REQUEST FOR ADDITIONAL INFORMATION (PART 3)

BY THE OFFICE OF NUCLEAR REACTOR REGULATION

HFC-6000 SAFETY SYSTEM TOPICAL REPORT, REVISION C

DOOSAN HF CONTROLS CORPORATION

PROJECT NO. 731

Part 3 of the RAI (Question Nos. 118–190) consists of the items given below.

118. HF Controls Corporation (HFC)-6000 Scope

To perform an adequate review of the suitability of the HFC-6000 for safety applications, it is necessary to confirm that the base platform under consideration can support the implementation of a safety function. Although it is understood that various configurations of the HFC-6000, in conjunction with additional components outside the platform scope, can be used to achieve the implementation of a safety system (e.g., RR901-000-01, Figure 2-1) and that the NRC will review these system architectures as part of a plant-specific application, it is important to understand how the base platform can be used for a safety function (e.g., how a single channel could be configured from data acquisition to trip condition determination through the output of partial trip results). Please provide a description of representative channel and system architectures based solely on the HFC-6000 platform within the scope of the TR.

119. HFC-6000 Scope

The assessment of the fault tolerance and reliability of the HFC-6000 requires a determination of whether available redundancy features are necessary for safety applications. For safety-related applications, will the HFC-6000 be implemented as redundant controllers (refer to, RAI Question No. 14), or should both redundant and non-redundant implementations be considered during the review of the HFC-6000 TR?

120. HFC-6000 Scope

Provide an updated list of the modules and components—both hardware and software—with all necessary identification (ID) information to uniquely specify the scope of the HFC-6000 platform included in the scope of the HFC-6000 TR (refer to, RAI Question Nos. 9 and 10).

121. HFC-6000 Scope

Please provide the documentation (such as design specification, test procedures, and reports) for the Jasper Electronics HML 601-5 power supply (or other rack-mounted power supply module selected for the HFC-6000 product line) (refer to, RAI Question No. 12).

122. HFC-6000 Scope

Section 4.2.1 of TS901-000-22 states that “the C-Link microprocessor section is also included on this module, but it is not part of this qualification program.” Section 5.1 states that the C-Link is “a second serial communication link not being qualified.” Section 5.1.3 states that “this Test C-Link function is not included in the scope of the qualification report.” Section 5.1.5 states that “the Test C-Link was not qualified as part of the qualification program.” Are the C-Link processor and connections to the C-Link NOT part of the base platform?

123. HFC-6000 Scope

Table 5.1 of TS901-000-22 identifies ECS-B232 as being among the “cards [that underwent] qualification process but will be dropped from consideration.” Is this module within the scope of the HFC-6000 TR?

124. HFC-6000 Components

Figure 5 of MS901-000-01, Revision E, depicts a “shared bus” and an “access control” block. The shared bus requires more explanation. As depicted, can the communications processors prevent the system processor from properly interacting with the access control block and, therefore, prevent the system processor from accessing the “public memory” or “dual-ported memory”?

125. HFC-6000 Components

DS901-000-01 states that the “SYS processor, which is a Pentium processor, has no built-in chip select, interrupt controller, I/O [input and output] ports or timer functions. The SBC6_CHSEL CPLD, in conjunction with the PBUSIF [process fieldbus interface] CPLD [complex programmable logic device], provides these functions.” Section 4.1.4 of RS901-000-37 describes the high-level function of each CPLD. Is there a more detailed definition of the requirements for each CPLD (e.g., specific requirements for bus arbitration for the PBUSIF CPLD that can be traced to specific design features or functions)?

126. HFC-6000 Components

The NRC staff position is that all programmable devices (e.g., CPLDs and field programmable gate arrays) are considered software and that they should be developed or dedicated in accordance with the same plans and procedures used for platform software development. What are the component development approach, heritage, and applicable operating history for the CPLD?

127. HFC-6000 Modes of Operation

The determination of when interactions such as software download are permitted depends upon a clear understanding of the terminology for modes of operation. The discussions of operation of redundant SBC06 modules in terms of primary controller mode and secondary controller mode seem clear and consistent. Several other modes of operation for the HFC-6000 are discussed throughout the docketed materials, but they are described inconsistently. For example, Section 7 of the TR refers to an online mode and an offline mode of operation. Section 4.1 of MS901-000-01 identifies “RUN,” “Offline,” “SIMULATION,” and “TEST” as operating modes set by dual inline package switches. DS001-000-06 identifies self-test and OSX88 multitasking operating modes for processors. DS901-000-01 states that there are two operating modes: (1) run mode (normal operation) and (2) self-test mode. What are the correct modes and proper terminology?

128. HFC-6000 Time Response

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

129. HFC-6000 Deterministic Performance

The execution sequence for the system processor indicates Group 0–7 tasks (TR, Figure 7-1). The defined tasks for controller processors (DS001-000-01, Table 1) only list Group 0, 4, 5, and 7 tasks. Please address the following items:

- Are there tasks defined for the other groups?
- The discussion of system processor software architecture mentions a Task 6 (TR, pdf Page 37). Is there a Task 6 or a task in Group 6?

130. HFC-6000 Deterministic Performance

The response to RAI No. 81 on the means for ensuring the correct resumption of the application task following the return from a context switch stated that the operating system saves “all current ‘Registers’ of [the] previous task into the software ‘Stack.’” What means are used to avoid stack overflow and to check for corrupted data?

131. HFC-6000 Deterministic Performance

Identify and describe the time-based routines that are envisioned for safety applications (DS001-000-01, Section 3.1.2 and Figure 5).

132. HFC-6000 Deterministic Performance

Several diagnostics appear to be based on error counts or time periods between events (e.g., the time period allowed during which the application task fails to complete its execution at least once before a context switch). If each of these are settable (i.e., counts or time periods) within an application, how is this variability taken into account in establishing the response time and deterministic performance of the HFC-6000?

133. HFC-6000 Deterministic Performance

What test is provided to validate the diagnostic that detects a failure to execute the application task at least once during a context switch cycle?

134. HFC-6000 communication

DS002-000-01 states that the dynamic database contains “important system status information and is broadcast by each node on the C-Link during its mastership periods.” For safety-related applications, what information or data from other C-Link nodes contained within the dynamic database does a receiving controller need or use (i.e., is any vital information transmitted across the C-Link)? Explain what functions would make information exchange between nodes necessary (refer to, RAI Question No. 22).

135. HFC-6000 Communication

DS002-000-01 states that the number of nodes for the C-Link and the sequence ID number for a specific node are preset by dual inline package switches. However, DS002-000-01 also stated that “all nodes update the Remote Status Table of all active nodes.” Please clarify this process and address the following items:

- Does this imply some degree of dynamic node definition so that a “deaf” node is deleted from the sequence?

- If a deaf node recovers, how does it get the other nodes to recognize it so that it can regain mastership of the token?

136. HFC-6000 Communication

The design safety discussion in the controller design specification (MS901-000-01) identified peer-to-peer (UCP) communication as a contributor to a potentially hazardous condition. Although DS002-000-01 and DS002-000-03 extensively describe the capability, HFC is excluding peer-to-peer UCP messaging across the C-Link from the scope of the review. In particular, Section 5.4 of DS002-000-01 shows broadcast communication only for nuclear safety applications versus broadcast and peer-to-peer communication for “normal” C-Link usage. Peer-to-peer communication is also indicated as not intended for nuclear safety applications. Please address the following items:

- How is peer-to-peer communication (UCP messaging across the C-Link) prohibited for nuclear safety applications?

- Can UCP messaging be disabled?

137. HFC-6000 Communication

The “Module Design Description” states that UCP messages are “mainly operator commands or inquiries from operator workstations and responses from the SBC06 System Controller to the operator workstations.” Section 2 of DS002-000-03 discusses UCP functionality as it relates to operator queries, not to interprocessor requests. Provide a description of the usage of UCP messages internal to an HFC-6000 node (i.e., among SBC06 processors or between Intercommunication Link (ICL) and input and output (I/O) board processors) and identify what messages are available for use.

138. HFC-6000 Communication

MS901-000-01 states, “A message event mechanism, with events passed between processors using Public Memory, is used by a processor in the HFC-SBC06 to notify another processor in the HFC-SBC06 that a UCP message has been placed in its respective message data store. Refer to DS001-000-001, Operating System Component Design Specification for details of the UCP message event mechanism.” Describe how UCP message events are handled.

139. HFC-6000 Communication

Clarify the terminology in Table 1 on “Defined Processor IDs” in DS002-000-03.

140. HFC-6000 Failure Modes and Effects

The determination of whether undetectable identifiable failures exist is significant in assessing the ability of a digital platform to comply with the single failure criterion of Institute of Electrical and Electronics Engineers (IEEE) Standard (Std.) 603. The “TR-107330 Requirements Traceability Matrix” of RR901-000-10 states that the HFC-6000 failure modes and effects analysis (FMEA) (RR901-000-01) identifies the need for runtime memory diagnostics to provide a means for detecting runtime memory bit failures. However, RR901-000-01 does not contain this finding. Please address the following items:

- Explain the inconsistency between the documents.
- Provide technical justification for the apparent determination that runtime memory bit errors are detectable and describe the means of detecting such failures.

141. HFC-6000 Failure Modes and Effects

The section in the TR that summarizes the FMEA states, “The existing HFC-6000 System design provides confidence that all failure conditions are detectable or that, for certain failures, the HFC-6000 System redundant components permit continued operation of critical system functions in the presence of automatic switchover.” Clarify the use of “or.” Please address the following items:

- Does this mean that there may be undetectable failures? What are they?
- How are these failures considered with respect to IEEE Std. 603, Clause 5.1?
- The TR further states, “The redundant architecture provides a mechanism for generating an alarm to notify the user that a failure exists.” Does this condition imply that a redundant controller configuration is necessary to support a safety application or simply that the preferred (but not required) configuration is necessary?

142. HFC-6000 Failure Modes and Effects

Section 8.2, “FMEA,” of the TR states, “HFC-6000 diagnostics are designed to detect most failures that were postulated for the FMEA.” What identifiable failures are undetectable? What failures require surveillance testing? What surveillance test detects each of these undetectable failures?

143. HFC-6000 Reliability and Availability

Failures in redundant and highly reliable systems are dominated by common-cause failures (CCFs). Without accounting for hardware CCFs, the availability of any redundant cabinet configuration will be greatly overestimated. Test, calibration, maintenance, or installation errors can cause simultaneous failures of redundant cabinet configurations. How were these addressed in the reliability and availability analysis? Please discuss how hardware CCFs are included in the availability assessments for redundant equipment and cabinet configurations.

144. HFC-6000 Reliability and Availability

MIL-HDBK-217F was used for reliability prediction of individual parts that have been used to build HFC-6000 modules. What factors were used to modify the base failure rate of the components because of stressors (e.g., temperature, electrical, and environment)?

145. HFC-6000 Reliability and Availability

The calculation of availability of redundant modules was based on the guidelines described in IEEE Std. 352-1975. Were any tests performed to measure the accuracy of the failure rate predictions?

146. HFC-6000 Reliability and Availability

The availability analysis assumed, in part, that the plant control system is in daily use and that failures would be detected within 1-day of their occurrence. It also assumed that spare parts are available to affect an immediate repair. These assumptions rely on the expectation that all equipment failures are announced or readily detectable. Several factors or considerations identified below can greatly influence the mean times to repair. Please address the following items:

- What if a normally “ON” discrete output fails “ON”?
- How does the model account for unannounced failures?
- How are failures treated that are only detectable by periodic surveillance, manual tests, or operator observation?
- What failures will be detected by observation of system behavior that are not detected and are not alarmed by self-diagnostics?
- How does the availability of the system account for faults that are not detectable by self-diagnostics or are not self-evident?

147. HFC-6000 Reliability and Availability

Relex® software was used to perform the MIL-HDBK-217F analysis on parts and assemblies of the HFC-6000 product line. What quality assurance (QA) program does Relex® follow (e.g., International Organization for Standardization (ISO) 9001)? Were hand calculations used to spot check the output from Relex®?

148. HFC-6000 Reliability and Availability

In calculating the availability, the failure rate of redundant components was determined by squaring the failure rate of a single component. The availability value of redundant components is then 1, which is the failure rate of redundant components. Thus, Tables 4 and 5 both show 100 percent availability values. CCFs will dominate the availability. Please discuss this item.

149. HFC-6000 Reliability and Availability

MIL-HDBK-217F (Pages 3-2 and 3-3) states. “The general procedure for determining a board level (or system level) failure rate is to sum individually calculated failure rates for each component. This summation is then added to a failure rate for the circuit board (which includes the effects of soldering parts to it) using Section 16, Interconnection Assemblies.” It also states, “For parts or wires soldered together (e.g., a jumper wire between two parts), the connections model appearing in Section 17 is used. Finally, the effects of connecting circuit boards together is accounted for by adding in a failure rate for each connector (Section 15 Connectors). The wire between connectors is assumed to have a zero failure rate.” To evaluate the results of the reliability and availability analysis, it is important to understand the completeness of the model used. Does Table 5 in RR901-000-04 account for all parts of the module or unit such as solder connections and connectors? Please discuss the extent of component coverage in the determination of the board level failure rate.

150. HFC Security

Regulatory Position 2.4.2 in Regulatory Guide 1.152, “Criteria for Digital Computers in Safety Systems of Nuclear Power Plants,” Revision 2, issued January 2006, addresses tampering with the developed system. Subcontractor suppliers assemble and configure HFC-6000 modules using software or firmware provided by HFC. What provisions are in place to ensure that the module vendor(s) do not intentionally or unintentionally modify or incorrectly install the software? How does HFC ensure that the correct, unmodified software was installed by the module vendor(s)?

151. HFC Security

The regulatory positions in Regulatory Guide 1.152, Revision 2, address the issue of unused, unneeded, or undocumented functionality. Given that the system software contains function blocks and features (e.g., peer-to-peer communication across the C-Link) that are not intended or necessary for safety applications, how does HFC ensure that this unused embedded functionality does not introduce unintended or unexpected failure modes?

152. HFC Quality Assurance

During the course of the first regulatory audit at the HFC facility (conducted from October 6 to October 9, 2009), some condition reports were generated to address issues identified in the thread audits. Please provide documentation of the condition reports and describe the remedial actions and resolutions that HFC accomplished through its corrective action program.

153. HFC Quality Assurance

As part of the assessment of the commercial-grade dedication (CGD) of preexisting software, the NRC must determine whether HFC followed its QA program under Appendix B, “Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants,” to Title 10 of the *Code of Federal Regulations* (10 CFR) Part 50, “Domestic Licensing of Production and Utilization Facilities,” in reconstituting the software requirements and design specifications. For design control, Appendix B specifies that independent verification must be conducted such that the “verifying or checking process shall be performed by individuals or groups other than those who performed the original design….” Section 8.4 (Page 8-12) of the TR states that “individuals or groups other than those that performed the original design review output documents.” In addition, in the response to RAI Question No. 1 describing the HFC QA program under Appendix B, Section 3, “Design Control,” states that “design outputs [must] be reviewed and approved. Design specifications are reviewed by an independent reviewer (someone in the same organization having no involvement in the design).” Please address the following items:

- Is this review activity different from that indicated on the title page of each design specification document (i.e., author, reviewer, and approver are identified)?

- If so, explain how these design documents are independently reviewed in accordance with the requirements of Appendix B to 10 CFR Part 50. Where are the independent reviews documented, and where are the reviewers identified?

- If not, what is the basis for using the authors of some design documents to review higher level or similar design documents (e.g., Jonathon Taylor is listed as the author for I/O module detailed design specifications DS901-000-04, DS901-000-07, DS901-000-08, and DS901-000-11; as the reviewer for I/O module design specification MS901-000-02 and for detailed design specifications DS901-000-02, DS901-000-03, and DS901-000-12; and as the reviewer for the general I/O module requirements specification 700901-06) or for using original authors to review subsequent revisions of design documents (e.g., B. Cain authored DS901-000-11 and subsequently reviewed Revision B; Jonathon Taylor authored the first five versions of RS901-000-01 and then was listed as the reviewer for Revision E)?

154. HFC Quality Assurance

Section 8.4 (Page 8-11) states, “To assure that the documentation reflects current design, the QA Program includes procedures and methods that ensured the correctness and completeness of the documentation at the end of each phase of the HFC-6000 design project.” Additionally, Quality Process Procedure (QPP) 1.2 states that the verification and validation (V&V) teams are responsible for “a full independent evaluation of a nuclear safety system’s documentation and test results by reviewing for omissions, inconsistencies, inaccuracies and errors of omission/irrelevant requirements with emphasis on the system performance requirements and design specifications.” Please address the following items:

- Given that the scope of the HFC-6000 platform proposed for review has changed from the initial submission in PP901-000-01, Revision A, why were the design documents not revised to reflect the current scope and to correct terminology (e.g., QIO versus ICL, CPC versus C-Link processor, and PCC versus ICL processor) and system description inconsistencies?

- Does HFC plan to apply these QA procedures to maintain the complete design document set for a safety-related version of the platform?

155. HFC Quality Assurance

In the response to RAI Question No. 1 describing the HFC QA program under Appendix B to 10 CFR Part 50, Section 2, “QA Program,” states, “Competency requirements are completed for Engineering, QC, Test and Production personnel for quality-affecting activities and work.” However, QPP 2.6, “Qualification of Test Personnel,” Revision B, is designated as cancelled.

Please address the following items:

- What is the rationale for canceling this procedure?
- What quality process controls ensure that test personnel are qualified to discharge their assignment?

156. HFC-6000 Software Dedication

Section 10.1.1.2 of the TR states, "Documents available for the HFC-6000 software are as follows: … • Software Requirements Specification." It also states that the verification of software documentation involved improvements to bring them to a suitable standard. It further states that the "SRS contains a complete specification for all system functions including their data structures and all relationships between those structures." The ongoing review of the TR and its supplemental documents has found that system and module requirements are identified in RS901-000-01, RS901-000-37, 700901-04, 700901-05, and 700901-06. Please address the following items:

- Is there a single document containing the complete software requirements specification?
- If not, specify the documents that provide the complete set of software requirements.
- A review of RS901-000-01, RS901-000-37, 700901-04, 700901-05, and 700901-06 found that software descriptions, instead of clearly identified requirements, are provided in several instances. Clearly identify the requirements within these documents to differentiate them from descriptions of software features.

157. HFC-6000 Software Dedication

In discussing compliance with Regulatory Guide 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," issued September 1997, in Section 8.5.2, the TR claims that the software requirements are "traceable, accurate, complete, consistent, ranked for importance or stability, verifiable, and modifiable." Please address the following items:

- Is there a documented assessment that verifies these claims?
- An evaluation of the requirements provided in RS901-000-01, RS901-000-37, and 700901-05 revealed that not all functions and operations provided by the system software have requirements. In particular, the requirements for the CQ4 function blocks are apparently not included. Provide a complete software requirements specification for the predeveloped software.
- Are all of the processing routines and instructions, capabilities of the software components, modules and files, and operating system functions traceable to software requirements?

158. HFC-6000 Software Dedication

A complete description of the software and firmware that has been dedicated for the HFC-6000 platform is needed to facilitate an assessment of the software dedication evidence. The response to RAI Question No. 26 states that the "document DS-001-000-07, 'Job Configuration Design Specification,' discusses the three firmware programs in detail." Please provide that document for review.

159. HFC-6000 Software Dedication

To assess the relevance of the ECS-1200 operating history as supporting evidence for the CDG of the predeveloped software (PDS), the significance of the difference between the two product lines (i.e., the ECS-1200 and HFC-6000) must be determined. Section 10.1.4.5 of the TR states, "HFC-6000 hardware and software are essentially identical to the existing ECS-1200 product line with the exception of changes in the form factor." Those changes include the "physical repackaging of current ECS-1200 components on HFC-6000 boards, redesign of the chassis for easier access for maintenance and improved seismic rigidity, and improved I/O termination connections for ease of installations." Section 10.1.2.1 states that the "form factor change includes rack size, connectors and packaging of field wires termination. The form factor change does not require changes to the existing operating system, communications and I/O software and this allows the software to be classified as PDS." Please address the following items:

- Please provide a detailed description of the differences associated with the "form factor" change.
- Are bus communications implemented differently for the two product lines?
- Are there differences in the logic or implementation for bus management functionality provided by onboard CPLDs?

160. HFC-6000 Software Dedication

Table 10-5 in Section 10.1.4.8 of the TR identifies the relevant defects of the ECS-1200. Why was the communication failure event at Ulchin Nuclear Power Plant, Unit 5 (Ji, International Atomic Energy Agency Technical Meeting on Implementing and Licensing Digital Instrumentation and Control Systems and Equipment in Nuclear Power Plants, November 2005) not discussed in this section or in the table?

161. HFC-6000 Software Dedication

A key element of the CGD process is the definition and evaluation of critical characteristics. Of the dependability characteristics, "built-in quality" addresses less quantifiable elements related to the development process and accompanying documentation than the other characteristics do. Electric Power Research Institute (EPRI) TR-106439 identifies the review of vendor processes and documentation as a method of verification (associated with CGD Methods 2 or 3) for assessing the built-in quality. These processes and documentation include (1) design, development, and verification processes; (2) QA program and practices; and (3) V&V program and practices. Acceptance criteria include evidence that the vendor maintains a QA program that is generally in compliance with a recognized standard and that it used a process for legacy software that addresses essentially the same elements as the current QA process.

The verification methods include a review of the evolution of vendor procedures and practices for software development, V&V, testing, and a determination of the degree to which the QA program and software development process were applied. The EPRI guidance notes that the preparation of supplemental documentation may be necessary. In the commercial-grade software evaluation documentation that HFC provided in the supplemental submission, the cited acceptance criterion is the existence of a nuclear quality assurance (NQA)-1 program, and the method of verification identifies records of internal and external audits, source code review records, source code test reports, and prototype test reports as evidence. In its response to NRC Request No. 1i, dated September 16, 2008, HFC stated that Forney, Inc., developed an NQA program based on NQA-1 in the late 1980s and early 1990s and that Forney, Inc., achieved ISO-9000 certification. To what extent was the standards-consistent program applied in the development of the PDS? (For example, was the PDS developed before the establishment of the program, and were there significant modifications and continued development of the PDS from the late 1980s forward?) Identify and describe key elements (i.e., life-cycle approach, planning, V&V, reviews, and testing) of the Forney, Inc., NQA-1-based program that were applied in the development of the PDS and identify what documentation exists.

162. HFC-6000 Software Dedication

Clarify the relationship between the HFC software QA plans and procedures for maintaining predeveloped software and the Branch Technical Position (BTP) 7-14, “Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems,” acceptance criteria for software life-cycle documentation. Explain the equivalence (e.g., provide a mapping) between the HFC QA program and BTP 7-14.

163. Qualification

RR901-000-10, Revision A, identifies the compliance status of many items as “in progress.” What is the current status of each of these items?

164. Qualification

In contrast to stated conformance with EPRI TR-107330 requirements, the qualification results do not demonstrate a comprehensive environmental stress withstand capability and programmable logic controller performance in compliance with the specified acceptance criteria. Please address the following items:

- Explain how deviations from the requirements of EPRI TR-107330 are justified and describe how quality issues with the execution of the test program have been addressed.

- Define the performance and environmental stress envelopes as supported by test results.

- Justify the omission of tests and analyses (specifically, the RS101 electromagnetic susceptibility test, the failure to scan test within the operability test sequence, and a radiation withstand analysis).

165. Qualification

Based on the discussion in EPRI TR-107330, scan time is the time required to complete input acquisition, execute the control logic, and complete command output. Appendix D of TN0401 states, "Failure To Complete Scan—Not applicable for the HFC-6000 system." Please address the following items:

- Is this not equivalent to failure to complete Task 7 at least once between context switches?

- Why is this test not applicable for the operability tests?

166. Qualification

Section 4.3.6.3 of EPRI TR-107330 states, "Evaluations, which provide confidence that none of the components in the programmable logic controller platform are degraded by exposure to the radiation level given in the previous section, are adequate for establishing radiation withstand capability." Section 2.5 of HFC TN0401 states, "Paragraph 4.3.6.3 of the EPRI standard identifies radiation exposure as an insignificant factor for aging of the control system. The evaluation for the system to operate reliably in the radiation level of the normal environment is deemed sufficient, so no specific test will be conducted for radiation exposure." Was any evaluation of radiation susceptibility conducted, and, if so, where is it documented?

167. Qualification

Section 5.2.D of EPRI TR-107330 requires initial calibration. Appendix D.3 to TN0401 identifies the following as a step in the prequalification test sequence:

> Initial Calibration. The calibration of analog input and analog output card will be verified and documented before completion of the prequalification phase of testing has been completed. This activity may be conducted concurrently with overall system setup and checkout.

The "Integration Procedure" description also states, "Initial calibration of the analog input and output modules will be accomplished during this phase of system configuration based on standard calibration procedures for each module type." Test procedure TP0401 specifies prerequisites for I/O functional testing, which includes the requirement to verify that analog I/O modules "have been tested, calibrated and/or configured per the applicable test procedure…." Why were AI modules for the test specimen out of calibration during qualification testing?

168. Qualification

Section 9.3.2.1.1 of the TR states, "During the initial baseline tests, some of the SOE [sequence of events] test data for the Operability Test and Prudency Test was overwritten during the test period due to a fault in the test data recording process.... Subsequent Operability and Prudency test results were used to supplement the lost data and verify the acceptability of the SOE test results." However, Step 5 of Section 4.1 in the test procedures TP0404, TP0406, TP0407, TP0409, and TP0411 requires the following actions, as stated: "Generate the test report files for Operability and the Burst of Events tests. Verify that all test results are within acceptable limits indicated in TP0402 and TP0403." Please address the following items:

- If Step 5 was executed as written, how was the software bug that caused the SOE log data record to be overwritten not detected during the execution of the first of these tests?

- What corrective action has been taken or is planned to ensure that procedural steps such as this one are performed as intended?

169. Qualification

Was the tester or simulator running the HFC plant automated tester application calibrated before the qualification testing of the test specimen? Was calibration confirmed and maintained during testing?

170. Qualification

Appendix A.15 of TS901-000-22 states, "The results of single power supply testing described below demonstrated that one power supply is sufficient to run the system without interruption in the event of the loss of the redundant supply. However, a single power supply is not required to sustain controller operation during a power interruption when redundant power supplies are provided." These statements are unclear. Please clarify.

171. Qualification

Appendix A.15 of TS901-000-22 states, "It is clear that the system controller suffered a partial reset." What is a partial reset?

172. Qualification

Section 6.4.2 of TS901-000-22 discusses anomalies in the qualification test findings for baseline performance. In particular, the discussion of analog response time identifies the 100 sample moving average algorithm for the AI16F module as the likely cause of the inability to satisfy the EPRI TR-107330 acceptance criteria. The more detailed discussion in Appendix A.8 also identifies the input filter as a contributing factor. The test summary states, "Reducing the response time to the 100 ms acceptance criterion would require modifications to both the input filter and the 100 sample moving average algorithm. This configuration of the card is available where the 100 ms response time is application critical." Please address the following items:

- Have the postulated causes of the excessive response time been confirmed?

- Have configuration changes to satisfy the acceptance criteria been demonstrated, and do these changes constitute a new AI module?

- Has the impact of changing the 100 sample moving average algorithm on input stability and other relevant characteristics been evaluated?

173. Digital Security—Design

The topical report states that the proprietary nature of the firmware significantly reduces/eliminates the system's vulnerability to attack. While the proprietary nature of the system significantly reduces the likelihood that computer viruses have been specifically written to attack this particular system, it does not guarantee that the system could not be compromised (either intentionally or unintentionally) if someone or some other device were able to logically access the system. For the developed system, what potential security vulnerabilities are resident in the system

(i.e., those system properties that would need to be addressed by either inherent system security features or security protections afforded by the overall architecture that the system is placed within)? (Reference Regulatory Position 2.1 in Regulatory Guide 1.152, Revision 2.)

174. Digital Security—Design

Between the review of docketed information and the findings of audits, it is clear that the system has the capability to resynchronize its firmware from programmable read only memory (PROM) to Flash and mirror application software from primary to secondary controllers. However, it is not clear that there are capabilities that are always set to occur (see RAI Questions 188 and 189). What are the (built-in) security design features (for which there is officially docketed information) that HFC wishes to have reviewed as part of this evaluation? (Note that a licensee may later supplement these protections based upon the application-specific environment.) (Reference Regulatory Position 2.1 in Regulatory Guide 1.152, Revision 2.)

175. Digital Security—Design

Where do the requirements exist (i.e., what is the controlled reference) for the security design features in the system? (Reference Regulatory Position 2.2.1 in Regulatory Guide 1.152, Revision 2.)

176. Digital Security—Design

Where are the approved message formats and data definitions defined (i.e., what is the controlled reference)? Are any messages developed on an application-specific basis? (Reference Regulatory Position 2.2.1 in Regulatory Guide 1.152, Revision 2.)

177. Digital Security—Design

Where is the installation process (i.e., at a licensee's facility) for the system defined? What are the security acceptance criteria for post-installation (i.e., those specific to ensuring that the system was not tampered with between shipment and installation)? (Reference Regulatory Position 2.2.1 in Regulatory Guide 1.152, Revision 2.)

178. Digital Security—Design

What reference documents the V&V process for development covered the security requirements? (Reference Regulatory Position 2.2.1 in Regulatory Guide 1.152, Revision 2.)

179. Digital Security—Design

What commercial off-the-shelf or predeveloped codes or tools are used on the platform? What *requirements* were imposed on the use of those tools and codes to protect them for any potential vulnerabilities? [Note: the implementation of any requirements may be addressed in RAI Question No. 181.] (Reference Regulatory Position 2.2.1 in Regulatory Guide 1.152, Revision 2.)

180. Digital Security—Design

What logical access control provisions (that may not have been described in response to RAI Question No. 174) are included in the platform design? (Reference Regulatory Position 2.3.1 in Regulatory Guide 1.152, Revision 2.)

181. Digital Security—Design

If a commercial off-the-shelf or predeveloped code was used on the platform, how is the overall system protected (via design) from any potential vulnerabilities in that code being exploited? (Reference Regulatory Position 2.3.1 in Regulatory Guide 1.152, Revision 2.)

182. Digital Security—Design

What processes in software development ensure that the security design features are/were incorporated into the implemented system? (Reference Regulatory Position 2.4.1 in Regulatory Guide 1.152, Revision 2.)

183. Digital Security—Design

What software development test processes or procedures were used to test security features? Are these procedures generic to the platform? Or are the test procedures application specific? (Reference Regulatory Position 2.5.1 in Regulatory Guide 1.152, Revision 2.)

184. Digital Security—Development

For the development life-cycle phases of the system (i.e., requirements through factory test), what vulnerabilities were identified that could have presented the opportunity for someone to tamper (intentionally or unintentionally) with the system to delete needed code or to introduce unwanted code? (Reference Regulatory Position 2.1 in Regulatory Guide 1.152, Revision 2.)

185. Digital Security—Development (Requirements)

For the vulnerabilities identified (in response to RAI Question No. 184) that could impact the system’s requirements development phase, what measures were taken to mitigate tampering with the system development via any of those vulnerabilities? (Reference Regulatory Position 2.2.2 in Regulatory Guide 1.152, Revision 2.)

186. Digital Security—Development (Design)

For the vulnerabilities identified (in response to RAI Question No. 184) that could impact the system’s design phase, what measures were taken to mitigate tampering with the system development via any of those vulnerabilities? (Reference Regulatory Position 2.3.2 in Regulatory Guide 1.152, Revision 2.)

187. Digital Security—Development (Implementation)

For the vulnerabilities identified (in response to RAI Question No. 184) that could impact the system’s implementation phase (i.e., the period from initial coding to installation of software onto testable hardware), what measures were taken to mitigate tampering with the system development via any of those vulnerabilities? Please address the following items:

- physical protection
- logical protection
- control of code during development
- protection of any codes/tools used in development
- verification of the code version(s)
- measures taken to ensure that there are no unneeded functions
- any checks performed during development

(Reference Regulatory Position 2.4.2 in Regulatory Guide 1.152, Revision 2.)

188. Digital Security—Development (Test)

For the vulnerabilities identified (in response to RAI Question No. 184) that could impact the system's test phase, what measures were taken to mitigate tampering with the system development via any of those vulnerabilities? How was the test environment protected? (Reference Regulatory Position 2.5.2 in Regulatory Guide 1.152, Revision 2.)

189. HFC-6000 Diagnostics

Based on the ongoing review of docketed information and discussions during on-site audits at HFC facilities, it is understood that the position of the write protect switch determines whether application software can be written into the onboard FLASH memory of a SBC06 controller. Furthermore, if write protect is selected for a controller that is returned to service with a primary controller already active, this configuration will prevent successful completion of the equalization for the startup of the secondary controller (i.e., the capability to write the primary controller application software into the FLASH memory of the secondary controller to equalize the application software between the two controllers is disabled). This situation could result in operation of the redundant controllers with different application software. What is HFC's intent for deployment of this system – i.e., do the operational/maintenance instructions that a licensee would receive address the setting of this switch to enable this function? Or is the setting of this switch an application-specific item? What diagnostic capabilities are provided to detect this condition and what action or alarm results following such detection?

190. HFC-6000 Diagnostics

Based on review of the topical review, review of requirements documentation and discussions during on-site audits, the staff understands that the capability exists for the device firmware to be written from PROM to Flash memory upon initialization/restart. However, this capability appears to only be enabled if particular jumper setting(s) are set "on". One of the design documents (MS901-000-01, "HFC-SBC06-DPM06 Boards Module Design Specification, System Controller," Revision E, March 27, 2009) contained instructions on firmware installation that appeared to instruct that the jumper be removed when the installation was complete (thereby, disabling the PROM to Flash synchronization upon subsequent restarts of the system). What is HFC's intent for deployment of this system – i.e., do the operational/maintenance instructions that a licensee would receive address the setting of the jumper(s) to enable this function? Or is the setting of this switch an application-specific item?