests (SCRs) were found in which no documentation that the actions were completed was available. CR No. 2009-0628 was opened to ensure that prototype tests were conducted for all HFC-6000 modules. RAI Part 3 Question 152, on the status of corrective actions to close condition reports opened in conjunction with the regulatory audits, provides the means for ensuring that the corrective action program for HFC is implemented.

6. Security and system functionality thread audits – Ten thread audits were conducted during this site visit. Five thread audits addressed security-related functionality. In addition to the coverage of operating system functionality in the security-related thread audits, three additional thread audits for operating system (OS) functions and capabilities were conducted. A thread audit of application functionality involved two traces of function block requirements through the HFC-6000 documentation. Finally, a quality control thread audit was conducted by tracing environmental qualification test records.

Some anomalies were identified in the thread audits and potential HFC actions to resolve the conditions were discussed. In some cases, CRs were initiated by HFC. Additionally, it was determined that specific questions in the RAI Part 3 will address the underlying issues associated with the anomalies uncovered in the thread audits. However, two questions will be added to the RAI set as a result of the audits.

The first security-related thread audit addressed write enable mechanisms for the HFC-6000 that support download of application software to a HFC-SBC06 controller module while it is out of service in a maintenance and testing assembly. The specific supporting mechanism that was audited is the write enable check function. No anomalies were found.

The second security-related thread audit involved system functionality to ensure application software integrity. The specific system functionality that was audited is the initialization mechanism that compares the firmware resident in flash memory with the firmware installed in PROM. Based on the thread audit findings, clarification of the preferred jumper configuration for the HFC-SBC06 controller module is needed. Additionally, it was unclear whether the cited prototype test provides adequate validation that the requirement is satisfied by the firmware implementation. As a result of the thread audit, CR No. 2009-0625 was initiated and a question will be included as part of RAI Part 3.

The third security-related thread audit related to equalization of application software between an online Primary controller and a Secondary controller undergoing initialization. In conducting the thread audit, it was noted that the requirement is ambiguously worded. A CR (CR No. 2009-0623) was opened based on findings of this thread audit.

The fourth security-related thread audit involved two communications checks to validate the integrity of message / data packets. The first trace concerned the use of CRC16 validity checks for Inter-Communication Link (ICL) communications. The second trace involved the use of CRC32 validity checks for Communication Link (C-Link) communications. It was observed that the source code review documents for these validation features were thorough and contained findings and recommendations to be addressed through the HFC corrective action process. However, it was unclear whether the resolution of these review findings had been taken to completion. CR No. 2009-0626 was opened in conjunction with this thread audit.

The fifth security-related thread audit related to communications validation features, specifically the use of formal message structures and pre-defined message content. A review of the test documentation relevant for validating this feature revealed that testing of an analog input module was not reported and the module may have been omitted from the tests. CR No. 2009-0628 was initiated based on the audit findings.

The sixth thread audit involved OS functions for terminating task execution. The selected function was the DELA function. It was noted that the prototype test procedure identified in the traceability matrix and by the HFC staff does not explicitly address this specific termination function (or any of the termination function options) but rather implicitly covers the function through testing of the software download functionality. Consequently, it is difficult to assess whether the test provides adequate validation that the requirement is satisfied by the firmware implementation.

The seventh thread audit addressed a diagnostic function of the HFC-6000 OS to ensure that an application task is executed for a complete program cycle at least once in a given interval (i.e., context switch interval). It was found that the selected diagnostic is implicitly covered by the identified requirement, is not explicitly described in the design documentation, and is not clearly demonstrated to have been tested based on the test documentation reviewed thus far.

The eighth thread audit dealt with internal messaging within the HFC-6000 controller module. Specifically, the use of the Universal Communications Protocol (UCP) for inter-processor messages was investigated. High-level requirements and a general discuss of the design were identified. Time constraints prevented a more detailed trace through the HFC-6000 documentation but RAI Part 3 contains a specific question on the topic that should provide the desired information.

The ninth thread audit addressed application functionality in the form of two selected function blocks. The traces conducted under this thread allowed an evaluation of progress in resolving a deficiency in the completeness of the software requirements specification that was identified as an open item through a thread audit conducted during the previous regulatory audit in October. The successful conduct of two traces for the selected function blocks in this thread audit give indication that the HFC staff is resolving this open item. The response to RAI Part 3 will enable a final determination on this item.

The tenth thread audit involved a trace of test records and supporting data from HFC-6000 qualification testing. Time-stamped test data corresponding to selected qualification tests were located and retrieved by HFC staff based on the date and time noted on the test records. No anomalies were found.

7. Status of open item resolution – The findings of this regulatory audit support a determination of the status of unresolved issues relevant to the review of the HFC-6000 topical report. Specifically, some open items were identified in the Audit Report for the regulatory audit conducted in October. Additionally, HFC opened some CRs during the course of the initial audit to address anomalies found during thread audits.

The open item on the scope of the HFC-6000 system relates to clear identification of the modules and components included in the platform under review. The qualification summary report contains a listing of these modules. This identification should be docketed in the response to RAI Part 3.

The open item on qualification of the HFC-6000 involves the performance and environmental stress envelopes demonstrated by testing and clear identification of deviations from the EPRI TR-107330 testing program and acceptance criteria. HFC is developing a summary document on qualification (RR901-000-37) to describe the qualification envelopes and clarify deviations from the generic qualification program of the EPRI guidance. RR901-000-37 Rev. B was made available to the audit team to support discussions of the qualification evidence. This report and supporting documents (e.g., RR901-000-36 Rev. A) should be docketed in support of the response to RAI Part 3.

The open item on maintenance of PDS involves the relationship between the HFC software quality assurance plans and procedures for maintaining PDS and the life cycle processes described in BTP 7-14. Specifically, this information is needed to facilitate the review of the HFC software quality program to manage PDS software against BTP 7-14 acceptance criteria. To resolve this open item, HFC has been developing a mapping of their QA documents to the plans and products described in BTP 7-14. The draft unnumbered document containing this mapping identifies HFC software documents that are equivalent to BTP 7-14 life cycle documents. This document was made available to the audit team and should be docketed in support of the response to RAI Part 3.

The open item on software dedication of PDS concerns the completeness and traceability of the software requirements specification that was re-engineered as part of the CGD process. Specifically, it was observed during the first audit that the software requirements documentation did not address function blocks (i.e., the CQ4 software modules). Among other characteristics, it is necessary to demonstrate the completeness, unambiguity, traceability, and testability of the requirements to satisfy the acceptance criteria for this evidence of software quality. To support thread audits during this site visit, HFC made available revised requirements and traceability documentation. Specifically, RS901-000-37 Rev. E and RR901-000-37 Rev. E were provided to the audit team. These documents demonstrate progress by HFC in addressing this open item. If the enhancement of the requirements and confirmation of traceability are appropriately captured in the completed documents, the open item arising from these thread audits should be resolved and a determination on the evidence regarding commercial-grade dedication of PDS can be facilitated. Both documents and their associated attachments and appendices should be docketed in support of the response to RAI Part 3.

The remaining open items from the initial audit involve clarification of HFC-6000 operating modes and the response time characteristics of the system. These items will be addressed through questions in RAI Part 3. The audit team and HFC staff reviewed the status of corrective actions taken to resolve CRs generated in conjunction with the regulatory audit conducted in October 2009. Four CRs were identified in the Audit Report for the regulatory audit conducted in October. HFC provided for review the documentation of each CR opened as a result of the initial regulatory audit. This material includes the original condition report initiation form, the CR form with the root cause determination and corrective action plan, and the Corrective Action Implementation form(s). The corrective actions resulted in the following report revisions: DD0401 Rev. B, WI-ENG-830 Rev. C, RS901-000-31 Rev. E, RR901-000-10 Rev. B, and WI-ENG-812 Rev. D. The corrective action for CR No. 2009-0539 is in progress. The software requirements specification documentation (i.e., RS901-000-37 and the associated requirements traceability matrices) is being revised to document the complete set of requirements for the HFC-6000 PDS. The completion of this corrective action will form the basis for the HFC response to RAI Part 3 questions on software dedication.

Conclusions

During the site visit, the scheduled audit activities were completed successfully. Ten thread audits were conducted, some condition reports (CRs) were initiated, some system change requests (SCRs) were reviewed, and the status of actions to resolve open issues was reviewed.

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. Identification of a few incomplete (e.g., omitted or not explicitly stated) or ambiguous requirements in the reconstituted software requirements documentation developed for the commercial grade dedication of pre-developed software [CR 2009-623 and 2009-625],
2. Insufficient evidence for clear (i.e., explicit) traceability between some requirements and test procedures resulting in uncertainty how a few requirements are adequately tested [CR 2009-624],
3. Errors in execution of procedural steps for qualification testing which led to insufficient data [CR 2009-630],
4. Insufficient evidence that the corrective action process had been taken to completion to address HFC findings documented during their source code review (e.g., no record of completion for some SCRs) [CR 2009-626].

HFC is addressing these anomalies through their corrective action processes.

Regarding the remaining open items, they are being resolved through generation of additional documentation by HFC and are addressed in questions within RAI Part 3. The information being generated by HFC will be used to support responses to RAI Part 3. This information includes a qualification testing summary (RR901-000-37), a mapping of the HFC QA plans and procedures to BTP 7-14 guidance, and updated requirements specification documentation for the pre-developed software (RS901-000-37, RR901-000-31). These documents should be docketed as part of the response to RAI Part 3.

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:

A-702331-36Q
ATP0402 Rev. D
DS001-000-03 Rev. C
DS002-000-01 Rev. C
DS002-000-02 Rev. D
DS901-000-01 Rev. D
MS901-000-01 Rev. E
RS901-000-37 Rev. E
RR901-000-31 Rev. E
RR901-000-31, Attachment A Rev. A
RR901-000-31, Attachment B Rev. A
RR901-000-31, Attachment C Rev. A
RR901-000-36 Rev. A
RR901-000-37 Rev. B
SR001-000-015 Rev. C
SR001-000-031 Rev. C
SR001-000-042 Rev. C
SR001-000-060 Rev. C
SR001-000-063 Rev. C
SR001-000-073 Rev. C
SR001-000-076 Rev. C
SR001-000-085 Rev. C
SR001-000-138 Rev. B
SR002-000-002 Rev. C
SR002-000-015 Rev. A
SR002-000-028 Rev. A
TR002-000-14 Rev. A
TR002-000-15 Rev. A
TS002-000-01 Rev. A
TS002-000-03 Rev. A
TS901-000-02 Rev. B
WI-ENG-204 Rev. B

<u>HFC Audit Team:</u>

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

DETAILED RECORD OF THE REGULATORY AUDIT AT DOOSAN HF CONTROLS ON DECEMBER 16-18, 2009

Thread Audit Detailed Record

1) Audit of write enable mechanisms – A previously traced feature of the HFC-6000 firmware was selected for reexamination to assess recent updates by HFC staff to the software requirements specifications for the HFC-6000 pre-developed software and to allow security characteristics arising from this capability to be considered. The selected feature concerns the write enable / disable functionality to support application software configuration management. The thread audit consisted of a forward trace through the requirements specification, design documents, source code, source code review, and test documentation.

The specific firmware module selected for audit is the write enable check function that sets a permissive flag based on the position of the write protect switch for an HFC-6000 controller. When this feature is enabled, the transfer of downloaded application software from random-access memory (RAM) to flash memory is permitted. The previous thread audit for this capability is identified as Thread #5 in the Audit Report for the regulatory audit conducted in October 2009.

The audit team made the following observations:

- The requirement for the capability is found in RS901-000-37 Rev. E. Specifically, Requirement 3.1.1.f states that the "firmware shall support the 'write protect' function." The docketed version of RS901-000-37 (Rev. A) states this requirement in terms of support for download of application code to flash memory when the write function is enabled by the write protect switch (i.e., Section 4.1.1, Requirement 12 for the system processor or SC firmware). RR901-000-31, Attachment B, Rev. A, "Equation Interpreter Requirement Traceability Matrix" identifies the requirement for the equation interpreter to support download of application software (Paragraph 3.2.d).
- The original trace of this requirement through the design phase documents, source code, and source code review, and test documentation was supplemented by further confirmation of validation through testing. The reference for the write protect test is Paragraph 5.11 of TS901-000-02 Rev. B, "HFC-SBC06/DPM06 Prototype Test Procedure." Review of the document indicated that the test procedure was performed on June 24, 2004, and was verified as successful by the HFC QA organization. No anomalies were found.

In performing the thread audit for this capability, a clarification to the previous audit report was accomplished. The software module reviewed in the thread audit "implements a write enable check" as stated. However, the module that "stops the Equation Interpreter if the switch is set to enable writing" is actually a separate module, which acts if the permissive set by the initiating module indicates that the write protect switch is configured to allow software to be written to Flash memory. Thus, these two modules are among several contributors to the execution of a software download.

As part of the corrective actions taken to resolve CR No. 2009-0539, HFC initiated revision of the software requirements specifications for the HFC-6000 PDS. Additionally, HFC is updating the associated requirements traceability matrices. This thread audit provided an initial assessment of these revisions. It was found that the revision of the requirements specification document is resulting in revised expressions of the requirements that are consistent with common practice and should be more amenable to establishing the characteristics required by the Institute of Electrical and Electronics Engineers (IEEE) Std 830-1993, “IEEE Recommended Practice for Software Requirements Specifications,” as endorsed by Regulatory Guide 1.172, “Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants.”

2) Audit of mechanisms to ensure application software integrity– System functionality to enable application software integrity to be checked was selected for audit because of its relevance to the security characteristics of the HFC-6000. The thread audit consisted of a forward trace through the requirements specification, design documents, source code, source code review, and test documentation.

The HFC 6000 platform contains a feature that, upon initialization or reset, compares firmware resident in the flash memory with the firmware installed in the PROM. If there is any discrepancy between the two sets of software, the code in the PROM is written into the flash memory. This capability ensures that any modification of the software in flash memory that may have occurred while the module is out of service will be corrected upon restart, which minimizes the potential for tampering with firmware.

The audit team made the following observations:

- The requirement for the capability is found in RS901-000-37 Rev. E. The specific requirement that drives this capability is found in Section 3.1.1.a, Table 1, describing the capabilities associated with Jumper #1. Inspection of the requirement indicates that the jumper has two possible settings. The primary (jumper on) condition is to have the system processor boot from the firmware on the PROM and synchronize the flash memory to the PROM software. However, the second jumper setting (jumper off) allows for direct boot from the flash without synchronization to the PROM firmware. [Note: there is a similar requirement for Jumper #8, which covers the C-Link processor (or SEP firmware) and ICL processor (or SAP firmware).]
- The design of this function is contained within several documents. MS901-000-01 Rev. E, “HFC-SBC06-DPM06 Boards Module Design Specification, System Controller,” contains multiple sections that discuss the PROM/FLASH firmware synchronization. Section 4.3, Table 2, essentially replicates the requirement language for the capability of Jumper #1. Section 4.5 states that the firmware must originally be burned onto the PROM and then installed on the printed circuit board. Section 4.5.1 contains the firmware installation procedure for transferring the firmware from the installed PROM onto the flash memory. Step 12 of the procedure instructs the installer to remove Jumper #1 after installation. [Based on this instruction, it would appear that the PROM/FLASH synchronization is not intended to be a normal operational condition. A question will be added to RAI Part 3 to ensure the intended configuration is clarified.] It was noted that Section 4.5.3 states that direct download of system program code to flash memory is not supported by the HFC-6000 platform. Sections 5.4.2.3 and 5.4.3.3 state that this prohibition on direct download is also true for the ICL and C-Link processors, both of which are required to be powered down and have installed a new PROM with any firmware modification.

- DS901-000-01 Rev. D, "HFC-SBC06-DPM06 Module Detailed Design Specification," Section 5.1.1.1, also describes the PROM/FLASH synchronization process.
- The audit team was able to review the source code review documentation for this capability. SR001-000-073 documented the source code review of software module SBCP6INI.A10. The record clearly identified the software module, the module version and its location in the SourceSafe tool. No anomalies were noted in the review.
- The test documentation that addressed this requirement was identified as TS901-000-02. The audit team review of the test specification noted that test credited for verifying the PROM/FLASH firmware synchronization capability did not specifically address that function. The test described in Section 5.4 covered successful processor initialization, but did not appear to verify that firmware from the PROM had been written to the flash memory upon initialization. The test set-up description (Section 4.1.1) identified that Jumper #1 was to be set to "on," consistent with synchronizing the PROM and FLASH; however, it did not describe the condition of the flash memory prior to the test and how the transfer from PROM to FLASH would be verified. A condition report (CR No. 2009-0625) was generated investigate whether the cited test procedure adequately addresses testing of the mechanism for ensuring application software integrity.

As a follow-up action to this thread, the HFC response to the RAI questions covering digital security should clearly articulate HFC's position on PROM/FLASH firmware synchronization for nuclear safety applications and how that position supports the digital security concept for the HFC-6000 platform. A question will be added to RAI Part 3 to specifically inquire about the HFC position on the identified configuration option and its impact on digital security. Based on the RAI response, any needed changes to the documentation should be made to clarify the position for nuclear safety usage.

3) Audit of Primary/Secondary controller equalization – The capability to equalize or mirror the application software of an online Primary controller by a Secondary controller undergoing initialization supports security considerations for the HFC-6000. This capability was selected for audit. The thread audit consisted of a forward trace through the requirements specification, design documents, source code, source code review, and test documentation.

A security-relevant capability of the HFC-6000 platform is the mirroring of application software from the Primary controller to the Secondary controller, upon the completion of initialization by the Secondary controller. The equalization capability supports digital security, as a controller module would need to be taken out of service in order to modify its software. Upon return to service within the installed cabinets, any undesired change to the software would be over-written with the application software of the Primary controller, which remained in service with operating application software. The only means to permanently alter the application software would be to remove both the Primary and Secondary controller modules. Removing both units from service should be readily detectable.

The audit team made the following observations:

- The requirement for the capability is found in RS901-000-37 Rev. E. Paragraph 3.1.4.c states that the "status" of the application shall be mirrored from the Primary controller to the

Secondary controller. While the design and test documents appear to support the actual mirroring of the application code, the language selected for the requirement, specifically the use of the word "status," creates ambiguity in what is to be copied from Primary to Secondary controllers. CR No. 2009-0623 was opened to address the ambiguous wording of the requirement.

- Section 5.4.1.2 of MS901-000-01 Rev. E addresses this capability. The section clearly states that the Primary controller transfers its image of application code to the Secondary controller via the DPM06 module after the Secondary controller completes its internal initialization.
- The source code review trace pointed to multiple code modules. SR001-000-138 covered the review of module STATSK.P10, which is a module that calls for the mirroring of the code to be performed. The document identified the file date and version, as well as its location in the SourceSafe tool. No anomalies were found.
- TS901-000-02, Section 5.10, clearly covers test of the equalization function for application software. The test describes a Secondary controller being brought online and being allowed to synchronize with the Primary controller already online. An engineering workstation is used to verify all applications were successfully equalized. The test then shuts off and restarts the original Primary controller (which becomes the Secondary controller upon re-initialization) and checks to see if it equalized with the new Primary controller.

As a follow-up action to this thread, the requirement should be revisited to ensure that it unambiguously states the capability that is integrated into the HFC-6000 module regarding equalization of application code from Primary to Secondary controllers. In addition, it was noted that the primary to secondary controller application software mirroring may not work if the secondary controller's write protect switch is not set to enable the function. HFC needs to explicitly state whether this setting is intended to permit this function all of the time and, if so, what steps are to be taken to ensure the correct settings are maintained.

4) Audit of communications integrity features – Ensuring the integrity of messages that may originate from other systems that interface with the HFC-6000 platform is an important security consideration. The mechanisms to validate the integrity of communication packets for both the ICL and C-Link of the HFC-6000 were selected for audit. The two tracks of this thread audit consisted of forward traces through the requirements specification, design documents, source code, source code review, and test documentation.

For the first trace, the C-Link processor, which potentially may be used as a communication interface to other safety divisions and/or other systems in a nuclear safety application, performs CRC32 checks to validate data packets. [Note: any use of the C-Link for interdivisional communication or bidirectional communication with other systems would need to be reviewed on an application specific basis.] For the second trace, the ICL processor performs a CRC16 validity checks on messages it receives. Rejected messages are logged.

The audit team made the following observations for the first trace:

- The requirement for the capability is found in RS901-000-37, Rev. E. Paragraph 3.2.6 states that the firmware shall depend on hardware CRC32 to validate data packets.

- DS002-000-01 Rev. C, "C-Link Protocol Software Component Design Specification," describes the CRC32 check capability in several sections. Sections 2.1 and 5.4.1 restate the requirement language. Section 2.3.3 contains the logic that uses the CRC32 check to evaluate data.
- The audit team examined two source code review documents. SR002-000-028 covered a software module review. Of note in that review was an observation that a particular function may be unneeded code that was only used for a testing purpose. The review recommendation was for the code to be removed. This observation confirmed that the source code reviews were concerned with unnecessary and unneeded functions, which is a particular point of emphasis in the security positions of Regulatory Guide 1.152 (Rev. 2). However, it was not clear that the recommended action had received appropriate follow-up. CR No. 2009-0626 was opened to confirm that System Change Requests (SCRs) are taken to completion. The source code review of another software module, SR002-000-015, was also reviewed. The module version, date and location in SourceSafe were all identified. No anomalies were identified during that review.
- TS002-000-03 Rev. A, "SEP Processor (C-Link) Firmware Operational Component Functional Test Specification," describes the test of the CRC32 check. Section 7.3 describes several conditions imposed on the communication link designed to induce signal errors. TR002-000-15 Rev. A, "C-Link Operations, Baseline Performance Component Functional Test Report," contains the results of the testing. Section 7.3 of the report showed multiple screen captures which depicted the detection of errors in received messages based on the CRC32 check.

The audit team made the following observations for the second trace:

- The requirement for the capability is found in RS901-000-37 Rev. E. Requirement 3.3.8 states that the ICL firmware shall perform a validity check on messages received. The requirement also mandates that messages that fail this CRC16 check be rejected and these "errors" logged.
- The CRC16 algorithm is described in DS002-000-02 Rev. D, "ICL Protocol Component Design Specification: Inter-Communications Link." Section 3.6 notes that the CRC16 algorithm is used for message transmission and receipt, and the algorithm is the same as the one used in the MODBUS protocol.
- The audit team examined the source code review of the code that implements the module calls to the CRC16 calculation and verification modules. This main module was the same as the one examined for the first trace under this thread (see above). In addition, the source code review for module CRC16.A10 (SR001-000-060, Rev. B) was reviewed. As with the other records of source code reviews examined by the audit team, the HFC source code reviews made relevant findings. In this instance, there was an observation noted in the source code review that there were some discrepancies associated with the code not adhering to the provisions of WI-ENG-204 (i.e., the HFC Coding standard). The finding did not note that any code functionality or behavior was affected, and discussions with HFC staff indicated that the inconsistency with the standard was likely associated with how the code was commented. The evidence that this source code review was thorough enough to make findings is a positive indication for the process; however, as with other source code reviews that were part of this audit, it was unclear how these findings were addressed via HFC's

quality assurance and corrective action processes. This anomaly was included in the condition report CR No. 2009-0626. Finally, the source code review record did note that the code was contained in the Serena Version Manager software library tool.

- TS002-000-01 Rev. A described the test procedure that injected several incorrect codes, values and set-up configurations for the ICL processor to evaluate. TR-002-000-14 Rev. A demonstrated that the code performed as expected in light of the various “error” messages sent to it. Screen captures and text descriptions of the test observations were provided in the report. Although it was noted that the ICL processor recognized these errors, the docketed topical report does not contain any display component. Thus, if this feature is to be used to alert operators to message errors, the mechanism to display the errors would need to be reviewed as part of the application.

As a follow-up action to the two traces for this thread, HFC should revisit any findings/observations made during the source code reviews and ensure that they received appropriate evaluation and disposition. Specifically, HFC should ensure that pending SCRs have been completed and that all source code review findings have been addressed through the corrective action process. Of particular interest are findings related to identification of unused and unwanted code.

5) Audit of communications validation features – The use of formal message structures and pre-defined message content supports security. The restriction of communication to known message types and configurations was selected for audit. The thread audit consisted of a forward trace through the requirements specification, design documents, source code, source code review, and test documentation.

The ICL, which provides the communication pathway between the various input/output (I/O) modules and the HFC controller modules, conducts communication using predefined messages and data definitions. These messages are pre-defined in the firmware.

The audit team made the following observations:

- The requirement for the capability is found in RS901-000-37 Rev. E. Requirement 3.3.1.d states that the firmware shall include all valid command codes and definitions for all message structures for the ICL protocol.
- DS002-000-02 Rev. D contains the descriptions of the message structures. Specifically, Section 3 of the document identifies the address codes, message codes and data fields that the ICL firmware is capable of using / recognizing.
- The audit team examined the source code review of the code that implements the message recognition. SR002-000-002, Rev. C documents the HFC review of the Q10TSK.A10 module. The review identified the version of the code module by version number and dates, as well as its location in their SourceSafe code library. The review recorded a discrepancy with regard to the uniqueness of the identifying revision information for the particular module evaluated. HFC staff explained that the discrepancy was likely an artifact of the transfer of module revision records from their prior software library to their current tool. It was, however, unclear if the finding had been handled per HFC quality assurance and corrective action processes to appropriately disposition the issue.

- TS002-000-01 Rev. A described the test procedure and test set-up for the ICL tests. Section 7 of the document describes that each module type that may communicate with the ICL processor will occupy one of the 53 available slots during testing. TR002-000-14 Rev. A, which contains the results of the ICL testing, was examined. Section 4.1 of the test report document contains the hardware test set-up. A comparison of modules included in the test (Table 1 of the topical report) against the modules included in the topical report (Table 6-1) revealed one inconsistency. Analog input module AI8M, which is included as part of the topical report, was not included in the test. It was unclear why the module was omitted from the test. CR No. 2009-0628 was opened to determine why the AI8M module was not covered by the test. The test demonstrated that all of the modules that were included in the test were able to perform the necessary initialization handshaking with the ICL processor and remain operating (using a sample application) for five minutes without error. Given the variety of field devices that may be connected to these I/O modules, an exhaustive test of every message did not appear to have been achieved with the sample application software in use. A more comprehensive test of the messages should be performed on an application-specific basis.

As a follow-up action to this thread, HFC should revisit any findings / observations made during the source code reviews and ensure that they received appropriate evaluation and disposition. Also, HFC should review the testing of the I/O modules and determine an appropriate corrective action for omitting the AI8M module from the ICL tests.

6) Audit of HFC-6000 operating system functions for task execution termination – A function of the HFC-6000 operating system (OS) task execution environment was selected at random for this thread. The audit consisted of a backward trace through the requirements documentation and a forward trace through the design documents, source code, source code review, and test documentation.

The HFC-6000 OS provides functions that are called at the completion of a task to terminate the task execution and return program control to the operating system. Seven execution termination functions are described in DS001-000-01 Rev. B, “Operating System Design Specification.” A particular function was selected for this audit. Calling this function to terminate execution of a task causes the next execution of that task to be delayed by the OS for a specified amount of time (i.e., some multiple of real-time clock tick counts).

The audit team made the following observations:

- The selected function is described in Section 2.3.1.4 of DS001-000-01 Rev. B. The corresponding requirement is documented in RS901-000-37 Rev. E, Section 3.1, Item 2c. The docketed RS901-000-37 Rev A does not explicitly address a requirement for this functionality but instead states that the OS performs the function of a task scheduler.
- The forward trace through the HFC-6000 documents was conducted using the requirements traceability matrix contained in RR901-000-31 Rev. E. As noted, the description of this function is contained in DS001-000-01 Rev. B. The options for task termination are also described in DS001-000-06 Rev. A, “System Software Components Design Specification,” Section 2.1.1.3.6. The source code file and source code review document (SR001-000-063 Rev. C) were provided to the audit team for review. The appropriate identification of the

software module was documented and the function was adequately described in the source code review. No anomalies were found.

- The prototype tests for the HFC-SBC06/DPM06 modules were identified in RR901-000-31 Rev. E for the testing of OS functionality. The prototype test procedure is documented in TS901-000-02 Rev. B. Section 5.9, “Verifying Logic Functions”, was identified as providing validation of the selected function for task execution termination. Specifically, the HFC staff stated that step 6, which involves downloading a compiled program to support logic function verification during prototype testing, would call the selected function.
- HFC staff stated that these tests also demonstrate other task execution functions. It was noted by the audit team that the testing of the selected function is implicit in the test procedure and the procedure does not specifically address this or the other OS task execution termination functions. The absence of an explicit treatment of OS functionality in the test documentation makes it difficult to assess whether testing provides adequate coverage of the software requirements.

As a follow-up action to this thread, HFC staff indicated that they will check to ensure that all of the OS task execution termination functions have been tested. The HFC response to the RAI questions concerning software dedication, specifically Question 157 on evidence to support claims of compliance with Regulatory Guide 1.172, should address whether the requirements for OS functionality are verifiable. The identification of software component tests to validate the requirements are satisfied by the PDS is one means of providing this evidence.

7) Audit of operating system diagnostic function for application execution – The mechanism for detecting a failure to execute at least one complete application program loop during a specified time (i.e., a “context switch” interval) was selected for a thread audit. The audit consisted of identifying the requirement that corresponds to the diagnostic mechanisms and then conducting a forward trace through the design documents, source code, source code review, and test documentation.

The topical report for the HFC-6000 in Section 7.1.1.2 states that the “main interpreter task shall be executed at least one complete application program cycle” within a specified time interval known as a context switch and a “system alarm flag will be set immediately if it failed to complete the entire application cycle.” After the time allowed for each “context,” the task scheduling OS restarts execution of its configured tasks (specified in the “Task Control Block” configuration list) from the beginning. Once all the other configured tasks have been executed, the application (or main interpreter) task executes repeatedly in a continuous loop until the end of the context time period. Diagnostic functions are provided by the OS to detect 1) whether the configured tasks fail to execute or 2) if the application task does not execute at least one complete loop during each context switch interval. The purpose of the first diagnostics is to detect hung execution of the system processor. The purpose of the second diagnostic is to detect interrupted or incomplete execution of the application task. Because the application task is executed last in the sequence of execution (albeit multiple times in a nominal configuration) for the time interval between context switches, it is necessary to confirm that the requirement for execution of at least one complete loop within each context interval is satisfied in order to have confidence in claims of deterministic and reliable performance.

The audit team made the following observations:

- Requirement 6 for the system processor (SC firmware) in RS901-000-37 Rev. E states that the firmware "shall provide sanity and watchdog checking, mailbox checking of the subordinate processors, and loop checking of the Equation Interpreter." While the requirement for loop checking explicitly addresses the diagnostic functionality to detect hung or failed execution of the application task, the HFC staff pointed out the implicit coverage of the "complete at least one loop during each context switch" diagnostic functionality.
- The forward trace through the HFC-6000 documents was conducted using the requirements traceability matrix contained in RR901-000-31 Rev. E. The referenced design descriptions are contained in DS001-000-08, "Redundancy and Failover Mechanism Component Design Specification," Sections 2.4 and 4.2 and DS901-000-01, "HFC-SBC06-DPM06 Module Detailed Design Specification," Section 2.4.1.2. These design description sections address controller failure detection mechanisms, controller failure detection, and control of the watchdog timer, respectively. While a loop counter is described to identify failure of the system processor to complete its software tasks, in particular the application task, the mechanism for detecting failure to execute at least one complete loop is not described. HFC staff described the setup, initialization, and maintenance of a loop check variable to detect the failure to execute at least one complete loop during the discussions associated with this thread. This variable is incremented only for complete passes through the application program. When a context switch occurs, the utility task that monitors flags and variables calls a function to evaluate the variable and reset it to a predetermined value. If the variable has not been properly incremented (i.e., it does not exceed a set value), a condition flag is set to indicate that the application has not been executed at least one complete loop since the last context switch. This flag can be used to support an event counter, provide notification to the operator, or trigger a recovery action. The use of this flag would be an application-specific review item.
- The relevant source code files and the associated source code review documents (SR001-000-085, SR001-000-015, and SR001-000-076, respectively) were provided to the audit team for review. With the guidance of HFC staff, the relevant functionality was located in the source code. For the first selected function, the source code review shows the relevant function calls from a table. For the second selected function, the source code review shows the utility function table and mailbox routines that include the functionality to set a status flag based on the value of a variable and then reset the variable. For third selected function, the source code review shows functionality to increment a variable for each loop completion. Both the second and third functions chosen for source code review explicitly show treatment of the loop counter variable (i.e., loop completion) but not the loop check variable (execution of at least one complete loop per context switch interval). This observed condition appears to result from the practical limitation on the level of detail shown in the flow diagrams for each module. No anomalies were found.
- The prototype tests for the HFC-SBC06/DPM06 modules and the Operability tests for the ERD111 qualification program were identified in RR901-000-31 Rev. E for the testing of the sanity and watchdog checking, mailbox checking, and loop checking functionalities. The prototype test procedure is documented in TS901-000-02 Rev. B. Sections 5.4, Power-up Test, and 5.5, EPROM, FLASH, and RAM Test, were identified as providing validation of these checking functions. Basically, processor initialization or memory failures during these

tests result in failover between primary and secondary processor so the detection functionality is considered to be validated. However, these tests do not provide active confirmation of the diagnostics. The Operability test procedure is documented in TP0402 Rev. E. Section 4.7, Failover Operability Test, was identified as the relevant test. The procedural steps for this test involve triggering failover by powering off cards or pushing the manual failover button. It is noted that these test procedures do not address the detection of a failure to execute at least one complete loop per context switch. The HFC staff described a test method they have used in which a configurable subloop is introduced as part of the application program for the test. By varying the parameters for the subloop, the execution time for the application can be adjusted so that it takes longer than the configured context interval to execute a complete application loop. Documentation of this test method was not reviewed. However, HFC staff identified TN901-000-09 Rev. A, which is an addendum to TP0402 Rev. F, as containing information on the demonstration of the failure of an application to complete execution at least once. To confirm the cited claim from the topical report (see above), definitive evidence should be provided by HFC that this or another test was used to validate the implicit requirement regarding checking for failure to execute at least one complete application program cycle (loop) within each context interval.

As a follow-up action to this thread, the HFC response to the RAI questions concerning deterministic performance, specifically Question 133 on validation testing for this particular diagnostic capability, should provide evidence of the specific tests performed to demonstrate the capability to detect a failure to complete at least one application program cycle in a context interval.

8) Audit of inter-processor messaging capability – The audit team initiated a thread audit addressing Universal Communications Protocol (UCP) message usage for online operation of a HFC-6000 controller. Because of time constraints on the final day of the audit, this thread could not be completed. The audit consisted of specifying the functionality to be traced and identifying the high-level requirement. Specific design components were not identified to proceed with review.

Docketed material from HFC (DS002-000-01 Rev. C) states that peer-to-peer communication between nodes on the C-Link network is not used for nuclear safety applications. Thus, UCP messages would only be used for internal (i.e., processor-to-processor) communication within HFC-6000 controller modules. On the final day of the audit, the HFC staff was asked to identify a sample inter-processor UCP message for review. The HFC staff identified equalization of the Secondary controller to the Primary controller as an example in which UCP messaging internal to an HFC-6000 controller node is used. Specifically, the system processor (SC firmware) of the Secondary controller instructs the ICL processor (SAP firmware) to update its I/O Table data using the current configuration stored in memory, which has been updated during the equalization process. The updated controller module design specification, MS901-000-01 Rev. F (Rev. C is docketed), provides a high level discussion of UCP message handling for the HFC-6000 controller module. Other than noting the UCP messaging for a Special Request task, the HFC staff did not identify any particular message tags (MTAGs) from DS002-000-03 Rev. B, “UCP Protocol Component Design Specification.” The MTAGs specify tasks to be activated in response to a message. However, the description in the component design specification for the

UCP tends to focus on external messaging, which should only occur with the controller in an offline (i.e., out of service) configuration. Regarding requirements for UCP messages, Requirement 8 for the SC firmware in RS901-000-37 Rev. E states the firmware shall support UCP messaging. However, the HFC staff was not able to identify requirements documentation for a specific UCP message in the time available.

As a follow-up to the discussion on UCP messages, the HFC response to the RAI Question 137 on the usage and types of UCP messages internal to an HFC-6000 node should discuss the specific requirements that are the basis for the messages and the means by which the messaging functionality was validated.

9) Audit of HFC-6000 function blocks – HFC-6000 CQ4 function blocks were selected at random for performing a thread audit for two functions. Each track of this audit consisted of a backward trace through the design and requirements documentation to identify a specific requirement for the function, followed by a forward trace through the design documents, source code, source code review, and test documentation.

The CQ4 block library provides modular software components that form the basis for constructing control algorithms to implement an application. For the first trace, the Median Signal Select (MSL) block was selected. The MSL selects the median value from as many as eight inputs. For the second trace, the Digital High Alarm (DHA) block was selected. The DHA sets a digital high-alarm flag if a selected input exceeds a specified alarm value.

The audit team made the following observations for the first trace:

- The MSL block is identified in Section 2, Table 1 of DS001-000-03 Rev. C, “HFC Control System Components CQ4 Blocks” (Rev. B is docketed). The corresponding requirements are documented in RS901-000-37, Appendix 20, Rev. B. Requirement 3e Items 1-9 identify specific capabilities of the block. Item 3 references the common requirements for the antiwindup (ATW) functionality.
- The forward trace through the HFC-6000 documents was conducted using the requirements traceability matrix contained in RR901-000-31, Attachment A, Appendix 20, Rev. A. In DS001-000-03, Appendix 20, Rev. A, a description of the MSL block is given in section 2.3.2. The ATW functionality is described in Section 4.1 of DS001-000-03 Rev. C. The source code file (XX4QMSL.P10) and source code review document (SR001-000-042) were provided to the audit team for review. The appropriate identification of the software module was documented and the function was adequately described in the source code review. No anomalies were found.
- The test documentation to validate the MSL requirements are satisfied is provided by ATP0402 Rev. D, “HFC-6000 Control System ERD111 – Control System Qualification Project Application Software Object Test Plan,” and TS901-000-22 Rev. B, “HFC-6000 Control System ERD111 – Control System Qualification Project Baseline Testing Summary Report.” The specific procedural steps relevant to demonstrating the functionality of the MSL with ATW processing is covered by Cases 8-11 in Table A16. It was noted that the test involved the High Signal Select block but the HFC staff stated that the same code used by

the HSL block to provide ATW processing is identical to that used for the MSL block. No anomalies are reported in the testing summary.

The audit team made the following observations for the second trace:

- The DHA block is identified in Section 2, Table 1 of DS001-000-03 Rev. C. The corresponding requirements are documented in RS901-000-37, Appendix 10, Rev. A. Requirement 3e regarding the provision of a uniform block structure for configuration and dynamic variables was selected for a forward trace.
- The forward trace through the HFC-6000 documents was conducted using the requirements traceability matrix contained in RR901-000-31, Attachment A, Appendix 10, Rev. A. Table 2 of DS001-000-03 Rev. C provides the description of the uniform Block Data Structure. The source code file (XX4QDHA.P10) and source code review document (SR001-000-031) were provided to the audit team for review. The appropriate identification of the software module was documented. Since the block data structure is common for the CQ4 blocks, the structure is not specifically described in the source code review. No anomalies were found.
- The test documentation to validate this requirement is satisfied is provided by ATP0402 Rev. D and TS901-000-22 Rev. B. The specific procedural step relevant to demonstrating that a uniform block data structure is provided is Step 1 of Section 3.1.11. This action involves opening a data block, which displays the data structure. No anomalies are reported in the testing summary.

The thread audit for these two function blocks was performed as a follow-up action to an open item from the first regulatory audit at HFC regarding incomplete software requirements for the HFC PDS. During the previous audit, it was determined that requirements for the HFC-6000 CQ4 blocks had not been documented. The audit finding was documented within Thread #2 in the Audit Report for the regulatory audit conducted in October 2009. HFC has been working to resolve the open item on requirements and these traces provided an opportunity to confirm that this issue is being effectively addressed. The revised requirements documentation and requirements traceability matrix can support the HFC response to the RAI questions on software dedication, specifically Questions 156 and 157 on the documentation of software requirements and the completeness of the software requirements specification, respectively.

10) Audit of test records and supporting data for HFC-6000 qualification testing – For this thread, specific tests were selected from the qualification test records for the HFC-6000 Control System ERD111 – Control System Qualification Project. The audit consisted of a forward trace from the test records to the data files corresponding to the selected tests.

During the conduct of HFC-6000 qualification tests, a Test Specimen Application Program (TSAP) was executed at selected times to generate performance data for the Test Specimen while under environment stress. Specifically, Operability and Burst of Events (BOE) functional test were executed. Data was captured from the Test Specimen and stored in Sequence of Event (SOE) files and Historical Archive System (HAS) files. The data in these files is time stamped and should be traceable based on the records for testing, which are documented as annotated test procedures.

The audit team made the following observations:

- For this thread, two tests were selected at random from the ERD111 Qualification Project. The environmental stress test at high temperature, high humidity conditions and the high frequency conducted susceptibility (CS114) test were selected. The first selected test was conducted from late afternoon on February 20, 2004, through late afternoon on February 22, 2004. Based on the test records, the predefined Operability and BOE functional tests were executed prior to 5:00 pm on February 22. The test records appear to indicate that the second selected test was conducted over the time interval from 2:00 pm to 4:30 pm on March 3, 2004. The Operability and BOE functional tests were executed during that time period. Thus, the associated data files should contain Test Specimen performance data while under stress.
- The audit team requested that HAS and SOE data be retrieved. Data corresponding to several Operability test functions (e.g., analog accuracy, digital response time, analog response time, communications operability) were stored in HAS files so the audit team selected one data set (analog response time) as the sample target for the HAS file trace. Data for the BOE test function was selected as the sample target for the SOE file trace. HAS and SOE data files corresponding to the late afternoon environmental stress test were identified by HFC staff. Time constraints prevented the HFC staff from retrieving the data for the CS114 test prior to the departure of the audit team. A subsequent e-mail correspondence to NRC from HFC confirmed that SOE data files from March 3, 2004, had been retrieved.
- During the performance of this thread audit, the audit team observed that handwritten notations of test execution times in the test record were not always be easily decipherable and that corrections were made in some instances to the logging of times for test phases. These conditions seemed to complicate the identification of what data files correspond to the selected tests. Nevertheless, the HFC staff appeared to be able to find the data given sufficient time.

As a follow-up action to this thread, HFC should consider adding sign offs and fill-in blocks (e.g., start times for test phases and/or data generation) on the test procedure/record documents for future qualification testing to ensure that sufficient information is recorded to clearly identify the data files and time-stamped data sets associated with specific tests and conditions.

Discussion of Life Cycle Security Measures

Regarding site physical protection, the facility in which the HFC-6000 development is performed is protected by a badge access system. The audit team observed that appropriate badging was required to access the facility without being granted access from someone already inside.

Regarding computing environment security, it was observed that the facility network on which the HFC-6000 software development is performed and the HFC-6000 component software versions are housed is protected by a firewall. In addition, the workstations on the HFC network are password protected. The audit team observed the password control.

Regarding software configuration management and version control / protection, the HFC-6000 component source code, compiled code, development tools and the compiler tools are all maintained within a software library tool. HFC-6000 software is controlled in Microsoft Visual SourceSafe 6.0, which has been in use by HFC since September 2006. Prior to that time, software for the HFC-6000 development was housed in a VAX code management system. The audit team observed software modules, organized by part number, in the SourceSafe tool. Each component module has all versions available for reference, as well as records of changes made to each software module. The team observed that even the change records from the previously used VAX code management system were now contained in the SourceSafe tool. The team observed a demonstration of the tool's capability to compare versions of a given module side-by-side, which facilitates review of changes between versions during code reviews. The SourceSafe tool also has the capability to grant varying access permissions to different users. The team observed the list of SourceSafe users and their respective access levels (i.e., read-write access or read-only access). The team also observed a compiled file, which contained both a "date of build" and checksum value with the code. It was noted that the firmware for the I/O cards are contained within a different software management tool. The team was shown the Serena Version Manager tool, which has equivalent capabilities to the SourceSafe tool. The Version Manager tool houses ICL module firmware.

The team observed the Test and Repair area at HFC where firmware can be installed onto HFC-6000 components. Any in-house firmware installations are performed on a stand-alone machine with software that is sent from document control. The team also observed the area of the facility where Factory Acceptance Tests are performed.

Discussion of Qualification Program Quality Assurance

Quality issues with the execution of the qualification program were discussed as part of the audit. These discussions focused on whether adequate procedures are in place to avoid deficiencies in future qualification testing such as those reported for the generic qualification of the HFC-6000 (i.e., the ERD111 project). One quality issue arose from the failure to ensure that the input modules used for the Test Specimen were calibrated. HFC described actions that have been taken to prevent a future occurrence of this situation. First, the calibration procedures supplied to I/O module vendors have been verified and are a point of emphasis. Second, a procedural step has been included in receipt inspection procedure (QPP 10.1) to ensure that calibration is confirmed at HFC site. The audit team observed that the test procedure step for confirming calibration as part of the qualification program (TP0401 Section 4.4.1 Item 4) was clearly was not accomplished during execution of the qualification program. The need to strengthen the procedure to avoid mistakes such as potential omissions of the action was discussed. One means of doing so would be to add active affirmation (e.g., sign-off line or box) on test procedures that calibration had in fact been confirmed. CR No. 2009-0624 was opened to ensure to procedures and processes are in place to address conditions that led to out-of-calibration modules being used for qualification testing.

Another observed quality issue involved the loss of data from the early phases of qualification testing. This data loss was the result of a software error in the data capture mechanism (i.e., code to record event data) of the Test System that affected the capability to store Sequence of

Events (SOE) data. It was noted that test procedure steps (e.g., TP0404, Section 4.1, Step 5) specify that the SOE and Historical Archive System data should be checked against the baseline performance. If this step had been performed, the software error would have been detected and the data loss could have been contained. HFC staff noted that the necessary interfaces to review the data files may not have been available at the testing laboratory. Nevertheless, it was observed that having procedural steps that cannot be executed could create a tendency to overlook or bypass steps and possibly compromise the rigor with which other steps in test procedures are followed. CR No. 2009-0630 was opened to review the qualification test procedures that are the baseline for future testing so that unnecessary or impractical steps are eliminated.

Apparent deviations in the qualification program that had been identified during the audit in October were discussed. Subsequently, a radiation exposure evaluation has been documented (RR901-000-36 Rev. A). The rationale for satisfying the requirements for low-frequency (magnetic field) radiated susceptibility test (RS101) is covered in the summary document. Testing radiated susceptibility for exposure to interference above 1 GHz is discussed in TN901-000-01 Rev. A, which is an addendum to TS901-000-25 Rev. B. Also, the rationale for addressing power hold up requirements from EPRI TR-107330 is covered in the summary document. Regarding the hold-up capability, HFC staff noted that current power supplies are now required to provide 40 ms hold up rather than the previous 20 ms capability.

Discussion of Configuration Management and Corrective Action Program

The audit team and HFC staff reviewed the status of corrective actions taken to resolve CRs generated in conjunction with the regulatory audit conducted in October 2009. Four CRs were identified in the audit report for the regulatory audit conducted in October. A condition report (CR No. 2009-0537) was opened to address platform component identification inconsistencies among docketed materials. Another condition report (CR No. 2009-0538) was initiated to resolve a deficiency or ambiguity in a work instruction that resulted in an instruction for information capture to not be followed in the documentation on at least one software module. CR No. 2009-0539 was opened as a result of an audit finding that function blocks had not been documented so the software requirement specification for PDS was incomplete. The fourth condition report (CR No. 2009-0540) was initiated because some documents had not been maintained to be consistent with revisions in other documents, some documents did not completely specify reference, (i.e., revision levels for cited documents were sometimes omitted), and some claims or evidence in some HFC documents are ambiguous and do not appear to be wholly consistent with information in supporting or higher level documents (e.g., the HFC-6000 topical report).

New CRs were generated as a result of the thread audits conducted during this site visit.

CR No. 2009-0623 was opened to address ambiguous wording for a requirement regarding what (e.g., status, data, software) is mirrored between Primary and Secondary controllers during the equalization process. RS901-000-37 Rev. E, Section 3.1.4.c states that the status of the application shall be mirrored from the primary controller to the secondary controller but there is no definitive indication of what constitutes "status." The firmware requirements will be reviewed by HFC staff to ensure that ambiguities are resolved.

CR No. 2009-0624 was opened to ensure that procedures and processes are in place and followed to address the conditions that led to out-of-calibration analog input modules being used in the Test Specimen during qualification testing.

CR No. 2009-0625 was opened to investigate whether prototype testing for the controller modules should be amended to either include an additional test or more clearly specify the relation between the test action and the items (i.e., functionality) under test. A review of the test procedure and test results by HFC staff is planned to confirm that the capability to transfer firmware code from PROM to FLASH was validated by testing.

CR No. 2009-0626 was opened to confirm that identified System Change Requests (SCRs) are taken to completion. Specifically, examples of SCRs that remain open were identified in which resolution of source code review findings about unused code has either not been executed or not been documented. SR002-000-28 identified unused code in module NICINT.A10. SCR 2596 was opened but has not been closed. A similar instance (i.e., SR001-000-060) was also identified.

CR No. 2009-0628 was opened to investigate the absence of prototype test results for the AI8M analog input module. In reviewing the documentation of prototype test results in TS002-000-01 Rev. A, test results were found for the other HFC I/O modules but not for the AI8M modules. HFC staff will confirm whether the test was performed for the AI8M module, locate the test findings and update the test summary documentation.

CR No. 2009-0630 was opened because review of qualification test procedures identified steps that could not be performed. Specifically, Step 5 of the Pre-Test procedure in TP0404 Rev. C "Environmental Stress Test Procedure" requires that Operability and Burst of Event pre-test data be compared against baseline limits. This activity could not be performed with the equipment at the Wyle test facilities so it is not feasible and should not be a required action for the test personnel. The HFC staff will review the test procedure to identify any other impractical or unnecessary steps, as determined from lessons learned during the generic qualification of the HFC-6000, and update the procedure for future use.

Discussion of Draft RAI Part 3

The draft RAI Part 3 was reviewed in discussions with HFC staff to ensure a common understanding of the topic, scope and intent of each question. The discussions enabled minor interpretation uncertainties to be resolved. HFC did not identify any sensitive information contained within RAI Part 3 that should be removed. Regarding specific items in which potential misunderstanding was addressed, question 151 on the means by which HFC ensures that unused or undocumented functionality does not introduce unintended or unexpected behavior was discussed to clarify the scope of the question. Specifically, it was clarified that the security provisions of Regulatory Guide 1.152, Revision 2, supplements the guidance in IEEE Std. 7-4.3.2 about the impact on the failure modes of computer-based safety systems to include security vulnerabilities. Thus, demonstrable one-to-one correspondence between requirements and design should address security features as well as performance features. Also, evidence from past usage should show that no (uncorrected) unintended behavior attributable to unused, unneeded, or undocumented functionality have affected performance or security. Based on these discussions, it was concluded by the audit team that Question 188 on operating experience data to support conclusions about the absence of undesired functions from the system code was covered within the scope of Question 151. Thus, Question 188 will be deleted from RAI Part 3. Question 149 on the coverage of parts in the availability analysis in RR901-000-04 Rev. A was also discussed to clarify the intent of the inquiry. The purpose of the question is to confirm that HFC adhered to the approach in MIL-HDBK-217F regarding the level of detail to be addressed in estimating component reliability. It was agreed that the wording for Question 149 would be revised to improve the clarity of the intent.

Based on the audit threads for security and system functions, two questions will be added to RAI Part 3. The first question will address the means for detecting or preventing the failure of the equalization of status and code between redundant primary and secondary controllers in configurations where the write capability to the onboard FLASH memory of an HFC-6000 controller module is disable (i.e., the write-protect switch is set). The second question will address configuration options that would result in initialization of HFC-6000 controller modules using code resident in flash memory rather than code burned into PROM.

The status of HFC responses to RAI Part 1 and RAI Part 2 was discussed. RAI Part 1 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML052850063) was dated September 28, 2005, and RAI Part 2 (ADAMS Accession No. ML062420465) was dated on August 29, 2006. The “HFC-6000 Topical Report Review (MC5380) Significant Issues Listing” (ADAMS Accession No. ML062420459) was included along with RAI Part 2. The HFC response to RAI Part 1, identified as HFCRAI-50928CONV Revision B (ADAMS Accession No. ML073390064), was submitted to NRC by letter on November 15, 2007. The HFC responses to RAI Part 2 and the Significant Issues Listing were included with the submission of PP901-000-01 Rev. C, “HFC-6000 Safety System Topical Report” (ADAMS Accession No. ML080780170). The discussion of these RAIs and responses focused on whether updated information was necessary and the need to ensure that the responses have been docketed. It was noted that RAI Part 3 addresses current information needs. To ensure consistency in documentation of the HFC-6000, HFC will review their responses and may provide a summary affirming the responses, indicating any modifications to the responses, and noting those questions and responses that are outside of the current scope of the HFC-6000 platform under review. NRC will ensure that the RAI responses are docketed.