DOOSAN HF Controls

Amendment 4 Re-Submission Overview

8/1/18

RR901-107-10 Revision D Comments

1. Conformance with NRC ISG-06 section C3 not fully shown. With respect to one or more of the following:
   a) System Description
   b) Hardware Development Process
   c) Software Architecture
   d) Software Development Process
   e) Environmental Equipment Qualifications
   f) Defense-in-Depth & Diversity
   g) Communications
   h) System, Hardware, Software, and Methodology Modifications
   i) Compliance with IEEE Std 603
   j) Conformance with IEEE Std 7-4.3.2
   k) Technical Specifications
   l) Secure Development and Operational Environment

RR901-107-10 Revision D Comments (Continued)

2. Relative to ISG-06, it is unclear where microprocessors are used VS FPGA, and what software/FPGA is used for each hardware item
3. IEEE 603 Section 5.5 compliance not proven
4. 10 CFR 50 Appendix A, GDC 21 and 23 compliance not proven
5. 10 CFR 50 Appendix B Compliance not proven for FPGA used
6. While the original submittal and approved HFC-6000 system was referenced, it is unclear what portions of the Amendment 4 submittal take credit for portions of the original submittal and what portions need new information (such as FPGA development process vs microprocessor development process)
7. CGID process for FPGA and firmware not proven in compliance with 7-4.3.2
8. Submittal is unclear as to what the differences are between the accepted microprocessor design development process is vs the new FPGA design development process, and what modules that applies to
9. What portions of the design process are commercially dedicated vs developed within the HFC process
10. Tools such are Onestep and Libero are not thoroughly documented or evaluated
11. Analysis of deterministic behavior not sufficiently proven, such as Failure Mode Analysis
12. Terminology of microprocessors vs FPGA is mixed throughout the submittal, making it unclear which is applicable to what modules

ISG-06 Section C3

- All sections reviewed. As this comment was very broad, some sections were found to not require updates.
- Sections are:

1. System Description
   A. VV901-300-10, HFC-6000 FPGA Test Specimen Design Description updated to Revision B
   B. Updated VV901-300-10 Rev B includes a table of what FPGA are used on each HFC-FPGA module, and in what quantities
2. Hardware Development Process
   A. Section 5.2 added to describe HW Development process
   B. States the overall design process used at HFC, and that WI-ENG-108 addresses changes in the Implementation and Test phases for FPGA-specific designs
3. Software Architecture
   A. Minor clarifications added to Section 5.3

ISG-06 Section C3 (Continued)

4. Software Development Process
   A. Section 5.4 added to describe SW Development process
   B. Section 5.5 added and referenced WI-ENG-108 to detail the differences between FPGA implementation activities and other HFC-6000 software implementation activities
5. Environmental Equipment Qualifications
   A. EQ report TR901-302-01 determined to be sufficiently details, no action taken
6. Defense-in-Depth & Diversity
   A. Section 6.10 expanded to show how design allows for Diversity and Defense in Depth, to be analyzed for plant-specific applications
7. Communications
   A. Reference to DS901-001-91 F-Link and G-Link Protocol Design Specification added to Section 6.7, details added to 6.4-6.6

ISG-06 Section C3 (Continued)

8. System, Hardware, Software, and Methodology Modifications
   A. Section 9 added to describe HFC SCR process
9. Compliance with IEEE Std 603
   A. References to EPRI RTM added to section 6.9.3, additional references added throughout Topical Report
10. Conformance with IEEE Std 7-4.3.2
   A. Section 7 added to detail tool qualification description
11. Technical Specifications
   A. RS and DS referenced for all modules
   B. VV901-300-10 updated, referenced
12. Secure Development and Operational Environment
   A. Section 6.11.2 added to address SDOE

ISG-06

- NRC states that relative to ISG-06, it is unclear where microprocessors are used VS FPGA, and what software/FPGA is used for each hardware item
  - VV901-300-10 adds more detail about the use of FPGA, specifically what FPGA are used in which modules
  - Table present in VV901-300-10 section 2.2.3

IEEE 603 Section 5.5 Compliance Not Proven

- “The safety systems shall be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis. Guidance on the application of this criteria for safety system equipment employing digital computers and software or firmware is found in IEEE Std 7-4.3.2-1993”

- Addition of reference to FMEA RR901-107-01 for failure conditions to Section 6.7

- Conditions details added to Section 6.9.3

10 CFR 50 Appendix A, GDC 21 and 23

- Criterion 21—Protection system reliability and testability.
  - Section added in 6.9.5
  - Referenced RR901-107-02, Reliability and Availability Analysis Report for FPGA Controllers
  - Testability detailed and points to DSs for specific cases

- Criterion 23—Protection system failure modes
  - Reference to RR901-107-01, FMEA for FPGA Controllers of HFC-6000 Safety Platform added in Section 6.9.5

10 CFR 50 Appendix B Compliance For FPGA Use

- Previous submittal referenced QAPM without much detail
- Quality Assurance Program as described in QAPM is the same from microprocessor-based HFC-6000 system and HFC-FPGA system
- Specific reference to QAPM and its organization and applicability added to section 6.8
- QAPM to be included in Acceptance Review submission

FPGA Vs. Microprocessor

- “While the original submittal and approved HFC-6000 system was referenced, it is unclear what portions of the Amendment 4 submittal take credit for portions of the original submittal and what portions need new information (such as FPGA development process vs microprocessor development process)”
  - Section 5.1 added
  - References to original HFC-6000 TR made more explicit, listing applicable section
  - Work instruction WI-ENG-108 referenced for clarity of FPGA development process differences, to be included in the submission
  - 5.2 HW Development Process section added for FPGA-specific HW development
  - 5.4 SW Development Process section added for FPGA-specific SW development

CGID Process for FPGA and Firmware

- “CGID process for FPGA and firmware not proven in compliance with IEEE 7-4.3.2”
- CGID not specifically referenced in TR
  - Section 7.0 added to address Tool Use and Qualification
  - CGID process not required due to testing in the development process

FPGA Vs Microprocessor Development Process

- “Submittal is unclear as to what the differences are between the accepted microprocessor design development process is vs the new FPGA design development process, and what modules that applies to”
  - Sections 5.2 and 5.4 added to RR901-107-10
  - WI-ENG-108 added to submission
  - Section 2.2.3 added to VV901-300-10 to describe what FPGA chips were used on which HFC-FPGA modules

CGDI Vs HFC Developed

- "What portions of the design process are commercially dedicated vs developed within the HFC process"
  - Section 7.0 details the portions of the design process that are covered under the HFC development process
  - OneStep has a separate section 7.1
  - Other 3rd party tools such as Libero are tested under V&V activity in accordance with IEEE 7-4.3.2m as detailed in section 7.2
  - No CGID required

Tools Qualification

- “Tools such are Onestep and Libero are not thoroughly documented or evaluated”
  - Tools qualification performed as part of V&V activities as described in Section 7

Deterministic Behavior Not Proven

- “Analysis of deterministic behavior not sufficiently proven, such as Failure Mode Analysis”
  - Section 6.7 expanded
  - RR901-107-01, FMEA for FPGA Controllers of HFC-6000 Safety Platform referenced for deterministic behavior of each HFC-FPGA module
  - DS901-001-91 F-Link and G-Link Protocol Design Specification referenced for deterministic behavior of F-Link and G-Link communication protocols

Terminology

- “Terminology of microprocessors vs FPGA is mixed throughout the submittal, making it unclear which is applicable to what modules”
  - VV901-300-10 updated adding Section 2.2.3 to explicitly state when FPGA are used, and in which modules
  - Terminology made more consistent throughout the Topical Report.

Documents For Submission

- New to this submission
  - Quality Assurance Program Manual, Rev M
  - WI-ENG-108-PI, FPGA Design, Implementation, and Test, Rev A

- Updated
  - RR901-107-10-PI Amendment for HFC-FPGA System to HFC-6000 Safety Platform Rev E
  - VV901-300-10, HFC-6000 FPGA Test Specimen Design Description, Rev B

- Unchanged
  - RR901-107-03-PI, EPRI TR 107330 RTM FPGA Controllers, Rev. B
  - TR901-302-01-PI HFC-FPGA Control System of HFC-6000 Safety Platform Qualification Test Report Rev B

Communication

- SharePoint
- Email Eugene.odonnell@Doosan.com
- Additional document submission on request

Questions?