U.S. NUCLEAR REGULATORY COMMISSION

OFFICE OF NUCLEAR REACTOR REGULATION

REQUEST FOR ADDITIONAL INFORMATION

"SUBMITTAL OF NON-PROPRIETARY INFORMATION FOR AMENDMENT 4

TO THE HFC-6000 SAFETY PLATFORM"

RAI-HFC-2020-DSGN-001

The U. S. Nuclear Regulatory Commission (NRC) staff is evaluating the HF Controls (HFC) platform against the requirements of the Institute of Electrical and Electronic (IEEE) Standard (Std.) 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations." IEEE Std. 603-1991, Clause 4, "Safety System Designation," requires in part, that, "The design basis shall also be available as needed to facilitate the determination of the adequacy of the safety system." Clause 5.5, "System Integrity," requires that safety systems be designed to accomplish their safety functions under a full range of applicable conditions enumerated in the design basis.

To establish a basis to support a safety evaluation (SE), the NRC staff requires information to clarify how the platform will operate in the presence of failures. The NRC staff requests HFC provide a failure modes and effects analysis that identifies the failure modes, including failures of system diagnostics, and describes the effects of these failures on the platform operation.

HFC Response:

RR901-107-11 "FMEA for HFC-FPGA Platform Functions and System," Rev. A has been submitted to the U.S. NRC in HFC letter dated February 19, 2020.

RAI-HFC-2020-DSGN-002

For applicable plants, Title 10 of the *Code of Federal Regulations* (10 CFR) 50.55a(h), "Protection and Safety Systems," requires compliance with the requirements of IEEE Std. 603-1991, and the correction sheet dated January 30, 1995. IEEE Std. 603-1991, Clause 4.10 requires in part that safety system design bases document the critical points in time or plant conditions after the onset of a design basis event.

The regulation at 10 CFR Part 50, Appendix A, General Design Criterion (GDC) 21, "Protection System Reliability and Testability," requires in part high functional reliability of safety systems. Timely operation is necessary for high functional reliability of safety systems.

In addition, Chapter 7, "Instrumentation and Controls," of NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," Branch Technical Position (BTP) 7-21, "Guidance on Digital Computer Real-Time Performance," provides guidance on real time performance.

A. Successful execution of the operational logic and application processing is not always guaranteed using a watchdog timer (WDT) for a field programmable gate array (FPGA) based designs. This is because individual logic functions within an FPGA are performed independently of each other. Therefore, the logic performing WDT functions operates independently from the logic performing safety functions. The NRC staff requests HFC provide information that describes how the WDT functions ensure that the execution of the operational logic related to the safety function within the system controller executes and is completed within its required periodicity.

HFC Response:

Watchdog functions are implemented in the HFC-FPGA system, which is designed to be used in nuclear power plant safety-related applications. Watchdog functions in the HFC-FPGA product are designed to perform three functions: 1) determine if the system is operating within expected limits, 2) identify abnormal functioning, and 3) force failover to a redundant processing function. The watchdog functions supplement the periodic diagnostics provided as part of the safety function that are designed to identify problems before a watchdog can time out and cause failover to the redundant controller. This action ensures continued safe operation of the system. Both watchdog and diagnostic failures can also occur on the redundant resource that force this resource to the failsafe condition. In this case, the system reports the redundant resource failure with a card alarm and reduces the redundancy status to degraded with no impact to the safety function.

RESET GENERATOR WATCHDOG

The first watchdog function is an external device reset generator [

] The reset generator device has [

]watchdog input. [

]

The watchdog input [ ] on the reset generator device monitors an internal timing signal output from the Diagnostic FPGA [

]

[

]

[

]

[

]

HEARTBEAT SEQUENCE WATCHDOG

The heartbeat sequence watchdog verifies that [ ] communication is functioning normally between the Diagnostic FPGA and the Control FPGA. This communication pathway is vital to the intended validation of the safety function,[

]

[

]

[

]

[

.]

[

]

[

]

[

]

APPLICATION WATCHDOG

[ ] The Application Watchdog is strictly an independent monitor and does not impede or prevent the performance of the safety function in any way.

B. Please provide additional information to indicate how the diagnostic functions within the FPGA-based modules are accomplished as well as a basis to support the assertion that the diagnostic function will not prevent, mitigate or delay the correct and timely operation of the safety function.

HFC Response:

The typical FPGA based system is a centralized I&C system consisting of redundant FPGA based controllers that communicate to a network of FPGA-based I/O modules. HFC leverages its extensive experience in I/O control to offer a large selection of I/O type modules that are HFC FPGA system compatible. The architecture of each controller and I/O module revolves around a pair of FPGA devices which communicate to each other and have some duplicated functions. Communication between duplicated functions serves as a basis for diagnostics that are used to validate application processing results and critical process data. Keep alive diagnostics are also implemented to verify process and diagnostic activity.

The diagnostics functions in the HFC-FPGA controller and input/output (I/O) FPGA Processing Unit (FPU) are accomplished in three categories: 1) power on diagnostics, 2) continuous DIAG block diagnostics, and 3) board operational diagnostics.

POWER ON DIAGNOSTICS

Power on diagnostics run every time a Controller or FPU I/O module has a power on event or the reset switch is actuated from the front bezel. Power on diagnostics [

] determine that the module has been configured properly and that communications are functioning properly with the mate FPGA [

]

DIAG BLOCK CONTINUOUS DIAGNOSTICS

[ ] These diagnostics are common to all HFC-FPGA Controllers and I/O FPU modules. [The diagnostics shown in the loop indicated with the green arrow

] run continuously. [

] Process Scheduler [ ] executes the required diagnostic checking function every [ ] as required for the architecture in which the diagnostics are running. [

]

[

]

[

]

Timeout occurs if one of the diagnostic checking functions fails to complete in [ ] This transition suspends the diagnostic loop and initiates a restart of the heartbeat sequence [

]

OPERATIONAL DIAGNOSTICS

Operational diagnostics fall into four categories: 1) memory diagnostics, 2) communication path diagnostics, 3) application diagnostics, and 4) I/O scan diagnostics.

Memory diagnostics implement a [ ] checksum to protect application data spaces. [

]

Communication path diagnostics are implemented using a [ ] algorithm. The communication path transmit logic uses the [ ] algorithm to append a [} value to payload data, [

]

Application diagnostics use the memory diagnostic to verify the data integrity before starting application processing. [

] support for each [ ] block in the application is verified before execution. The { } block provides exception status (i.e., divide by zero, overflow, underflow, qNaN, SNaN, inexact result, and infinite) during the execution of each [ ] block. [

] Control FPGA and the Diagnostic FPGA use the [ ] bus to synchronize diagnostic task readiness. When the Process FPGA and the Diagnostic FPGA both indicate application results are ready, the process result is validated [

]. The Diagnostic FPGA has the same resource and inputs to calculate the same application result and provide validation. {

}

I/O scan diagnostics are executed by Input and Output FPU modules. {
} The Control and Diagnostic FPGAs on an input FPU monitor the scan data and compare results to validate the input scan [
] The Control and Diagnostic FPGAs on output modules receive the same application result from the HFC-FPGA Controller. The Control and Diagnostic FPGA validate the received F-Link output scan data before use.

[

]

C. DS901-001-91, "F-Link and G-Link Protocol Design Specification," Revision A, describes the operation of the safety function communication pathway referred to as the F-Link. To make a safety determination related to the operation and performance characteristics of the F-Link, the NRC staff requests HFC to place Sections 2, 3, and 4 of DS901-001-91 on the docket.

HFC Response:

DS901-001-91 "F-Link and G-Link Protocol Design Specification," Revision A, has been submitted to the U.S. NRC in HFC letter dated December 18, 2019.

D. To establish confidence that the system will perform in a deterministic manner, the NRC staff needs more information related to the FPC-08 module. Although the communication protocols within the G-Link and C-Link are not part of the safety function communication pathway, the NRC staff needs to ensure the FPC-08 module's operation does not interfere with the safety-related communication pathway within the F-Link. Therefore, HFC is requested to provide information delineating all communication pathways within the FPC-08 module and include an explanation of how interference of the safety-related communication pathway (the F-Link) is prevented.

HFC Response:
The controllers and I/O modules communicate process and diagnostic data with each other over redundant differential serial busses using a master-for-a-moment communication protocol that allows each I/O module in the system a time-slot for communication with the controller(s) and time-slots for controller communication to I/O modules. This timeslot based system cycle allows

for deterministic communication and application processing for reliable system control. FPC08 is based on similar design.

The FPC08 base card has four transceivers that perform the [ ] physical interface to the backplane, [ ] The F-Link transmitter functions for F-Link 0/1 are disabled by configuration of the FPGA and the PCB. [

]

Failure of either F-Link Transmitter for F-Link 0/1 disables one safety function bus but does not disable the safety function, as it can communicate using the redundant bus.

Figure 1 FPC08 G-Link Gateway Interface Detail

RAI-HFC-2020-EQ-001

The NRC staff is evaluating the HFC platform against the requirements of IEEE Std. 603-1991. IEEE Std. 603-1991, Clause 5.4, “Equipment Qualification,” requires, “Safety system equipment shall be qualified by type test, previous operating experience, or analysis, or any combination of

these three methods, to substantiate that it will be capable of meeting, on a continuing basis, the performance requirements as specified in the design basis.

Guidance in Regulatory Guide (RG) 1.209, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants," and RG 1.100, "Seismic Qualification of Electrical and Active Mechanical Equipment and Functional Qualification of Active Mechanical Equipment for Nuclear Power Plants," and criteria in their endorsed IEEE standards may be used for environmental and seismic qualifications on safety-related equipment and systems. The NRC staff will evaluate if alternative approaches are acceptable, if used by HFC.

Electric Power Research Institute (EPRI) TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC [Programmable Logic Controllers] for Safety-Related Application in Nuclear Power Plants," was accepted by the NRC staff in a SE report by letter dated July 30, 1998, which HFC used for the environment and seismic qualifications on its HFC-FPGA platform system. EPRI TR-107330 was endorsed by the NRC for qualifying commercial PLCs.

A. Per the description provided by HFC in the topical report (TR), RR901-107-10, "Amendment for HFC-FPGA System of HFC-6000 Safety Platform," Rev. F, the HFC-FPGA platform in the TR was developed as a safety-related system, not a commercial product, for use in safety applications of nuclear power plants. Therefore, HFC is requested to provide additional information that addresses the above RGs (e.g., RG 1.100 and RG 1.209) related to the environmental and seismic qualifications for its HFC-FPGA platform. This information is needed to demonstrate the platform's ability to operate as a safety-related platform has been satisfied.

HFC Response:

TR901-302-02, HFC-FPGA Equipment Qualification Summary Test Report, Rev. A, Section 6 states that the qualifications tests performed were specifically defined by the conditions set in both EPRI TR-107330 and NRC RG 1.209. The purpose of these tests is to demonstrate the capability of the system hardware and software to continue operating within specified tolerances under extreme conditions. The full Operability and Prudency tests were run in between different qualification tests (Environmental, EMI/RFI, Seismic) to more accurately assess the effects of each specific test on the Test Specimen.

The Qualification Test System was monitored during the qualification test and any fault messages from the operational diagnostic were noted and evaluated. All self-diagnostics (including hardware watchdog timers) were in operation during qualification tests. This approach satisfied RG 1.209 Regulatory Position 2 that "qualification testing should be performed with the I&C system functioning, with software and diagnostics that are representative of those used in actual operation, while the system is subjected to the specific environmental service conditions, including abnormal operational occurrences."

Appendix B of TR901-302-02 states that the Environmental stress test performed was done in accordance with both RG 1.209 and IEEE Std. 323-2003. The environmental conditions from EPRI TR-107330 Figure 4-4 were used for generic platform qualification as bounding environmental conditions.

Appendix C of TR901-302-02 states that the Electromagnetic Interference / Radio Frequency Interference test was performed in accordance with RG 1.180, Revision 1, using additional guidance from EPRI TR-107330 as applicable.

Appendix F of TR901-302-02 states that the Seismic withstand test performed was done in accordance with both RG 1.100, Revision 3, and IEEE Std. 344-2004. The Operating Basis and Safe Shutdown Earthquake test spectra defined in Section 4.3.9 of EPRI TR-107330 were used as bounding response spectra.

No Radiation withstand test was conducted during the qualification test.

10 CFR Part 50, Appendix A (GDC 19-Control Room) states that adequate radiation protection shall be provided to permit access and occupancy of the control room under accident conditions without personnel receiving radiation exposure in excess of 5 E-2 sieverts (5 rem) whole body, or its equivalent to any part of the body, for the duration of the accident. Since HFC-6000 FPGA system will be in the mild environments (e.g., Auxiliary Building or Main Control Room), no radiation withstand capability was tested. The HFC-6000 FPGA system is not intended for use in harsh environments (e.g., Containment Building).

No smoke qualification test was performed. The primary protection for smoke is related to plant-specific fire protection designs that assess fire damage in defined fire zones, control fire and smoke propagation by design features and fire response procedures, and provide alternate safe shutdown means that are unaffected by fire damage to equipment in fire zones. This position is consistent with RG 1.209, which directly speaks to the topic in the discussion (Section B); however, no specific qualification test requirements were defined as a Regulatory Position (Section C). The RG discussion concludes that the most effective approach for addressing smoke susceptibility is to minimize the likelihood of smoke exposure by rigorously adhering to the fire protection requirements in 10 CFR Part 50.48, "Fire Protection," or other individual plant license commitments.

B. Section 4.2, “Functional Requirements,” of EPRI TR-107330, states that the overall response time from an input to the PLC shall be 100 milliseconds (ms) or less. In addition, RG 1.118, “Periodic Testing of Electric Power and Protection Systems,” states, in part, that total system response time is calculated based upon the description of a functional test is to be a test of all logic components (i.e., all relays and contacts, trip units, solid state logic elements, etc.) of a logic circuit, from as close to the sensor as practicable up to but not including the actuated device.

   However, the NRC staff found in Section 8.2.2, “Operability Tests,” of the TR RR901-107-10, “Amendment for HFC-FPGA System of HFC-6000 Safety Platform,” Rev. F that the acceptance criteria for response time are 100 ms for the digital logic and 300 ms for analog logic. HFC is requested to provide clarification and justification for the proposed criterion on system response time, whether that be a total of 100 ms (digital) and 300 ms (analog), for a total of 400ms per division (from sensor to final actuation device). Please explain what the overall expected system response time, including the overall response time from sensor output to the final actuation device will be.

HFC Response:

[

]

For this equipment qualification test, the HFC Plant Automated Tester and Test Specimen Application Program included separate algorithms to support direct measurement of Test Specimen response time for analog and digital logic components, which are measured separately.

All measurements for the digital response time were less than [ ] from input to output. All measurements for the analog response time were less than [ ] The analog algorithm is modified to produce an analog step instead of a digital output trip to eliminate the transfer delay produced by conversion circuitry.

RAI-HFC-2020-EQ-002

Section 5.2, "Pre-Qualification Acceptance Test Requirements," of EPRI TR-107330 states that the generic qualification sample must be calibrated to National Institute of Standards and Technology (NIST) traceable sources.

Additional information describing how the measuring and test equipment used for the HFC-FPGA qualification tests is traceable to the NIST nationally or international recognized standards is requested. HFC is requested to provide additional information to demonstrate that the measuring and test equipment used for the HFC-FPGA qualification tests is traceable to recognized and accepted standards.

HFC Response:

[

]

Measuring and test equipment (M&TE) used for the qualification tests were calibrated by a 3rd party vendor, MATsolutions. They were certified to ISO/IEC 17025:2005 by Perry Johnson Laboratory Accreditation.

Specific Certifications of Calibration for each equipment used are kept by Quality Control and can be viewed during the audit.

M&TE used in qualification labs are covered by the qualification lab's Quality Assurance program.