UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

April 27, 2020

Mr. Yin Guo
System V&V Lead
HF Controls Corporation
1624 West Crosby Road
Suite 124
Carrollton, TX 75006

SUBJECT: REGULATORY AUDIT PLAN FOR MAY 4-22, 2020, AUDIT OF "SUBMITTAL OF NON-PROPRIETARY INFORMATION FOR AMENDMENT 4 TO THE HFC-6000 SAFETY PLATFORM" (EPID L-2018-TOP-0031)

Dear Mr. Guo:

By letter dated April 15, 2019 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML19109A158), HF Controls (HFC) submitted for U.S. Nuclear Regulatory Commission (NRC) staff review a licensing topical report (LTR) "Submittal of Non-proprietary Information for Amendment 4 to the HFC-6000 Safety Platform." The LTR is supported by documentation that includes plans, requirements, design specifications, programming and hardware testing, independent verification and validation, and equipment qualification testing.

The U.S. NRC staff is currently reviewing the LTR for use in safety system equipment at nuclear power plants. As part of its review, the NRC staff will be performing a remote regulatory audit of HFC by conducting a number of conference calls and reviewing documents via a remote access website. The audit will be conducted between May 4 and May 22, 2020.

The audit will determine the degree that the processes and outputs used have resulted in satisfying regulatory requirements for safety system applications at nuclear power plants. This audit will provide information necessary to complete the NRC staff's evaluation of the LTR. Enclosed is a copy of the plan the NRC staff will follow during the audit.

If you have any questions or require any additional information, please feel free to contact me at 301-415-7297 or via electronic mail at Joseph.Holonich@nrc.gov.

Sincerely,

/RA/

Joseph J. Holonich, Senior Project Manager
Licensing Processes Branch
Division of Licensing Projects
Office of Nuclear Reactor Regulation

Enclosure:
Audit Plan

Docket No. 99902026

REGULATORY AUDIT PLAN FOR MAY 4-22, 2020,
AUDIT OF THE "SUBMITTAL OF NON-PROPRIETARY INFORMATION FOR AMENDMENT 4 TO THE HFC-6000 SAFETY PLATFORM" (L-2018-TOP-0031)

Date: Week of May 4, 2020 to be completed by May 22, 2020

Location: Remote with correspondence to Doosan HF Controls, 1624 W Crosby Rd, Carrollton, TX, 75006

Audit Team Members:
Richard Stattel, Audit Team Leader, NRR/DEX/EICB
Jack Zhao, Audit Team Member, NRR/DEX/EICA

Background
By letter dated April 15, 2019 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML19109A158), HF Controls (HFC) submitted for U.S. Nuclear Regulatory Commission (NRC) staff review topical report (TR) "Submittal of Non-proprietary Information for Amendment 4 to the HFC-6000 Safety Platform.'" By letter dated June 11, 2019, (ADAMS Accession No. ML19127A009) the NRC completed its acceptance review and found that the material submitted was sufficient to begin our review of the HFC platform. On February 19, 2020, the NRC issued a Request for Additional Information to HFC to obtain information necessary to complete our review (Package ADAMS Accession No. ML20021A228). This audit activity will enable the NRC staff to more efficiently gain understanding, verify information, and/or identify information that may be required to support a safety determination in its safety evaluation.

Audit Scope:
This audit will be conducted in accordance with NRR Office Instruction LIC-111, "Regulatory Audits." The NRC staff will review non-docketed procedures and records related to the HF Controls (HFC)-6000 Amendment 4 submittal with information associated with the field programmable gate array (FPGA)-based HFC-6000 platform. The material under review will primarily cover portions of the design and development processes and the performance aspects of the platform as they relate to the suitability of the platform to operate as part of a safety-related component, function or system. The audit also examines the qualification measures and tests taken by HFC to ensure satisfactory operation of the platform under all credible environmental conditions related to the performance criteria of the platform.

Regulatory Audit Bases
To support determinations that will be made in its safety evaluation, the NRC staff is reviewing portions of HFC's design, development, verification and validation (V&V), and qualification process used for the HFC-6000 FPGA-based platform that will aid in its evaluation of the platform's fault tolerance and level of robustness.

Design and Development Processes

- The NRC staff is evaluating the HFC 6000 FPGA platform against the acceptance criteria in the Institute for Electrical and Electronics Engineers (IEEE) Standard (Std.)

603-1991. Section 4, “Safety System Designation”, supports the establishment of the design basis for the safety system. Clause 5.3, “Quality”; directs the designer to ensure the components and modules that comprise the safety system are of sufficient quality to ensure low failure rates. Additionally, it directs the designer to ensure the safety system equipment be designed, manufactured… tested …in accordance with a prescribed quality assurance program. Clause 5.5, “System Integrity”, states that the safety system shall be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis.

- Within 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) 7-14, “Guidance on Software Reviews for Digital Computer-based Instrumentation and Controls Systems,” describes “Reliability” as ensuring that all requirements for fault tolerance and failure modes are fully specified for each operating mode. Software requirements for handling both hardware and software failures should be provided, including requirements for analysis of and recovery from computer system failures. Requirements for on-line in-service testing and diagnostics should be provided.

- BTP 7-21, provides guidelines for reviewing digital system real-time performance and system architectures in instrumentation and control (I&C) systems. It also describes systems that use a watchdog timer (WDT) function and its accompanying basis to verify correct execution or operation of the safety function during each WDT’s given periodicity and complete as designed prior to the next iteration of the given operational cycle.

Environmental Qualification Processes

Additional technical areas under review by the NRC staff as part of its safety evaluation, are HFC’s environmental testing program and related processes used for the HFC-6000 FPGA-based platform.

- The NRC staff is evaluating the HFC 6000 FPGA-based platform against the acceptance criteria in IEEE Std. 603-1991. Clause 5.4, “Equipment Qualification”, requires that “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.

Another purpose of the audit will be to gain a better understanding of the overall HFC programmatic processes applied to the FPGA-based platform to support the safety evaluation of the HFC-6000 Platform and to assess the capabilities of the HFC-6000 platform to determine if an HFC-6000 based I&C safety system will be capable of meeting regulatory acceptance criteria as described in Chapter 7 of the NRC Standard Review Plan, NUREG-0800. The NRC staff will use the results of this audit to support its safety conclusions.

Audit Activities:

Design Quality and Performance Characteristics – The purpose of the audit as it relates to the design of the platform is to gain knowledge and information that can be used to support a safety evaluation that determines the HFC platform is suitable for use in a safety-related application.

The NRC staff will discuss, with appropriate HFC staff, portions of the design characteristics and development processes of the HFC-6000, including its fault tolerance and failure resistance, that includes the use of its diagnostic features that include the watchdog timer (WDT) functions within the platform. Specifically, to gain a better understanding of the design of the platform, the NRC staff will discuss with HFC personnel its planning activities and requirements management program including discussions related to its requirements specification and requirements traceability programs. Additionally, the NRC staff will discuss with program and system experts, HFC's configuration management, secure development and operational environment (SDOE) and verification and validation (V&V) programs. This information will support the determinations that will be made in the safety evaluation.

Equipment Qualifications (EQ) – The NRC staff will review and evaluate the detailed testing plans, procedures, actual records for environmental, seismic, and EMI/RFI qualifications of the HFC 6000 FPGA-based platform. The NRC staff will also discuss with the appropriate HFC personnel, or its agents, aspects of its EQ program that will aid in supporting HFC's claim that the EQ tests for the HFC-FPGA platform were conducted according to applicable regulatory guidance and that acceptance criteria were met for the HFC-FPGA platform.

The NRC staff will discuss with the appropriate HFC staff members, the overall EQ program utilized by HFC, specifically reviewing elements of EQ testing processes, test procedures, and related acceptance criteria and test results for EQ related test activities.

Information Necessary for the Regulatory Audit:

Related to the design, development and V&V processes of the HFC Platform, the applicant should be prepared to:

- Discuss and provide documentation that supports the following HFC programs and how each demonstrates conformance with applicable NRC guidance or recognized industry standards:
    - Requirements Development – including Requirements Specifications and Requirements Traceability
    - Configuration Management
    - Demonstration of a Secure Development and Operational Environment during software/firmware development and operation.
    - Verification and Validation

- Discuss with HFC personnel, the platform's failure modes and effects analysis (FMEA) for the platform, that HFC will likely have developed by the time of the audit, including the systemic impact of the failure, the platform's method of failure detection and notification to the operator.

- Discuss, with appropriate HFC personnel, the operation of the three watchdog timers (WDTs) within the given FPGA-based HFC-6000 modules, including the relationship between the different types of WDT functions of the platform. This should include the circuit design characteristics and a description of the composition of the devices (hardware-based and/or software-based). Discuss how all functions of the WDTs support verification that the logic within the platform is operating satisfactory.

- Discuss any remaining open items related to the design of the HFC-6000 platform

Related to the EQ Program of the HFC-6000 Platform, the applicant should be prepared to have the following documentation and information available before the audit begins:

- All testing plans and procedures used for the HFC-FPGA EQ.
- Testing records for EQ tests conducted, including any failures which might have occurred during the complete EQ testing process and the documentation that demonstrates the failures or deficiencies were corrected or resolved.
- Documentation to demonstrate the implementation of a suitable quality assurance program implemented at the applicant's and its contractors' facilities.
- Documentation for the HFC TUV SIL 3 certification and any limitations or constraints related to that certification.
- Documents to show the Certifications of Accreditation and Calibration for the EQ test equipment.
- Re-test reports for the power interruption test: TR901-2002-02, TR901-2002-03, and TR901-2002-05.
- Test reports, both summary and detailed, produced by contractors NTS and ETL.

Team Assignments

Design and Development Activities

Richard Stattel	Requirements Development and Traceability Configuration Management Secure Development and Operational Environment WDT and Diagnostic Functionality of Platform Failure Modes and Effects Analysis Verification and Validation Activities

Equipment Qualification (EQ) Program

Jack Zhao	Environmental Testing Policies, Processes, and Procedures EQ Test Results and Test Records

Note: Team Assignments for NRC staff may change as required, during the audit.

Logistics

The audit will take place remotely. The audit will commence on the morning of Monday, May 4, 2020, and conclude by, May 22, 2020, unless the audit team determines it has completed its audit activities sooner and, as such, the audit schedule and its closeout will be adjusted accordingly.

HFC Audit Schedule			
Date	***Time***	***Activity***	***Participants Lead / Part***
Monday May 4, 2020	9:00 to 10:00am (All times are in Eastern Standard Time)	*Entrance call: • NRC – purpose of audit; • HFC staff – provide discussion of testing facilities used for equipment qualification	NRC / HFC
	10:00am to 11:00am	*HFC to provide requirements thread traceability demonstration.	HFC / NRC
	12:00pm to 3:00pm	Audit team to independently perform requirements thread audit.	NRC
	3:00pm to 4:00pm	*Call to discuss initial thread audit results.	NRC / HFC
Tuesday May 5, 2020	9:00am to 9:30am	*Morning call between the NRC staff and HFC to discuss activities and logistics for the day	NRC / HFC
	10:00am to 11:00am	*Call to discuss HFC Configuration Management Tasks.	NRC / HFC
	12:00am to 2:00pm	Audit team to independently perform SDOE audit activities.	NRC
	2:00pm to 3:00pm	*Call to discuss HFC SDOE activities.	NRC / HFC
	3:00pm to End of Day	Audit team to independently perform SDOE audit activities.	NRC
Wednesday May 6, 2020	9:00am to 9:30am	*Morning call between the NRC staff and HFC to discuss activities and logistics for the day	NRC / HFC
	10:00am to 11:00am	*Call to discuss HFC Equipment Qualification.	NRC / HFC
	11:00am to 3:00pm	Audit team to independently perform HFC Equipment Qualification audit activities.	NRC
	3:00pm to 4:00pm	*Call to discuss open items.	NRC / HFC
Audit Closure Date to be determined. No later than: May 22, 2020	9:00am to 9:30am	*Morning call between the NRC staff and HFC to discuss activities and logistics for the day	NRC / HFC
	10:00am to 3:00pm	Audit team to perform miscellaneous audit activities in all areas and write initial audit notes for audit closure meeting.	NRC
	4:00pm to 5:00pm	*Call - Audit Exit. NRC to provide summary presentation of audit results.	NRC / HFC

Deliverables

The NRC regulatory audit report should be issued by August 6, 2020.

SUBJECT: REGULATORY AUDIT PLAN FOR MAY 4-22, 2020, AUDIT OF "SUBMITTAL OF NON-PROPRIETARY INFORMATION FOR AMENDMENT 4 TO THE HFC-6000 SAFETY PLATFORM" (EPID L-2018-TOP-0031) DATED APRIL 27, 2020

DISTRIBUTION:

PUBLIC	RidsNrrOd	RidsOpaMail	RidsNrrDex
JHolonich, NRR	RidsNrrDorlLlpb	MWaters, NRR	
RidsACRS_MailCTR	RidsNrrDexEica	RidsNrrDorl	DMorey, NRR
RidsOgcMailCenter	RStattel, NRR	BVenkataraman, NRR	
JJohnston, NRR	JZhao, NRR		

ADAMS Accession No.: ML20043F266 ***concurred via email**

OFFICE	NRR/DORL/LLPB/PM*	NRR/DORL/LLPB/LA*	NRR/DE/EICB/BC*
NAME	JHolonich	DHarrison	MWaters
DATE	03/18/2020	03/17/2020	04/21/2020
OFFICE	NRR/DORL/LLPB/BC*	NRR/DORL/LLPB/PM*	
NAME	DMorey	JHolonich	
DATE	04/24/2020	04/27/2020	

OFFICIAL RECORD COPY