FOR INFORMATION ONLY

REQUEST FOR ADDITIONAL INFORMATION (PART 2)

BY THE OFFICE OF NUCLEAR REACTOR REGULATION

HFC-6000 SAFETY SYSTEM TOPICAL REPORT, REVISION A

DOOSAN HF CONTROLS CORPORATION

PROJECT NO. 731

Part 2 of the RAI (Question Nos. 60–117) consists of the items given below:

060 Section: n/a, Page: n/a

Please describe the status of the generic design. Has all coding been completed? Are there any design changes in progress? Are all generic documents final (no draft documents or unsubmitted revisions or revisions in process)?

061 Section: n/a, Page: n/a

Describe the fault tolerant features, in hardware and software, of the digital design. Describe the types of faults that are tolerated by these design features. Show how these features would respond to various faults, and show that the effectiveness of the safety system is not compromised.

062 Section: general, Page: n/a

In consideration of the large number of questions raised in regard to the Topical Report (TR), and of the considerable amount of explanatory and supplementary material anticipated in response to those questions, staff suggests that it would be beneficial for the applicant to revise the TR to incorporate the additional information directly. If this information is not incorporated directly into the TR, then it will be necessary for staff to cite the information sources and quote substantial portions of the information in the Safety Evaluation Report (SER). All future users of the TR would then need to take all of that additional information into consideration. The SER would be much simpler and that the amount of effort required by future users of the TR would be much less if the information were consolidated. Please advise staff as to how you intend to proceed in this regard.

063 Section: general, Page: n/a

Development and maintenance tools directly impact the implementation of the intended functions. If these tools do not function as intended, the system operation will not be as intended. It is not clear that the proper functioning of every application developed by such tools will or even could be fully tested. Please explain how the proper operation of these tools is ensured, and provide the supporting documentation.

064 Section: general, Page: n/a

In the discussion of Regulatory Guide (RG) 1.152, for example, on Page 8-13, there is a statement to the effect that something meets "all applicable guidance." In all such cases, throughout all documentation submitted for review, please identify the specific guidance considered "applicable" and the specific design or process attributes that demonstrate that the guidance was met.

065 Section: general, Page: n/a

Manual actuation must typically be independent of the safety system. HFC-6000 uses various kinds of interface modules to support manual actuation. Describe the specific design features of the HFC-6000 manual actuation devices, including answers to the following: Do the HCF interface modules act independently of the system, including independently of the input/output (I/O) modules? Would additional control panel devices independent of HFC-6000 be required to provide independence for those functions? If devices independent of HFC-6000 are required, then what is the purpose of the HFC manual interface modules?

066 Section: 8.8.2, Page: 8-31

The assertion that a failure of communication link (C-Link) cannot disable any safety function implies that no safety-related messages can be distributed over the C-Link and therefore that all I/O needed by a controller must be connected to the intercommunication link (ICL) dedicated to that controller. Controller independence is therefore ensured even within a safety channel. Please explain how this configuration will be enforced in plant-specific applications. Note that Figure 6-1 and Section 7.2.1 do not preclude the use of C-Link for safety functions.

067 Section: 7.2, Page: 7-5

(Figure 7-2) Only the single board computer (SBC), ICL, and I/O appear to be critical to reactor protection system (RPS) and engineered safety features actuation system (ESFAS) safety functions. Please clarify which devices and functions are included in the safety review request, and indicate how it will be ensured that any items that are excluded from the review will not be implemented in plant-specific applications without appropriate NRC review and acceptance. Some observations concerning items addressed in the referenced figure follow. Please confirm the observations, or indicate appropriate corrections.

a) The peripheral communication controller (PCC) and the control switch module (CSM) and manual/automatic (M/A) stations would only be needed if safety-related panel controls and displays were to be implemented. These are not typically required in actuation systems such as RPS and ESFAS.

b) The flat panel display (FPD) would only be needed if safety-related graphics displays were needed. In that case, the associated portion of the flat panel controller (FPC) would also be required.

c) The inter-channel broadcast functions provided by the FPC have the potential to violate the Institute of Electrical and Electronics Engineers (IEEE) 279/603 requirements for independence among safety channels. Please show that there is adequate electrical and data isolation and physical separation. Show that there are adequate provisions to ensure that one channel cannot adversely affect another, especially under conditions of faults, failures, and equipment or operator errors.

d) The C-Link would be needed for safety functions only if the functions were distributed among system controllers in such a manner that one controller is dependent upon another for successful operation. Such controller interdependence would be in conflict with the assertion in Section 8.8.2 to the effect that C-Link failure cannot disable any safety function. It appears that the Data Isolation/Buffer (Figure 7-2) provides functional isolation between the safety system and nonsafety equipment, and that the C-Link is not required to provide this isolation. It therefore appears that C-Link serves no safety function. Its purpose in the safety system is therefore not clear. Please explain.

e) (Similar concept, but not related to Figure 7-2): If control functions (PID controllers, signal lags, summers, etc.) are to be included in the safety-related scope of this system, then please identify specifically which functions are to be included and explain the development and verification and validation (V&V) of each. Also show how unqualified modules will be excluded from the safety system both in the initial implementation and in future modifications.

f) Show that non-safety devices and functions are adequately separated from safety devices and functions, and that the safety functions are adequately isolated from them. This request applies both to hardware and software. Note the RG 1.152 addresses concerns regarding non-safety functions performed by a computer that also performs safety functions. Show how these concerns are resolved in the proposed design.

068 Section: 7.3, Page: 7-13

The human machine interface (HMI) as described includes functions not typically considered to be safety-related, and it appears that the functions that might be safety-related are able to be provided via the CSM and M/A stations.

a) Please explain your intentions in including these functions in the safety system rather than as auxiliary nonsafety-related capabilities.

b) Show that no HMI operation or failure can adversely affect any safety-related function.

c) If the functionality of the HMI is safety-related, show that all aspects of the HMI, including hardware, application software, operating system, development system (including software), etc. are suitable for safety-related service.

069 Section: 8.1.2, Page: 8-2

The following statements reflect the staff understanding of the design, but are not explicitly addressed in the submittal. Please update the appropriate sections of the report and the design documents as appropriate to fully describe the system. Please confirm or correct each of these statements as appropriate.

a) The SYS processor is the highest-level processor in the system. That is, the SYS processor governs the operation of all associated processors and modules, and is not itself governed by any other processor or module (except in the sense of waiting for replies or status information, etc.). If a system has multiple SYS processors, they would be configured in such a manner that there is no interaction among them, and so none is dominant over any other.

b) The SYS processor is not dependent upon any peripheral device for its operation. That is, there is no disk drive or other device permanently connected to the SYS processor.

c) The application program is entirely contained in read-only memory (ROM) or in flash memory that is loaded by means other than via the SYS processor.

d) There is no need for any BIOS in the system controller or in the I/O modules.

070 Section: 6.1, Page: 6-2

Please provide docketed copies of the Requirements Specification (RS) & Design Specification (DS), and explain how it is ensured that the RS requirements are accurately transferred into the DS.

071 Section: 6.1, Page: 6-2

Show that there are no failure modes whereby an SBC06 could lock-up the dual-ported memory (DPM) and thereby prevent the back-up from taking over or causing the back-up to start with incorrect or obsolete data.

072 Section: 6.1, Page: 6-2

Does the back-up SBC06 monitor the primary and take over when appropriate? Or does the primary have absolute power over fail-over? How is it ensured that a failure will not cause the failed processor to take control and refuse to relinquish it?

073 Section: 6.1, Page: 6-2

Regarding maintenance fail-over: If fail-over is forced manually as a test and something goes wrong, the result could be a spurious trip or actuation. How is such negative impact avoided? How often should this (manual forcing) be done?

074 Section: 6.1, Page: 6-3

The description of the general functions of the 3 processors does not address the inter-channel broadcast function. Figure 6-4 suggests that this function is related to ICL by way of an additional module, FPC06. Please clarify. Please confirm that the SYS processor does not execute communications-related functions.

075 Section: 6.1, Page: 6-3

Primary/secondary controller access to DPM is controlled by software rather than via hardware:

a) Where is this in the general software structure?

b) Show that there is adequate control over user/operator/customer access to this software.

076 Section: 6.3, Page: 6-8

a) How are unused 10BaseT connections protected from later use such as internet connections or connection to unapproved devices or networks?

b) Bullet 6 refers to isolation between safety systems, but Figure 6-4 and other references show no C-Link connections to devices in other channels other than connection to Non-1E equipment.

Connection to other safety channels appears to be via FPC06, not C-Link. Please clarify.

c) Describe the isolation provided for nonsafety connections in accordance with the requirements of IEEE-603, and show that it is not possible for any fault of any kind in the nonsafety equipment to adversely affect the safety equipment. Show that there can be no fault in the nonsafety equipment that can result in “denial-of-access,” “continually busy,” or other such indirect interference with the operation of the safety equipment.

077 Section: 6.5, Page: 6-11

Qualification must be plant-specific. Generic qualification cannot be reviewed.

078 Section: 7.1.1.1, Page: 7-3

The subordinate processor “mailboxes” appear to function as watchdog timers except that the initial setting, the decrement amount and the cycle time are all adjustable. Describe how the settings are selected, implemented, and controlled.

079 Section: 7.1.1.1, Page: 7-3

If the primary controller is in the process of updating DPM when it fails, the DPM image will be incomplete and access to DPM might be blocked for the secondary controller (which will now become primary). How is it ensured that the failure will not inhibit access to DPM, and how will the new primary deal with the incomplete image? Might some of the DPM data be corrupted by the failure, especially if a "write" was in process at the time of the failure?

080 Section: 7.1.1.2, Page: 7-4

Please explain the function of the mailboxes. Are these used by the "watchdog strobe?"

081 Section: 7.1.1.2, Page: 7-4

When the SYS processor resumes Task 7 following an interruption due to a context switch, how is it ensured that it will resume operation at the proper point and with the proper state and data? To what extent is this resumption vulnerable to failures, and how has it been ensured that all credible failure possibilities have been adequately addressed?

082 Section: 7.1.1.2, Page: 7-4

Show that a "Context Switch" away from Task 7 cannot interrupt the task at a time when the interruption might have an adverse effect. For example, it may be necessary to delay the Context Switch for some elements of the task, or to wait until certain elements have been completed or reach a state wherein the interrupt would have a lesser impact. Please show that Context Switching will be delayed when necessary, or show that interruption of Task 7 at any randomly-selected point in time will never have any adverse effect. Show that there are no timing considerations for the resumption of the task, or show how it is ensured that timing considerations will always be satisfied without adverse impact. Show that any delay provisions or other aspects of the Context Switch will not stall the processor or otherwise adversely affect the system in the event of equipment or communications failure.

083 Section: 7.1.1.2, Page: 7-4

Can anything other than a Context Switch interrupt Task 7? Can any of the other tasks be interrupted by a Context Switch or by anything else? Why? How is proper resumption ensured?

084 Section: 7.1.1.2, Page: 7-4

The intended meaning of the last few sentences of the last large paragraph is not clear, due to various editorial issues such as ambiguous pronoun references, missing articles, and missing verbs. Please rephrase the intended statements.

085 Section: 7.2.1, Page: 7-6

The C-Link processor must interact with both the SYS processor and external equipment. How is it ensured that some condition in the external equipment will not place the C-Link processor into some state or mode of operation that would have a negative impact upon the SYS processor? For example, perhaps some external condition could cause the C-Link processor to monopolize the attention of the SYS processor and therefore interfere with the SYS processor attention to the Equation Interpreter tasks.

086 Section: 7.2.2.2, Page: 7-8

The final sentence suggests that the secondary controller may perform functions other than mirroring the primary controller ("... the secondary controller remains available to support secondary loopback and secondary scanning.") If the secondary controller has functions different from the primary controller, then those functions would no longer be performed following a primary-to-secondary failover. Please explain why this is acceptable.

087 Section: 7.2.3, Page: 7-10

Show that the use of interrupt-driven software in these applications does not result in a proliferation of possible software states too large for comprehensive review and testing. Include consideration of the potential effects of software and hardware errors and transient phenomena, including the effects of significant plant transients that might impose a considerable processing and actuation load on the system.

088 Section: 7.2.3, Page: 7-10

(Also other sections) It appears that, whereas the SBC06 System Controller has communications processors separate from the function processors, the I/O modules have only one processor for all functions including communications. Please confirm or clarify.

089 Section: 7.2.5, Page: 7-12

FPC contains both a single-board computer and a separate FPD controller module. Note that the symbol used for this single-board computer (SBC) is similar to the symbol used for the main controller (SBC06) shown as a separate module in Figure 7-2. The description indicates that all functions except for initialization are executed by the FPD controller, but does not address the function of the SBC within the FPC. Please describe the function of this SBC, as distinct from the function of SBC06. Please also explain the role of the QNX Operating System (OS), what safety

functions are performed by the QNX OS, the qualification process for the QNX OS, and which processor utilizes the QNX OS.

090 Section: 8.1, Page: 8-1

References to watchdog timers in Section 7 indicate that the timers are built into the system controller and utilize shared random access memory (RAM). There has been no previous mention of an independent timer that counts down by itself and is simply reset by the controller. Please describe the functions and operation of the watchdog timer, including: How does this watchdog timer initiate safety actions independently of system I/O? How are the particular actions to be taken under specific situations configured, selected by the system, and executed?

091 Section: 8.1, Page: 8-1

Describe the system controller timing analysis. Show that it addresses all aspects of system performance, including communications, I/O polling, and other interfaces that might affect response time as measured from the arrival of signals at the I/O module input terminals to the occurrence of appropriate response signals at the system output terminals. This analysis will be a critical element of any plant-specific review that may be performed in the future. Inclusion of a detailed methodology for this analysis in the present review would facilitate future reviews of plant-specific applications.

092 Section: 8.1.2.2, Page: 8-2

The references to self-diagnostics and to task priorities suggest that SYS processor operation is more complex than the simple deterministic linear stepping through the 8 task groups described in Section 7.1.1.2. Please describe the full set of functions performed by the SYS processor and explain how these functions interact with one another. In addition: Do some of the tasks in the 8 task groups involve processor interrupts or branching into multiple levels of subroutines? What self diagnostics are performed, and how is it ensured that return from them and from all other program branches and subroutines will be timely and proper?

093 Section: 8.1.1, Page: 8-1

The third bullet indicates that C-Link provides communication to the FPD, but Figure 6-4 and related descriptions indicate that the FPD is connected via ICL. Please resolve this apparent discrepancy. Please address the possibility that there are system configurations other than what is presented in this TR, and explain how it is ensured that the TR-described configuration is correct and would be implemented in a plant-specific application. It appears that the TR is based upon a system that has considerable flexibility and has a considerable history of design changes and upgrades. How is it ensured that references to inapplicable configurations and to obsolete design information have been purged from the TR?

094 Section: 8.1.2, Page: 8-2

Please describe the means by which the system software is loaded into the system controller modules and other modules, and describe the controls employed to ensure that the correct program is loaded and that it is loaded correctly.

095 Section: 8.1.2.1, Page: 8-2

This section contains a statement to the effect that the SYS processor deterministic performance is not affected by I/O or communications issues. But untimely I/O or communications could result in incorrect output states if the processor were to utilize unrefreshed data. Since the concept of "timeliness" includes the tacit assumption that the achieved output is not only "on-time" but also correct, and since the output cannot be correct if the inputs are not correct, please justify this statement. Similarly, some communications errors could have the potential for causing other kinds of problems for the SYS processor, such as denial of access to shared RAM. Please include consideration of such effects in your response.

096 Section: 8.1.3.1, Page: 8-3

Please explain what information the error counters convey, how they are used, and how the system as a whole responds to individual errors and to cumulative errors.

097 Section: 8.1.3.1, Page: 8-3

Please describe the diagnostics performed by the ICL processor and explain how it is ensured that these activities will not interfere with the timely operation of the safety-related aspects of the system.

098 Section: 8.1.3.2, Page: 8-4

The use of the secondary ICL for I/O communications which are not available on the primary ICL does appear to improve the availability of a communications channel, but it is not clear that the time required for the determination that the primary communication has failed, for the invocation of the secondary channel, for the secondary poll and response itself, and for the data transfer through DPM, would not compromise the deterministic system timing and increase the risk of using obsolete data. Please explain how timely operation is ensured in the event that the secondary ICL is invoked for I/O communication.

099 Section: 8.1.7, Page: 8-6

This section is titled "Deterministic Performance Conclusion," but is presented as a statement of a design goal rather than as a conclusion derived from the available data. Show how it will be ensured that this goal will be met in plant-specific applications.

100 Section: 8.2, Page: 8-6

The objective of the reference to "detectable failure condition" is unclear: the point of an failure modes and effects analysis (FMEA) is to show that all credible failures are either detectable or benign, or to highlight conditions requiring design changes to make them so. It is the undetectable failures that are potential concerns and that the FMEA is expected to highlight for design modification. Please confirm that the FMEA found no undetectable failures which subsequent design or procedural modifications have not yet rendered detectable or harmless.

101 Section: 8.2, Page: 8-7

As stated in the final paragraph and elsewhere, these are preliminary conclusions based upon a preliminary FMEA. They are therefore of limited value in the assessment of the proposed system.

Is the intent that the final FMEA be developed only on a plant-specific basis? If not, then please provide the final analysis and explain how plant-specific details are to be addressed (for example, perhaps there is to be a plant-specific supplement, or perhaps all possible plant-specific variations will be included in the final generic FMEA and so no plant specific analysis will be needed.). Similarly, the conclusions regarding IEEE-603 & -379 require knowledge of the details of how the system is implemented in regard to a specific plant, and it is not clear how they can be justified on a generic basis.

102 Section: 8.2, Page: 8-6

The cited Electric Power Research Institute (EPRI) report (TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants") is specifically applicable to programmable logic controllers, but the HFC-6000 design information describes a system more like a distributed control system than a PLC. Please explain how it is ensured that an FMEA based upon this report but addressing the HFC-6000 is comprehensive and complete given the potential differences between this system and the type of system for which the report was intended.

103 Section: 8.3, Page: 8-7

How are software, communications, and design/implementation errors accounted for in the quoted availability figures? Please provide the analyses by which these figures were derived.

104 Section: 8.5, Page: 8-11

Some of the documents and criteria in this section apply to specific applications in specific nuclear power plants. These cannot be reviewed on a generic basis. Some are directly applicable to the HFC-6000 independently of the details of any particular application. Conformance to those documents and criteria can be addressed for this topical report, independently of future plant-specific applications, if adequate support is provided in connection with the topical report review. Some of the statements concerning such criteria are simple assertions of compliance without supporting references. To the extent that you are requesting generic disposition of such items, please indicate which specific items you are requesting to be addressed generically and please provide sufficient information and documentation to support the stated conclusions.

Documents and criteria that apply to plant-specific details should be removed from the topical report or should be clearly designated as needing to be fulfilled on a plant-specific basis. Any information concerning them in the TR should be clearly identified as examples.

105 Section: 8.5.2, Page: 8-13

RG 1.168 (V&V): The described process appears to be applicable to software that was developed with the intention that it be used in nuclear safety-related service. Please explain how the software developed prior to the use of RG 1.168 is addressed in this regard. Please explain how it will be ensured that software that is developed in the future either for plant-specific applications or for generic applications will conform to this RG.

106 Section: 8.5.2, Page: 8-16

Branch Technical Position (BTP) 14: Please detail the points of conformance with and variance from the BTP. Please explain what is meant by "acceptable" development plans and design

outputs for new software. Please explain how the remaining software meets the BTP or, for software that has not been developed yet, will meet it.

107 Section: 8.5.2, Page: 8-17

BTP-17: Please describe the surveillance test provisions and the automatic self-testing.

108 Section: 8.5.3, Page: 8-19

IEEE-1016: Please provide a copy of the Software Design Description

109 Section: 8.5.4, Page: 8-21

EPRI TR-107330: Please provide a copy of the matrix that shows HFC-6000 design compliance. Please explain how the matrix is controlled and maintained when there are changes to the system design or to any of the referenced documents or requirements. Please explain how HFC-6000, which appears to have more in common with distributed control system (DCS) than PLC, is adequately addressed in the guidance of TR-107330, which is intended for PLC.

110 Section: 8.7, Page: 8-28

It appears that the C-Link itself is bidirectional, but the link to the outside world ("Universal Data Packet Broadcast" on Figure 6-4) is broadcast-only without handshaking or other transmit/reply functionality and without the opportunity for outside equipment to request any particular data. This suggests that the outside equipment must be in constant or scheduled "listen" mode, to receive general broadcasts and extract whatever data from the generic data stream it may need, and that there is no "receive" capability in the "Data Isolation/Buffer" shown on Figure 6-4. Since it would be expected that most commercially-available communications equipment is bidirectional or at least includes handshaking provisions for confirmation that a transmitted message has been received, the buffer must either be an unusual design or must have the receive/handshaking capability disabled. Please explain how this is accomplished.

Is the "ECS-B232 Fiber-Optic Transmitter/Repeater Board" mentioned in the third paragraph the "Data Isolation/Buffer" shown on Figure 6-4?

111 Section: 8.7, Page: 8-28

Besides disrupting communications with panel devices, a denial-of-service attack on the ICL would also disrupt plant data acquisition and, most importantly, the transfer of commands out to plant equipment through the I/O output modules. In such a case, the ability of the controller to continue to function would be obviated by its inability to command the plant. How is the system protected from such an attack?

112 Section: 8.7, Page: 8-28

Is it physically possible to install a modem or network interface card anywhere in the system or in the maintenance/engineering/programming equipment, and thereby open a link from the safety-related equipment to the outside world? If original equipment manufacturer (OEM) computers are used for the single-board computer or for any of the maintenance or configuration equipment, or if standard interfaces are used between the safety-related equipment and any of those devices, those provisions would seem to allow for the possibility of such connections. Please explain how it

is it ensured that such connections are impossible and that uncontrolled computers cannot be connected through the interfaces.

113 Section: 8.7, Page: 8-28

The end of the fourth paragraph suggests that there are nonsafety functions as well as safety functions in this system. What are the nonsafety functions? How are they physically and functionally separated from the safety functions? Please explain in detail how the provisions of IEEE-603 and of RG 1.152 are met in regard to nonsafety functions performed by safety-related computers.

114 Section: 8.7, Page: 8-29

The use of "logic gate arrays" is mentioned in the first line of text on this page. Please clarify the application of these arrays. Are they a fixed part of the system infrastructure?

115 Section: 8.7, Page: n/a

This summary of security provisions apparently draws from a more comprehensive analysis, and it presents conclusions without including the details of the supporting information. Please provide the detailed analyses supporting this summary. In addition, please explain how it will be ensured that future owners will understand, implement, and support the security provisions that you have assumed to be present.

For example, the summary indicates that "All PCs connected to the plant network should have their devices for reading removable media deactivated or removed." This would require that all universal serial bus (USB) ports be disabled so that flash-memory-based "thumb drives" cannot be connected. But some systems utilize USB ports for important connections such as keyboard, mouse, and printer. Also, connected computers may have compact disk (CD) burners for the acquisition of plant data for off-line analysis, and it is doubtful that such devices could be made incapable of reading, as well as writing, CDs. This statement requires that somewhat unusual and otherwise undesirable provisions be enforced, and potential users will need to understand what is necessary. Please clarify what is intended and show how the indicated provisions are possible and reasonable.

116 Section: 8.7, Page: n/a

In regard to virus protection, it is stated that "the more likely event being an authorized user inadvertently introducing malicious code... All PCs connected to the plant network should have their devices for reading removable media deactivated or removed." Also in this section is the statement "the HFC-6000 is a closed system, there is no opportunity for outside cyber security threats such as a virus ..."

a) What HFC-6000 hardware and software would have to be accessed via removable media?

b) Wouldn't all safety software for the system be implemented via non-accessible gate arrays and firmware?

c) How could PCs connected to the plant network have access to the HFC-6000 system?

117 Section: 2.1, Page: 2-1

Regarding the reference to "Appendix A" for document structure: There is a "document map" following Page 10-34, but it is unsigned and is apparently incomplete. It is identified both as "PP901-000-02 Rev A" and as "Appendix -", but not as being related to PP901-000-01. The Document Map itself includes an Appendix A presented as Pages 8 & 9. Please clarify these references and appendices.