FOR INFORMATION ONLY

REQUEST FOR ADDITIONAL INFORMATION (PART 1)

BY THE OFFICE OF NUCLEAR REACTOR REGULATION

HFC-6000 SAFETY SYSTEM TOPICAL REPORT, REVISION C

DOOSAN HF CONTROLS CORPORATION

PROJECT NO. 731

Part 1 of the RAI (Question Nos. 1–59) consists of the items given below

1. Please provide a complete description of your Appendix B Quality Assurance program.

2. Institute of Electric and Electrical Engineers (IEEE) 603, "Criteria for Safety Systems for Nuclear Power Generating Stations," required by Title 10 of *Code of Federal Regulations* Part 50.55a, "Codes and standards," subsection (h), states, in Section 5.6.1, on independence between redundant portions of a safety system, that "Redundant portions of a safety system provided for a safety function shall be independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any design basis event requiring that safety function." In the same standard, a "Channel" is defined as: An arrangement of components and modules as required to generate a single protective action signal when required by a generating station condition. A channel loses its identity where single protective action signals are combined. Show how these requirements are met in the proposed system.

3. Application of the proposed system will result in changes to the setpoint uncertainty allowances for the associated safety functions. It may be expected that the modified instrument channels will exhibit reduced uncertainty and reduced drift as compared with the existing analog channels, and that the operating margins may therefore be increased. It may also be expected that the expected deviations over the calibration interval would be reduced, resulting in a need for tighter deviation limits. Please specify the uncertainty and drift considerations applicable to the analog input modules, and show how those data were determined.

4. There are several references to "broadcast" communications and to "tokens" used for communications control. But most if not all of the associated communications schemes appear to be ethernet, which is inherently bidirectional and which does not use tokens. Please clarify or explain these apparently conflicting concepts.

5. Electric Power Research Institute (EPRI) topical report (TR)-107330 was specifically written to provide guidance for PLC based systems. The staff's safety evaluation of this report explicitly cautions potential users, stating "Because the term 'PLC' is used by various manufacturers to label digital equipment with capabilities from relatively simple to very complex, care should be exercised to assure that TR-107330 is not used to attempt to qualify equipment outside its scope." HFC-6000 is much more complex than a typical PLC. Use of TR-107330 in connection with HFC-6000 therefore does not appear to be appropriate. Please justify the use of TR-107330, or alternatively justify the use of other guidance such as EPRI TR-106439, which provides guidelines for the dedication of commercial grade digital equipment.

6. It appears, from the system description, that the Intercommunication Link (ICL), an RE-485 serial network, is used to carry sensor input signals from the individual input/output (I/O) boards to the SBC06 system controller, and to carry trip signals from the system controller. In the past, digital systems approved by the staff have had both sensors and trip signals hardwired, and have not used a network for this type of data transfer. The hardwired methods approved in the past have provided demonstrable deterministic behavior, and it does not appear that the ICL has a similar degree of deterministic behavior. The use of a communications method such as the ICL needs to be particularly justified. Please provide sufficient information to demonstrate the following:

   A. How the ICL operates.
   B. The timing and control of the ICL.
   C. How deterministic behavior is maintained.
   D. The various failure modes of the ICL and how these failures are detected.
   E. How the priority of signals is determined.
   F. Why use of a network architecture such as the ICL is suitable for safety-related use.
   G. Why this added system complexity adds a corresponding safety value.
   H. Maximum signal transmission delay.
      – Also, show how this maximum delay is computed and why it is acceptable.
   I. Show that the ICL communication process cannot interfere with the operation of the primary function processor

7. For each type and use of processor, the SYS microprocessor, the ICL microprocessor, the C-Link microprocessor, the I/O modules microprocessor, the HMI microprocessor, and any other microprocessor used in the HFC-6000 system, please provide the following information:

   A. Complete hardware description, including any support chip set.
   B. The commercial grade dedication process and vendor acceptance documentation.
   C. The part 21 reporting responsibility for the dedicated hardware.
   D. Source and qualification of processor BIOS.
   E. Software requirements specifications.
   F. Software architecture description.
   G. Software design specifications.
   H. Verification and validation analysis.
   I. Test Procedures and test results.
   J. Failure Modes and Effects Analysis (FEMA)
   K. Requirements Traceability Matrix.

   Please verify that the configuration management plan, coding standards and language, verification and validation (V&V) procedures, and the hardware and software quality control procedures used in the development of applications using these microprocessors are the same as those used in the design of the overall system.

8. Please provide the following documents pertaining to the HFC-6000 system:

   A. Software management plan.
   B. Software development plan.
   C. Software quality assurance plan.
   D. Project Quality Plan (referred to in section 8.4)
   E. Software Configuration Management Plan and any Configuration management reports.

F. Integration plan.
G. Installation plan.
H. Maintenance plan.
I. Software safety plan.
J. Software verification and validation plan, including TP0408B – Test System application Program (TSAP) Verification Test Procedure (referred to in Section 9.2.4.2)
K. Safety analyses
L. Verification and validation analysis and test reports.
M. Software requirements specifications.
N. Hardware and Software architecture description.
O. Software design specifications.
P. Operations, Maintenance, and Training manuals. (referred to in PP901-000-02)
    i. UG004-000-01 Engineering Workstation User's Guide
    ii. UG004-000-02 Cathode Ray Tube User's Guide
    iii. UG004-000-03 Historical Archiving System User's Guide
    iv. UG004-000-04 One-Step Software User's Guide
    v. UG004-000-05 Software Installation User's Guide
    vi. UG004-000-06 HIFR User's Guide
    vii. UG004-000-07 Site Planning and Installation Guide
    viii. UG004-000-08 Control System Maintenance Manual
    ix. UG004-000-09 I/O Simulation Manual
Q. Test Plans (referred to in Section 9.2.4.1):
    i. TN0401 Master Test Plan
    ii. TP0401 System Setup and Checkout Procedure
    iii. TP0408 TSAP Validation Test Procedure
    iv. TP0402 Operability Test Procedure
    v. TP0403 Prudency Test Procedure
    vi. TP0404 Environmental Stress Test Procedure
    vii. TP0407 Electro-Magnetic Interference/Radio frequency Interference Test Procedure
    viii. TP0409 Electrostatic Discharge (ESD) Test Procedure
    ix. TP0406 Surge Withstand Test Procedure
    x. TP0405 Seismic Test Procedure
    xi. TP0410 Burn-in Test
    xii. TP0411 Isolation Test Procedure
R. Test Reports corresponding to each of the individual test procedures
S. Configuration List (MCL) (referred to in section 9.2.2)
T. Requirements Specification for the Test Specimen and the TSAP software (referred to in section 9.2.2)
U. FMEA (Failure Modes and Effects Analysis, document RR901-000-01)
V. Design bases and design features, test plans, and test reports for the separation and isolation among safety channels and for the separation and isolation of safety channels from nonsafety channels.
W. Module Design Specification (referred to in Appendix A)
    i. MS901-000-01 HFC-SBC06
    ii. MS901-000-02 HFC-6000 I/O Card
    iii. MS901-000-03 HFC-PCC06
X. DS004-000-01 HFC Common Glossary (referred to in Appendix A)
Y. Vendor/Customer System Specification
Z. HFC Quality Assurance Program Manual (QAPM) (referred to in Section 10.1.5.5).

AA. Any recent external reviews and audits which have been performed. (referred to in 10.1.5.2.3)
BB. Requirements Traceability Matrix. (referred to in section 8.5.4)

9. Please specify (list) all hardware modules, including module part number and revision level, which are considered part of the HFC-6000 system. Include citations of all applicable documentation and design/manufacturing control information for each module.

10. Please specify (list) all software modules considered part of the HFC system. Include version information, revision levels, and all other applicable references for each module.

11. Please explain your criteria for determining the need for additional NRC staff review as a result of changes to hardware or software used in or in conjunction with HFC-6000. What degree of change to any of the hardware or software listed above would invalidate the NRC approval, and would require additional staff review?

12. Please provide the documentation (such as design specification, test procedures and reports) for the rack-mounted power supply module for the HFC-6000 product line, including the changes HFC is implementing as a result of the failed power supply surge test. How will HFC ensure that the failed design will not be used in nuclear safety applications? Have the resulting design changes been incorporated into <u>all</u> power supplies used by the HFC-6000 in all applications, and the failed design expunged from all future fabrication and use? How has HFC ensured that the design and physical characteristics that contributed to the failure are not present in any other module?

13. Revise the definition for “Regression Test” in TR Section 2.2 to include customer driven scope changes, or justify the exclusion of such changes.

14. In TR Section 6.1, Page 6-2, System Controller Module - one of the principle functions is listed as “redundant controller operations”. Is the HFC-6000 required to have redundant controllers, or can the system be purchased with only a single controller per channel? If it is possible to configure a system without redundant controllers, show that adequate reliability would be maintained.

15. In TR Section 6.1, Page 6-3, System Controller Module - The term “broadcast” is used to describe an ethernet network. “Broadcast” generally means a one-way communication, with no request or acknowledgment, in contrast with ethernet which is inherently bidirectional. Please clarify whether the communications are broadcast or ethernet, and if they are ethernet then please explain how it is ensured that the reply signals and handshaking process will not compromise the safety-related operations of any processor even in the event of hardware or software failure.

16. In TR Section 6.1, Page 6-3, System Controller Module - This states that public memory is used to communicate and coordinate the three independent microprocessors. Please explain the way public memory works, how the memory is partitioned, which processor has priority, how lower priority processors are locked out, and what prevents inadvertent overwrites. How is independent operation of the processors ensured if they all share the same memory and are therefore all potentially influenced by one another?

17. TR Section 6.1, Page 6-3, mentions 3 types of private memory, programmable read-only memory (PROM), Flash and random access memory (RAM). Please describe how each of

these is utilized. How are PROM chips controlled to ensure that the installed devices contain the proper data or programs?

18. TR Section 6.1, Page 6-4, states “output channels receives digital images”. Similar use of the word “images” is used throughout the topical report. Please explain how the word “images” is intended.

19. In TR Section 6.2.5, Page 6-7, Analog Input Module, discusses “ an onboard 8C188EB microprocessor.” No Intel data exists for this device. Is this meant to be a 80C188EB microprocessor?

20. In TR Section 6.2.5, Page 6-7, Analog Input Module, states that there are 16 analog field inputs. Please describe each type of analog field input module and the type of inputs which each module is capable of handling (i.e., 4-20 milli Ampere, 0-10 volt, some other type of input, or some combination of signals). Please describe any accessories that might be needed in conjunction with the modules, such as external resistors for current-based signals or external bridges for resistance thermal detector signals.

21. In TR Section 6.2.8, Page 6-7, Pulse Input Module, states that the configuration parameters for each pair of input channels are entered by bezel switches. Explain the design and management control features that prevent unauthorized or inadvertent changes. Explain what would happen if the switches were changed during normal operation (e.g. system response, alarms, etc.). Please answer these requests in regard to all modules having bezel controls of any type, not just for the specific modules and controls mentioned here. Please provide a comprehensive listing of all such modules and the controls provided for each.

22. In TR Section 6.3, Communication Modules, Figure 6-4 shows “Broadcast dynamic data among safety channels”. (Also described in Section 8.8.1) IEEE 603, “Criteria for Safety Systems for Nuclear Power Generating Stations,” required by 10 CFR 50.55a, “Codes and standards,“ subsection (h), states, in Section 5.6.1, on Independence between redundant portions of a safety system that “Redundant portions of a safety system provided for a safety function shall be independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any design basis event requiring that safety function.” In the same standard, a “Channel” is defined as: An arrangement of components and modules as required to generate a single protective action signal when required by a generating station condition. A channel loses its identity where single protective action signals are combined. It would seem that the dynamic data exchange between safety channels is inconsistent with the independence requirement, and combines the channels before a single protective action signal is generated. Explain the functions that make it necessary and the data that is sent. How is the requirement for channel independence maintained? Please describe in detail all communications and data exchange between channels, and the effect if this communications and data exchange were to fail.

23. In TR Section 6.3, Communication Modules, it is not clear if the ICL link services one SBC06, or if this same link services all SBC06 controllers. Please verify that the ICL Link is limited to one channel.

24. In the drawing on Page 6-1, the flat panel display (FPD) and code management system (CMS) and manual/automatic (M/A) stations are shown as connected directly to the SBC06

System Controller. In Figure 6-4 on Page 6-8, the FPD and CMS & M/A stations are shown as connected to the SBC System Controller via the ICL link. Please explain or correct this inconsistency.

25. In TR Section 6.3.2.3, HFC-FPC06 Module & 4 Safety Channel Communication Links, there is a statement in the discussion of the Fast Ethernet ports, which states "One port is configured for broadcast only, and the remaining three are configured to receive only operation." How is this configuration done? Can the configuration be changed to allow other types of communication? How can an ethernet port be configured to be broadcast only or receive only?

26. TR Section 7.1.1, Page 7-1, HFC-SBC06 Controller states that the three processors each have a "separate independent firmware program". Please describe these programs in terms of type, language and functions with respect to each other.

27. TR Section 7.1.1.2, SYS Processor Software Architecture states that the SYS Processor software uses a generic real-time Operating System. Please explain whether this operating system a commercial off-the-shelf (COTS) item, or whether it was written specifically for this application. If the operating system is COTS, please provide the documentation generated during the dedication process. If the operating system was written specifically for this application, please provide the specification, test and qualification documentation.

28. TR Section 7.2.1, Communications Link Software, discussed the Network Interface Chip and its broadcast of data. Please discuss the broadcast process/protocol, including the communications protocols message sequences, and any required acknowledgment messages.

29. TR Section 7.2.1, C-Link Software, and TR Section 7.2.1.1, Token Passing Scheme, both state that the token passing process permits deterministic execution of data transfer. Please explain the protocol, with particular emphases on the deterministic nature and the timing requirements. What controls the passing of the token?

30. TR Section 7.2.2, Inter-Communications Link (ICL) Software, states the ICL protocol is HFC proprietary. Please describe the ICL protocol in detail, including timing requirements.

31. TR Section 7.2.2.3, Polling, describes the poll-response communications protocol, and states that if an I/O module is polled without response within the timeout interval, and error is logged. How long is this interval, and what would happen after several failed polling attempts? How is flagged to the operator? How does the system respond to such a condition? What happens to the output signals?

32. TR Section 7.2.3, Input/Output Module Software, also discusses the interrupts. Please discuss how the use of interrupts affects the requirement for deterministic behavior of the safety system. What would happen if the interrupts were continually received?

33. TR Section 7.2.4.2, Page 7-12, Communications with CSM or M/A stations, states that each CSM included from one to four pushbuttons. This would indicate that there are four different versions of the CSM. Please provide details on the differences and similarities of these four versions, or please explain how one CSM can have differing numbers of pushbuttons without differing model or part numbers.

34. TR Section 7.2.5, Page 7-12, HFC-FPC06 FPD Controller Software, states “One port of four ports is used to broadcast the dynamic database (DDB) to the other three safety channels.” Please describe, with regard to communication between safety channels, what type of data is sent and by what method. Include discussion of any hand shaking that is required. What would occur if this communications were interrupted or if it were to fail so as to flood the channel with erroneous communications in either direction? Show how this communication provision is consistent with safety channel separation and isolation requirements of IEEE-279 and-603, or revise the design accordingly.

35. TR Section 7.2.5, Page 7-12, HFC-FPC06 FPD Controller Software, states that the real time operating system used in the FPC06 module is the QNX real time operating system. Please describe the commercial grade dedication procedure used for the operating system, what critical characteristics were considered, and how these critical characteristics were verified. Describe how configuration control is imposed upon the software. Please provide a copy of the commercial grade dedication documentation.

36. TR Section 7.4, Page 7-13, The Development and Maintenance Tools, briefly describes these tools. Please explain how each of these tools was chosen, and the commercial grade dedication process used to confirm the suitability for nuclear use. Please provide a copy of the commercial grade dedication documentation. Please describe the V&V process for each tool and show how the tool outputs are verified and validated. Show how it is ensured that each tool functions as intended at a level of confidence suitable for nuclear safety applications.

37. In TR Section 8.1.1, System Controller, states: “An HFC safety system can be configured with either single or redundant System Controllers.” Will HFC require that systems intended for safety-related use in nuclear power plants use redundant controllers?

38. In TR Section 8.1.2, SYS Processor Characteristic, discusses the real time clock (RTC) “ticks”, and that these are the only external interrupts. Are any other interrupts used, external or internal? What would the effect on the system be if the RTC stopped, or if the interrupt frequency doubled?

39. In TR Section 8.1.2, SYS Processor Characteristic, discusses a timing analysis. Please provide that timing analysis.

40. In TR Section 8.1.3, ICL Processor Characteristics, discusses the use of public and private memory. Please provide a detailed description of public and private memory, including how the memory is allocated and any predefined locations in memory. If dynamic memory reallocation is used, please describe the process.

41. In TR Section 8.1.3.1, Operation in a Non-Redundant Configuration, discussed ICL message error logging. How often can this occur before the system determines there is a hard error, and how is this error reported to the operator or maintenance personnel?

42. In TR Section 8.1.4, C-Link Processor Characteristics, states that use of a token passing protocol in the IEEE Standard 802.3 compliant 10BaseT Ethernet makes the link deterministic.

A. The use of the term "compliant" suggests that this is not actually a IEEE Standard 802.3 link, but rather that it differs from 802.3 in some manner. Please clarify, and identify and explain all points that are at variance with the standard.
B. Please show how a Ethernet link can be deterministic.
C. Please describe the token passing protocol.

43. In TR Section 8.1.4, C-Link Processor Characteristics, states that "Hardware and software associated with the C-Link processor are validated by diagnostics during initialization. Please describe how this is done.

44. In TR Section 8.1.4, C-Link Processor Characteristics, states that "When a remote station receives the token, it becomes the communications master and is allowed to transmit its messages to the other stations for a fixed maximum time." What is that maximum time, and how is it fixed?

45. In TR Section 8.1.4, C-Link Processor Characteristics, states that "Based on predefined data, the C-Link controller can determine if the token passing sequence is configured and operating properly." Please show how this is done.

46. In TR Section 8.1.5, I/O Module Characteristics discussed the Watchdog timer. Please provide specific details on the nature of the watchdog timer, how and when the watchdog timer is set, how long the timer is, and the sequence of events if the timer times out.

47. In TR Section 8.1.5, I/O Module Characteristics, states "During the interval between polling messages, the I/O processor runs I/O scan cycles on a 10 milli-second (ms) (nominal) cycle building a response message. The I/O processor also performs background diagnostics." Is this 10 ms cycle time the time for one I/O message, or the time for the entire cycle of message polling?

48. In TR Section 8.1.6 states "The QNX operating system provides deterministic, real-time task scheduling for the FPC tasks." Please show how the QNX operating system provides deterministic behavior. Please describe the dedication process, V&V, and configuration controls for this software.

49. TR Section 8.2, Failure Mode Effects Analysis (FMEA)
    A. Please provide the FMEA .
    B. The second paragraph states: "The evaluation of postulated system failures provides assurance that no latent design errors are present in the legacy components derived from previous HFC control system designs." Please show how this was determined.
    C. The second paragraph further states: "Any detectable HFC-6000 hardware failure after the initialization will be resolved by scheduled on-line diagnostic software and the operator surveillance of system performance. All detected failures will be reported as alarms." Please show how this is done.
    D. The first bullet states: "The probability that a single common mode failure or an undetected failure mode condition exists in the HFC-6000 system is negligible". Please explain the criteria for deeming a failure probability to be "negligible." Please provide the analyses and justification for this conclusion.
    E. The fourth paragraph states: "These features provide confidence that the HFC-6000 control system architecture will satisfy the single failure requirements of IEEE Standard 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and IEEE Standard 379-2000, "IEEE Standard Application of the Single-

Failure Criteria to Nuclear Power Generating Station Safety Systems." Since the single failure requirement is based upon plant-specific architecture and use, explain how HFC can make such a determination.

50. TR Section 8.3, Reliability and Availability
    A. The first paragraph states: "The availability of this system configuration is 99.94% for redundant controllers and 99.99997% for redundant systems". Do these values include software failure? Provide the analyses by which these values were determined.
    B. The third paragraph states: "A software tool, RELEX software was used to perform the MIL-HDBK-217 Analysis on parts and assemblies of the HFC-6000 product line". Is it the intent of HFC to provide the RELEX software for review and approval? How was the RELEX software dedicated for safety-related use? Does the RELEX software analyze both hardware and software? Please provide a fully-licensed copy of the RELEX software with all documentation. Also provide copies of all relevant RELEX-generated output data and reports and the associated input models and data.
    C. The fourth paragraph states: "Some modules of the HFC-6000 safety system have a redundant configuration, which means that one module can be lost without degrading functional operation of the HFC-6000 as a whole". Please provide a list of those modules which have a redundant configuration, and which do not. Is it the intent of HFC to require that all modules with the capacity for redundant configuration use the capacity in safety-related use by licensees? Explain how it is ensured that the system as-installed and as-maintained will include the same redundancy configuration as that analyzed.
    D. The fourth paragraph further states: "The calculation of availability of redundant modules was based on the guidelines described in IEEE Standard 352-1975." IEEE Standard 352-1975 has not been reviewed or endorsed by the NRC. Is it the intent of HFC that the staff review and endorse the standard in conjunction with the review of the HFC-6000?
    E. The fifth paragraph states: "For this analysis, the duty cycle was assumed to be 100 percent. The temperature profile is set at 26.4 degree C. It is assumed that the plant control system is in daily use, and failures will be detected within one day of occurrence." Why was the temperature profile set at 26.4 degree C, and how was it determined that all failures would be detected within one day?

51. TR Section 8.4, Quality Assurance Program
    A. Throughout this section, when describing the HFC compliance with various standards, terms such as "follow the guidance," "patterned after," "followed those described," and "used the guidance." These terms suggest ambiguity in regard to full compliance with the standards. Please indicate which standards are fully complied with, and for all standards which are not fully complied with, identify all differences between what is required by the standard and what was done by HFC. Include the analysis that show that the differences are not significant.
    B. On Page 8-9, HFC 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." Please provide documentation on these procedures and methods.
    C. On Page 8-9, HFC states: "To assure that the QA Program was being rigorously adhered to the Programs mandated; an independent verification effort to assess compliance with the QA Program and to provide on-going assessment of the adequacy of the measures was undertaken to ensure technical correctness of the QA processes."

Please provide details on the independent verification effort, including the procedures used and the final report on this effort.

D. On Page 8-10, HFC states: "At a minimum, a formal management review of the quality system is performed annually, to ensure its continuing appropriateness and effectiveness in satisfying HFC's business policies and objectives." Please provide a copy of the last formal management review of the quality system.

52. In TR Section 8.5.2; Compliance with NRC Documents:
    A. The discussion on Regulatory Guide (RG) 1.53, Single Failure Criterion states: "There are no undetectable failures within the HFC-6000 platform." Please show how this determination was made. Please identify how this includes operating history, deterministic information and/or analysis.
    B. The discussion on RG 1.62, Manual Initiation of Protective Actions states: "The amount of equipment common to both manual and automatic, isolation is kept to a minimum. Please explain what is meant by "a minimum." Show that no failure of the HFC system can prevent manual initiation of the protective action.
    C. The discussion on RG 1.62, Manual Initiation of Protective Actions also states: "Plant-specific designs will not allow a credible single failure to prevent system level manual actuation." Since no plant-specific design is available for review, please explain how this determination was made.
    D. The discussion on RG 1.152, Criteria for Programmable Digital Computer System Software in Safety-Related Systems of Nuclear Power Plants states "Where the legacy qualification process did not compare favorably with this standard, compensating factors were used." Please explain what this means, explain which features of the standard were not applied rigorously, and explain what compensating factors were used in regard to each of those features. Since this system has never been used in nuclear safety applications, it is not clear how questions of "legacy" provisions are applicable.
    E. The discussion on RG 1.173, "Development Software Life Cycle Processes for Digital Computer Software Used In Safety Systems of Nuclear Power Plants" states: "The activities for the HFC-6000 software life cycle model were deemed successfully completed when sufficient input information has been processed and sufficient output information has been generated." Please explain how this determination was made, the criteria used to determine the sufficiency of input and output information, and who made this determination. Please clarify that the model has already been "deemed successfully completed" and that the "sufficient input information" and "sufficient output information" have already been acquired and processed or generated as applicable. Please explain how application-specific considerations (considerations related to the application of the HFC-6000 in a particular installation at a particular nuclear power plant) fit into this determination.

53. In TR Section 8.5.4; Other Documents", the discussion on ISA S67-06-1984, Response Time Testing, states "The response time of the HFC-6000 system has been verified to be within acceptable limits." Please identify what that worst case response time value is, how it was determined and the type testing done to verify it.

54. In TR Section 8.8; Isolation and Independence, HFC discussed compliance with Annex G of IEEE Standard 7-4.3.2. RG 1.152 indicates that NRC has not endorsed the annexes of IEEE Standard 7-4.3.2 due to lack of consensus in the industry. Please identify what testing, component specification, and analysis of the three communication paths was done to determine that data isolation and independence exists.

55. TR Section 9.3.3.1.1, Environmental Test Results, please provide the analysis, or test report, with regards to the intermittent failures of the SBC06 controller. This information should consider if any latent, and permanent, effects to the controller were caused by the power drop, or cycling, to the test setup. Since other modules may be expected to be of similar circuit construction and to use similar components, show how it was determined that other modules are not subject to the same sort of failures. Explain how the design of this and other modules was modified to suppress such failures, and how it will be ensured that no modules of the failed design will be used in nuclear safety applications.

56. TR Section 9.3.3.3.1, ESD Test Results. Please provide further analysis why the M/A station resetting itself, is not considered a problem. A situation should be considered where functions where being changed or operations where being performed when the M/A station reset itself when a pulse is applied. This should be part of the analysis or provided separately. Also show that the unexpected M/A station behavior was unique to specific design features of the M/A station and that none of the other modules is susceptible to the same sort of influence.

57. In TR Section 9.3.3.4.2, Surge Test Results, the conclusion identified an alternative power supply, or alternative solutions, to use because the existing power supply did not pass this test. It also states requirements for “special” surge protection will be addressed on a plant specific basis. Please explain why the power supply should not be considered part of the Test Specimen configuration, which was qualified, and the plan to do surge testing or analysis on a plant specific basis. Explain how the alternative power supply or alternative solutions are known to resolve this problem. Specify the alterative power supply, and provide the alternative test reports.

58. TR Section 9.3.3.5.1, Seismic Test Sequence
    A. The test reports should include the report for the Prudency Test. Those documents should further explain why the deviations were not “significant” and the potential for increased effect due to the same failure mode are nonexistent.
    B. The test report, or suitable document, should include HFC’s decision to include the locking bar on the power supply rack or modules with enhanced locking tabs, as a result of the anomaly found during the Seismic Test 2. The staff believes the modifications, and or new test plans and procedures, should also include the changes as a result of the failed power supply surge test results.
    C. Please provide an analysis to address the type of failure in controller B and, more importantly, the potential for that type of failure to occur in both controllers simultaneously.

59. TR Section 9.4, Conclusion, stated that although tested with the Test Specimen, HFC identified the following 4 modules, as examples, that will not be included in the HFC-6000 product line for nuclear plant safety applications.

HFC-AC34 Special Analog Card	HFC-AI8L Thermocouple Input Card
FPCB Flat Panel Controller Box	HFC-1309 Power Supply

    Please identify to the staff:
    A. HFC’s alternative to, and plans for qualification of, the HFC-AI8L Thermocouple Input Card.
    B. Any other modules which were tested but will be excluded from nuclear applications.

C. What modules are forecasted in the future to be added and what qualifications will be done.