April 3, 2017

James Powers
Vice President, Nuclear Island & Business Development
Toshiba America Energy Systems Corporation
3545 Whitehall Park Drive
Suite 500
Charlotte, NC 28273

SUBJECT: REGULATORY AUDIT REPORT FOR MAY 16-20, 2016, TOSHIBA "LICENSING TOPICAL REPORT FOR TOSHIBA NRW [NON RE-WRITABLE]-FPGA [FIELD PROGRAMMABLE GATE ARRAY]-BASED INSTRUMENTATION AND CONTROL SYSTEM FOR SAFETY-RELATED APPLICATION," UTLA 0020P, REVISION 2 (TAC NO. ME9861)

Dear Mr. Powers:

By letter dated February 23, 2015, Toshiba Corporation (Toshiba) submitted Revision 2 to "Licensing Topical Report For Toshiba NRW-FPGA-Based Instrumentation And Control System For Safety-Related Application" (Agencywide Documents Access and Management System Accession No. ML15062A183). The topical report (TR) is supported by documentation that includes plans, requirements, design specifications, programming and hardware testing, independent verification and validation, and equipment qualification testing.

From May 16, 2016, through May 20, 2016, the U.S. Nuclear Regulatory Commission (NRC) staff performed a regulatory audit at the Toshiba facilities in Japan. The audit was conducted to support the NRC staff evaluation of the Toshiba TR.

The purpose of this letter is to provide Toshiba with the results of the regulatory audit. Documented in the report are the observations the NRC staff identified during the audit.

If you have any questions regarding this matter, I may be reached at 301-415-7297 or by electronic mail at Joseph.Holonich@nrc.gov.

Sincerely,

/RA/

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

Project No. 729

Enclosure:
As stated

SUBJECT: REGULATORY AUDIT REPORT FOR MAY 16-20, 2016, TOSHIBA "LICENSING TOPICAL REPORT FOR TOSHIBA NRW [NON RE-WRITABLE]-FPGA [FIELD PROGRAMMABLE GATE ARRAY]-BASED INSTRUMENTATION AND CONTROL SYSTEM FOR SAFETY-RELATED APPLICATION," UTLA 0020P, REVISION 2 (TAC NO. ME9861) DATED: APRIL 3, 2017

DISTRIBUTION:

PUBLIC	RidsNrrDpr	RidsNrrDprEicb
KHsueh	RidsACRS_MailCTR	RidsNrrDprPlpb
RidsOgcMailCenter	RidsNrrLADHarrison	JHolonich
RidsNroOd	RidsResOd	RAlvarado

ADAMS Accession No.: ML16257A022; *concurrence via email **NRR-106**

OFFICE	DPR/PLPB/PM	DPR/PLPB/LA*	DE/EICB/BC	DPR/PLPB/BC	DPR/PLPB/PM
NAME	JHolonich	DHarrison*	MWaters	KHsueh	JHolonich
DATE	9/30/16	2/9/17	3/24/17	3/31/17	4/3/17

OFFICIAL RECORD COPY

REGULATORY AUDIT REPORT FOR MAY 16-20, 2016, TOSHIBA "LICENSING TOPICAL REPORT FOR TOSHIBA NRW [NON RE-WRITABLE]-FPGA [FIELD PROGRAMMABLE GATE ARRAY]-BASED INSTRUMENTATION AND CONTROL SYSTEM FOR SAFETY-RELATED APPLICATION," UTLA 0020P, REVISION 2 (TAC NO. ME9861)

Background

The regulatory audit plan (Agencywide Documents Access and Management System (ADAMS) Accession No. ML16070A018) for the audit of the Toshiba facility in Tokyo, Japan detailed the plans and expectations for the trip. The audit was in support of the NRC staff's review of the Toshiba Power Range Monitoring (PRM) System and Oscillation Power Range Monitoring (OPRM) Unit Licensing Topical Report (LTR). The NRC staff's efforts on the audit are expected to support generation of a safety evaluation (SE) of the PRM system and OPRM unit to their potential use in safety related systems in domestic nuclear power plants.

Regulatory Audit Basis

The purpose of this regulatory audit was to gain information needed to determine if the software developed processes used, and the outputs of those processes have resulted in a PRM system and OPRM unit that meet regulatory requirements for safety system applications at nuclear power plants. This audit provided information necessary to complete the NRC staff's evaluation of the Toshiba LTR.

Audit Activities

The NRC audit team, consisting of Rossnyev Alvarado, Daniel Warner, and Samir Darbali from EICB visited the Toshiba facility in Fuchu, Tokyo, Japan, from May 16-20, 2016, to perform the regulatory audit. The following activities were performed during this audit:

1. Entrance Meeting

At the entrance meeting, the audit team provided an overview of the audit plan and objectives for the audit. Facility logistics and a detailed audit schedule were discussed.

The Toshiba Project Manager (PM) introduced a number of Toshiba staff members, including the Fuchu Operations-Energy Systems and Solutions General Manager, Design Engineers, Project Quality Assurance (QA) Group, Independent Verification and Validation (IV&V) teams, among others.

As part of the entrance meeting, the Toshiba PM provided a presentation including an introduction of the NRC staff as well as the Toshiba staff involved with the audit and it identified the planned shop tours and demonstrations. The presentation also provided an overview of the Toshiba FPGA-based platform and the experience they've had in Japan, as well as a description of the QA Programs used.

Factory Facility Tours and Demonstrations

The Toshiba staff provided a factory facility tour for the audit team. The audit team was able to view a demonstration of the PRM system and the OPRM unit, tour the cabinet fabrication facility, view a demonstration in the Power Platform Development Department (PPDD) System Development Room where Functional Elements (FEs) and Field Programmable Gate Arrays (FPGAs) are developed, and view a demonstration of an FPGA chip being burned in the room where the FPGA chips are manufactured. More details on these tours can be found in the attachments to this document.

2. Thread Requirement Reviews

The NRC staff was able to complete this audit activity successfully. For both the PRM system and OPRM unit, the audit team performed a thread audit of select system and software requirements with the intent of tracking implementation requirements through each phase of the development process. The audit used the Requirements Traceability Matrices (RTM) that were created for each phase. The following threads were evaluated for the PRM system during this audit:

- Response Time Requirements – Average PRM Upscale High-High
- Low Voltage Power Supply (LVPS) Module – power supply requirements

For the OPRM Unit, the following requirement threads were evaluated during the audit:

- R06-150: 5.2.1.3.0-12. (1) Input. The OPRM unit shall receive signals listed in table 5-71, unit input list.
- R37-YYY: 5.5.7.1.0-4. The communication data links to be provided for external systems have a one-way communication…

Detailed notes for the PRM requirements thread reviews are provided in Attachment 1 and for the OPRM requirements in Attachment 2.

3. Software Development and Independent Verification & Validation

The purpose of the IV&V portion of the audit was to confirm that the Toshiba IV&V activities were performed and documented per its approved processes, with a focus on record keeping, documentation, and management activities. In addition, during this review the NRC staff also evaluated if the IV&V team was sufficiently independent. The NRC staff was able to complete this audit activity successfully.

Detailed notes for this review are provided in Attachment 1 for the PRM System and Attachment 2 for the OPRM Unit.

4. Configuration Management

   The NRC staff reviewed the Configuration Management activities established for the PRM system and OPRM unit. For this audit activity, the NRC staff reviewed Nuclear Energy Systems & Services Division (NED), Nuclear Instrumentation & Control System Department (NICSD) and PPDD documents that describe configuration management activities, document control, design change control, and nonconformance control procedures. The NRC staff also observed how these procedures were implemented, and interviewed Toshiba personnel responsible for such activities.

   The NRC staff was able to complete this audit activity successfully. A detailed description of the NRC staff observations is provided in Attachment 3 to this audit report.

5. Software Quality Assurance

   The NRC staff met with NED and NICSD Quality Assurance (QA) groups to discuss QA programs and procedures used by NED and NICSD. The NRC staff was able to complete this audit activity successfully. Detailed notes for this review are provided in Attachment 1 for the PRM System and Attachment 2 for the OPRM Unit.

6. Secure Development Environment

   The NRC observed the secure development environment established at the Toshiba Fuchu Complex for the PRM system and OPRM. For this audit activity, the NRC staff reviewed Toshiba, NED, NICSD and PPDD procedures and guidelines that describe the secure development environment controls, observed how these security controls were established, and interviewed Toshiba personnel responsible for these activities.

   The NRC staff was able to complete this audit activity successfully. A detailed description of the NRC staff observations is provided in Attachment 4 to this audit report.

7. Commercial Grade Dedication

   NRC Staff reviewed the PRM System and OPRM Unit processes and procedures for Commercial Grade Dedication (CGD) of the components developed commercially. In particular, NRC Staff reviewed processes used to identify critical characteristics (CCs). Then the NRC staff reviewed how Toshiba evaluated these CCs during the dedication of commercial items. For this activity, the audit team selected several CCs and traced acceptance by reviewing all documents created and confirmed the information provided in the Final Technical Evaluation Report (FTER).

   The NRC staff was able to complete this audit activity successfully. A detailed description of the NRC staff observations is provided in Attachment 1 for the PRM System and Attachment 2 for the OPRM Unit.

8. Exit Meeting

During the exit meeting, Toshiba was provided with a summary of the audit team's observations and findings, and Corrective Action Requests (CARs) created during the audit.
Open items identified during the audit were included in the project open items list. Additionally, the audit team identified a list of documents to be posted in the portal so the NRC staff can determine if they should be docketed to complete evaluation activities. Conclusions

The NRC staff successfully completed all audit activities outlined in the audit plan. Several requirements threads were performed to ensure they were properly implemented through the life cycle. Interviews were conducted with Toshiba personnel from the IV&V, Design Engineering, QA, and Configuration Management groups.

The following observations were identified and discussed during this audit.

1. The identification and resolution of problems and anomalies identified during the IV&V process followed for the OPRM unit is not clearly described in the V&V plan submitted. The NRC staff requested clarification on the process used to identify and manage anomalies. To address this request, Toshiba provided a table describing each IV&V activity for each lifecycle phase, and the processes followed to review and identify anomalies.

2. The IV&V plans do not describe the methods used to record their review. For example, the use of design input sheet and the Vendor Document Checklist (VDCL) were not described in the IV&V plan. However, the IV&V plans identify the standards that describe these methods, but because these standards are not provided with the documents, the reviewer could not review the methods used.

3. The NRC staff found that QA procedures identified in the docketed plans were superseded. To address this problem, Toshiba provided a map of the NQ and AS documents used. Toshiba initiated CARs and Site-CARs (SCARs) to address inconsistencies. Toshiba prepared a document map identifying its document name, issue date, the AS and NQ standards referenced, and their applicable revision. Toshiba should consider including this as part of the baseline of the document

4. Use of project review meeting (PRM) and design review (DR) meetings to evaluate the design is not described in the LTR or in documents docketed. Toshiba relies on these meetings to review the design and identify problems and anomalies. The meeting reports are used to identify and record problems and anomalies. The process to use PRM and DR meetings should be explained.

5. The RTM docketed was for the system validation testing phase. This document traces the requirements from the System Design Description (SDD) to the unit Detailed Design Specification (DDS) and identifies the requirements that were validated in the module validation testing. However, Toshiba created RTMs for each lifecycle phases and how these RTMs are related and used for requirements traceability are not explain in the LTR.

6. When tracing requirements and reviewing system validation, The NRC staff could not find all requirements identified in the Equipment Design Specification (EDS) for the OPRM unit. Toshiba explained the EDS includes requirements for multiple units and not only for the OPRM unit. To facilitate the audit, Toshiba prepared a mapping of the requirements applicable to the OPRM unit.

7. The Commercial Dedication Instruction (CDI) for the AGRD module identifies a different OPRM Unit DDS that is identified in the RTM (same title, different number). During the audit Toshiba explained that it is the same document, but it is using a different number. Specifically, Toshiba uses a Toshiba Project Document No. (used for each project) and a Document filing No. (used by NICSD). The Project Control Document List (PCDL) identifies both, so people can use this for cross-reference. PCDL is the document list to control documents, and identifies those documents that require configuration management.

The following CARs were initiated as a result of the audit activities.

1. SCAR-16-011 issued to fix NQ-3019, which refers to AS-300A009 instead of NQ-3009.

2. SCAR-16-012 issued to describe the differences between QA and Quality Control (QC) in NQ-3019.

3. SCAR-16-010 issued to revise the IV&V plan NQ- 3019, which states that for classification of conditions adverse to quality refer to AS-300A009, but this standard was superseded by NQ-3009.

4. SCAR-16-016 issued to describe PCDL and verification follow sheet in NICSD IV&V Plan.

5. CAR-16-073 issued to describe VDCL and design input sheet in NED IV&V Plan.

6. SCAR-16-018 issued to describe the process to identify anomalies in the NICSD IV&V plan.

7. CAR-16-074 issued to address the discrepancy between the FTER and the Qualification Test Summary Report. Specifically, the FTER referred to the Qualification Test Summary Report as FPG-TRT-C51-1001 while the actual report number is FPG-TRTC51-0101.

8. SCAR-16-017 was issued to document in the Security Assessment Meeting Minutes how personnel have been registered for access rights to the project management system.

The following open items were identified during the audit.

1. Description of the classification scheme (safety function, important to safety) used for requirements identified in the commercial grade dedication of the OPRM unit.

2. Please describe the resolution of the observations, as well as the CARs issued during the audit. If software plans are revised, please provide new revisions.

3. Please place summary reports for Software Safety Analysis Reports (SSAR) from NED and NICSD in the portal and submit it on docket. This document is listed in ISG-06 for phase 2 submittal. The NRC only has the SSAR from the design phase. Therefore, the NRC staff asked Toshiba to docket the SSAR.

4. The Final Technical Evaluation Report was submitted with extra pages. Toshiba America Nuclear Energy (TANE) printed additional pages that belonged to the SSAR when TANE submitted the document to the NRC. Toshiba will submit the correct version to the NRC.

5. Please place the following documents in the portal, which were prepared to support the audit:
    a. IV&V team activity and action for anomaly
    b. CGD flow outline
    c. Mapping of design criteria in EDS
    d. Document map
    e. RTM Flow diagram
    f. Traceability of the CGD for the AGRD module

The NRC staff expects the licensee to provide responses to these open items to support completion of the Toshiba NRW-FPGA-based Instrumentation and Control System for Safety Related Applications safety evaluation.

Attachments
1. PRM System Audit
2. OPRM Unit Audit
3. Configuration Management
4. Secure Development Environment

Principal Contributors: Rossnyev Alvarado, NRR/DE/EICB
Samir Darbali, NRR/DE/EICB
Daniel Warner, NRR/DE/EICB

Attachment 1 – PRM System Audit

1.1 Requirements Thread for PRM:

The NRC staff performed thread audits of selected system and software requirements. The purpose of this activity was to track implementation requirements through each phase of the development process. The NRC staff used the Requirements Traceability Matrices (RTM) created for each phase of the system lifecycle. The following threads were evaluated for the PRM system during this audit:

- Response Time Requirements – Average Power Range Monitor (APRM) Upscale HighHigh
- LVPS Module – power supply requirements

1.1.1 Response Time Requirements – APRM Upscale High-High (Equipment Requirement Specification (ERS) Requirement 5.1.3.1):

The NRC staff traced the following requirement through each phase of the development process. This requirement states that the APRM Upscale High-High response time, which is measured as the total delay time from a step change of the Local Power Range Monitor (LPRM) input current to the change of the APRM trip auxiliary unit output, shall be equal to or less than 40 milliseconds.

Using the RTMs generated for each phase, the NRC staff was able to trace the response time requirement from the beginning of the project through the final system validation testing. This trace was only performed in one module (LPRM module). The remainder of this section will describe how the requirement was traced through each phase of the project.

In the Project Planning and Concept Definition Phase RTM, this requirement is identified as Item #10.

The Requirements Definition Phase RTM, indicates that item #10 from the Project Planning and Concept Definition Phase RTM is incorporated into Section 2.6, Response Time, of the LPRM Unit Design Specification (5G8HA748 Rev. 3). This section identifies that the combined response time of the LPRM Module, Transmit (TRN) Module, APRM Module, Digital Input/Output (DIO) Module and APRM Trip Auxiliary Unit totals 40 ms or less.

The Design Phase RTM indicates that the requirements of Section 2.6 of the LPRM Unit Design Specification are incorporated into Section 2.3, LPRM Data Output, of the [ ] FPGA Design Specification (5G8HA780 Rev. 2). This section identifies the output frequency for the [ ] FPGA as [ ] ms.

The Implementation Phase RTM indicates the requirements in Section 2.3 of the [ ] FPGA Design Specification are incorporated into Section 4.1, Very High Speed Integrated Circuit (VHSIC) Hardware Description Language (VHDL) Functional Testing, of the FPGA Test Specification (8T8H3396 Rev. 1) The VHDL Functional Testing identifies ModelSim to test the FPGA code. The ModelSim test confirmed the output frequency of the [ ] FPGA to be [ ] ms.

The Validation Testing Phase RTM indicates the requirements in Section 2.6, Response Time, of the LPRM Unit Design Specification are incorporated into Section 6.3 of the Unit Test Specification (5T8H6724 Rev. 3). Section 6.3 describes the process to check the analog output response of the LPRM. By using an oscilloscope, the pulse generator output signal and the LPRM analog output value were monitored. The mock input current signal to the LPRM was adjusted from [ ]% to [ ]% via step change while measuring the analog output response time. This testing is performed by transient monitoring the output of LPRM channel 1. The measurement is performed [ ] times and the expected test result is a response time below [ ] ms.

In the System Validation Testing Phase RTM, Item 10 from the Project Planning and Concept Definition Phase RTM is incorporated into Section 6.3.1 of the System Validation Testing Phase System Validation Test Procedure (FPG-TPRC-C51-0001 Rev. 2). This section describes the APRM Upscale (High-High) Trip Function and Response Time. It tests the response time at different microampere settings to ensure the trip of the Trip Auxiliary Unit is equal to or less than 40 ms from the time of the change in LPRM signals.

The test report results were documented in the Operability Test Record, FPG-06-ETR-001-03. Review of the final test results for APRM High-High Response Time measurement resulted in a measured response time of [ ] ms which met the original ERS acceptance criteria of ≤ 40 ms. Therefore, NRC staff successfully complete this audit activity.

1.1.2 LVPS Module – Power Supply Requirements (ERS Requirement 5.2.3.10):

During the thread audit, NRC staff traced the following requirement through each phase of the development process. This requirement states that the LVPS module supplies +5VDC, and +/-15VDC to the other modules in the unit.

Using the RTM that was created for each phase, NRC staff was able to trace the power supply requirement from the beginning of the project through the final unit testing. This trace was only performed through one module (FLOW module). The remainder of this section will describe how the requirement is treated through each phase of the project.

In the Project Definition and Concept Definition Phase RTM, this requirement is identified as Item #118.

At the Unit level, the Requirement Definition Phase RTM indicates that requirement #118 is incorporated into Section 3.6 of the FLOW Unit Design Specification (5G8HA750 Rev. 2). Section 3.6 describes the LVPS Module (HNS500). Item 4 of Section 3.6 identifies the

Nominal Output as +5V:[ ]A, +15V:[ ]A, -15V:[ ]A. At the Module level, the Requirement Definition Phase RTM indicates that requirement #118 is incorporated into Section 2.2, Power Supply Requirements, of the Flow Module Equipment Design Specification (5G8HA754, Rev 1). This section states the following: (1) +5 VDC: +5 V +/- [ ]% consumption current about [ ] mA, (3) +15 VDC: +15V +/- 5% consumption current about [ ] mA, and (4) -15 VDC: -15V +/- [ ]% consumption current about [ ] mA.

The Design Phase and Implementation Phase do not address this requirement since it is a physical requirement and these phases focus on the FPGA design and testing. Therefore, the next phase in which this requirement was traced was during validation testing.

In the Validation Testing Phase RTM, the requirements from Section 3.6 of the LVPS FLOW Unit Design Specification (5G8HA750 Rev. 2) are incorporated into the Flow Unit Test Specification (5T8H6726 Rev. 5). The test specification sections were reviewed and they detail the instructions on how to perform the tests and the standard used to determine if the tests are passed successfully.

TheNRC staff asked Toshiba for the results of the testing performed using the Flow Unit Test Specification. Toshiba provided the FLOW Unit Test Record (ATC-060393). Section 4.2 of the Flow Unit Test Record identifies that both LVPS1 and LVPS2 passed the power supply voltage adjustment when tested individually using the LPVS module operation test. Section 4.3 identifies that the measurement of power supply voltage for the FLOW unit also passed. For Section 5.3, Table 5.2.3 identifies the state of the STATUS module indicators and Trip Signal Output when turning on and turning off one of the two power supplies. When LVPS1 was turned off, both the FAIL (Y) (yellow light) and LVPS 1 (Y) lights were on and the Trip Signal Output was failed. When LVPS1 was turned on, these cleared. When LVPS2 was turned off, FAIL (Y) and LVPS 2 (Y) were both on and the Trip Signal Output was failed. When LVPS2 was turned on, all the lights cleared. Therefore, the FLOW Unit successfully passed the tests required by 4.2, 4.3 and 5.3, and met the requirements in the ERS. The NRC staff was able to successfully complete this audit activity.

1.2 PRM Independent Verification and Validation:

The NRC staff reviewed the software quality processes and procedures, interviewed Toshiba IV&V personnel and reviewed the IV&V process. In addition, the NRC staff took tours with Toshiba personnel to view the PPDD and Toshiba Design and Manufacturing Service Corporation (TDMS) fabrication areas where the FEs are created and tested as well as the process for fabricating the completed FPGAs.

Procedure AS200A130 Rev. 3, “Digital System Verification & Validation Procedure,” was one of the primary procedures reviewed for the PRM system. This procedure provides the software IV&V process for digital systems. The scope section identifies that the activities in the procedure are required for US Class 1E safety related digital system development and details the activities and employees that the procedure applies to.

As part of the IV&V audit, an interview was held with Toshiba IV&V personnel. The NRC staff and Toshiba reviewed the IV&V reports with particular emphasis how the different lifecycle

phases were performed by NICSD and then verified by NED. Toshiba created an IV&V report for each phase of the system lifecycle. The IV&V reports were primarily based on the old (original) process. However, there was a section where the new process was used because a portion of the NICSD IV&V Report needed to be re-verified. The Project Planning and Concept Definition Phase IV&V Report was prepared using the old process and was performed by NED on the completed NICSD IV&V report. Then NED prepared the ERS, Software Quality Assurance Plan (SQAP) and Preliminary Hazards Analysis (PHA) Report IV&V. The Requirement Definition Phase and Design Phase IV&V Reports were written by NED based on the NICSD IV&V Report documents. During the Implementation & Testing Phase, the IV&V team performed a review of the code. Any minor or major error messages generated were documented. Toshiba issued a supplement to the Implementation and Integration Phase V&V report as a result of not performing a dynamic timing simulation in the FPGA testing process. NICSD issued a SCAR and FPGA testing was performed to include the dynamic timing simulation. NED then reverified the Implementation and Integration Phase V&V Report using the new process and included it as Attachment 6 to Part V of the Licensing Topical Report.

During the interview, Toshiba indicated that FPGA testing included all connections between FEs being toggled and functional testing. The setup for testing is the same setup that was demonstrated during the tour. They also identified that the old process did not have QA personnel present in the FPGA burning room as they do now with the new process.

During the interviews with Toshiba staff, NRC staff observed that a special sticker is included on documents requiring an independent review that the reviewer must sign to ensure independence. QA inspections such as source verification are done by the IV&V team. After the job order was issued, NICSD then assigned individuals to the IV&V team. The Equipment Requirement Specification was prepared by NED. Table 6.1 of the SQA procedure identifies the NED Reviewer and approver for the various documents. The design and V&V processes described these activities and NRC staff confirmed they were performed as described.

NRC staff was able to successfully complete this audit activity.

1.3 <u>PRM Software Quality Assurance:</u>

The NRC staff reviewed Software Quality Assurance (SQA) documentation including FPG-PLN-C51-0002, “Software Quality Assurance Plan.” Section 3.1.1 of the SQAP references P-101, “NICSD Manufacture of FPGA-Based Equipment.” The NRC staff reviewed P-101. It identifies the process for developing and procuring digital systems to be sold as safety-related to commercial US nuclear plants or to be used in safety-related qualification activities. It contains a detailed description of the lifecycle from the Project Planning and Concept Definition Phase through the Requirements Definition, Design, Implementation and Integration, Validation Testing, and Operations and Maintenance phases.

Section 4.1.1 of the SQAP discusses the process for documenting concerns and transmitting them to NED, which is performed in accordance with NICSD Standard D-68016. The NRC staff reviewed D-68016, “Procedural Standard for FPGA Products Development”. This procedure describes the process to be followed by NICSD for the development of units for use in safety related FPGA products or to be used in qualification activities for such products. It

outlines aspects of the software development life cycle including requirements definition, design, implementation, testing, and how to report concerns during development.
The NRC staff interviewed Toshiba personnel regarding SQA. The NRC staff and Toshiba walked through the SQA procedure FPG-PLN-C51-0002, Rev. 2, "Software Quality Assurance Plan." Toshiba identified that in the beginning, FPGAs were identified as software and therefore a SQAP was used. When the FPGAs were first classified as software, the QA people didn't know how to handle it so the project team had to assist with the SQA. Now that the QA group is more familiar with FPGAs, they are now responsible for the SQA process for the OPRM unit. They also noted that there is an attachment to the SQAP that shows the mapping between the SQAP and EPRI TR-107330.

In the old process, PPDD was a sub-organization of NICSD and NED was responsible for the system level design. As a commercial vendor for NED any components, up to and including the unit level, coming from NICSD used the CGD process. As part of the process, work order sheets were prepared in accordance with the AS standard and this document clearly defines the roles and responsibilities for the employees involved while the group manager was responsible for assigning people their responsibilities for the project.

AS200A130 Rev. 3, "Digital System Verification & Validation Procedure." In particular, Section 6.5.2 discusses preparation of Nonconformance Notice Reports (NNRs) to document any test failure, test procedure errors or other nonconformances in accordance with AS-300A008, "Nonconformance Control and Corrective Action Procedure." NRC staff reviewed this document during the audit and determined it was applied appropriately. Also, the NRC staff discussed Software QA with the project personnel. Toshiba described the various ways to report defects and errors. NED uses Nonconformance Notification Reports NNRs for identification of product deficiencies. NICSD issued Vendor Nonconformance Notification Reports (VNNRs) in accordance with AS-300A006 whenever NICSD (as a commercial vendor for NED) identified any product deficiencies. For a process deficiency, Toshiba identified and tracked the deficiency using a Corrective Action Request (CAR). Toshiba identified that NNRs and CARs have similar significance levels: High (10CFRPart21), Significant (i.e., requires a Root Cause Analysis), Not Significant (i.e., Correction), Recommendation, and Other.

During the interviews with Toshiba staff, Toshiba explained that any CARs generated internally by NICSD were reviewed by NED as part of the verification process. If there was a nonconformance in the validation/testing phase, they would then go all the way back to the design phase, make the required changes and then re-do the activities for implementation/integration and then validation testing phases.

The NRC staff reviewed the following examples of NNRs, VNNRs, and CARs:

- NNR-06-001-1 (Issued August 2 2006):

  During the Environmental Tests, an APRM Inoperative alarm occurred. After investigation, Toshiba identified the cause of the failure to be water on the surface of the circuit board. Toshiba built a barrier to avoid condensation from the ceiling of the chamber and re-ran the tests with no failures. The equipment that was qualified will be installed in the main control room of a nuclear power plant. The environmental condition of the main control room in a

nuclear plant is non-condensing and there can't be water drops from the ceiling. Even if there was water drops from the ceiling, water can't contact the equipment because it is installed in a closed rack. Therefore, this failure cannot occur in a nuclear power plant.

- VNNR-07-001 (Issued July 27, 2007):

While storing components, Fuchu Complex had an incident where the relative humidity exceeded the limit due to weather conditions and shutdown of the building air conditioning. A dehumidifier was installed to prevent any future recurrence.

- CAR-07-014 (Issued May 11th, 2007):

The CAR identifies two issues. 1) Contrary to AS-200A111 R.1 and AS-200A112 R.1, a commercial grade survey plan was not issued. 2) The exhibits of AS-300A002 R8 are best suited for an audit or survey, but not for documenting very visibly via commercial grade survey that supplier controls meet Engineering requirements. An exhibit needs to be developed, or a separate procedure, for commercial grade surveys. To address both issues AS-300A002 was revised and impacted personnel were re-indoctrinated to the revised procedure.

At the end of the interview with Toshiba personnel, there were questions with regard to updates to procedures and software tools and how the training of employees is kept up to date with the procedures. Toshiba identified that when a QA procedure is revised and issued, it is distributed by paper to the various groups. Each group then indoctrinates the employees and an electronic record is used to track the indoctrination. When a software tool changes, they perform On the Job Training (OJT). If a new tool version is provided, the vendor provides information on the updates which is then provided to the designer as needed.

NRC staff were able to successfully complete this audit activity.

1.4 PRM Commercial Grade Dedication:

The NRC staff selected two Critical Characteristics (CCs) of the PRM system and followed them through the CGD process. The two characteristics for the PRM selected were Grounding/Shielding Requirements (Section 5.2.4.5 of the Equipment Requirements Specification (ERS)) and Failure Detection and Self-Test Requirements – Watchdog Timer (Section 5.1.6 of the ERS). To take these CCs through the CGD process, the NRC staff used FPG-DRT-C51-0102 Rev 0, "Final Technical Evaluation Report", which includes Appendix A, "Comparison Table of ERS/PQAP Requirements and Qualification Activities for Ensured Satisfaction." This table identifies: the ERS requirement, the EPRI TR-107330 item it corresponds to, how the requirements are confirmed, any remarks on the method selected for confirmation, any Critical Characteristics for Acceptance (CCA) and Design (CCD), and how the requirements are being verified. The following sections describes the results of this review.

1.4.1 Grounding/Shielding Requirements (ERS Section 5.2.4.5):

Section 5.2.4.5 of the ERS states: “The PRM system shall meet IEEE 1050 and EPRI TR102323 grounding requirements. This includes supporting connection to single point, multi-point and floating ground systems, and providing a ground connection point on each chassis. The PRM System shall meet IEEE 1050 and RG 1.180 shielding requirements. This includes providing shielding connection points for the I/O module field terminations.”

For the Grounding/Shielding Requirements, the FTER identified the CCAs as: unit model numbers, provision of grounding points and provision of shielding points. These were verified by the Source Verification Check Sheet and Record for Commercial Grade Dedication (FPG-06ESVR-0001, Rev. 0).

The Source Verification Check Sheet and Record for Commercial Grade Dedication (FPG-06-ESVR-0001 Rev. 0) identifies the Acceptance Plan (FPG-PLN-C51-0008 Rev. 1), the Item/Service Description, the NED Item/Service Identification Number (PN-0020614 Rev. 2), the supplier/manufacturer (Fuchu Operations – Industrial and Power Systems & Services 1, Toshiba-cho, Fuchu-shi, Tokyo-city), the supplier/manufacturer part numbers (, the applicable Toshiba purchase order (Job Order Sheet FPG-JOS-C51-0001, Rev. 5), and the record of acceptance for the various CCAs being verified with source verification. The record includes verification of the applicable requirements for Grounding/Shielding Points within the document and identifies them as acceptable with a signature and date.

Other documents reviewed that were identified in the “Summary of Document Relationship (IM-2014-001106)” provided by Toshiba include: the Procurement Planning Sheet, Technical Procurement Specification, QA Specification, Job orders to NICSD, and the Acceptance Checklist for Commercial Grade Items. Toshiba provided these items to NRC staff fo review during the audit.

The Procurement Planning Sheet (PP-FPG-IM001 Rev. 1) provides a plan including schedule for use in preparation of the PRM equipment. It identifies the various stages in the process from Preparation of a Dedication Plan all the way to Packing Inspection & Shipping Inspection along with proposed schedules.

The Technical Procurement Specification for Test Specimen Units, Interconnecting Cables (PN0020614 Rev. 3) identifies in Appendix A the design requirements that are applicable, along with the conditions, exemptions, modifications and clarifications. Appendix A identifies that the requirements in 5.2.4.5 of the ERS for Grounding and Shielding are only partially required. The Additional Information for the Procurement, located in the Technical Procurement Specification, identifies that the vendor is not required to verify with IEEE1050 and TR-102323 and the vendor will only provide units specified by 5B8H5916 Rev. 2 as the baseline.

The Quality Assurance Specification for Test Specimen Modules (FPG-RQS-A70-0006, Rev. 0) defines the QA requirements necessary for design of the PRM modules. These quality assurance requirements include QA program requirements, submittal documents, right of access, nonconformance and corrective action, extent and frequency of monitoring and source surveillance and inspection, QA Record requirement, pre-fabrication meeting, identification and

certification of material, acceptance, notification procedure, QA/QC interface, past nonconformance reflection, change request from vendor, special process, prevention of contamination, spare and replacement parts, process control, dimensional inspection, translation control and special mention matter.

The Job Order Sheet (FPG-JOS-C51-0001 Rev, 7) identifies the components being ordered, the boundary of the order (design, material procurement, fabrication, examination, and testing), the requirements imposed on the vendor (i.e., Procurement Specification PN-0020614, Equipment Requirement Specification FPG-RQS-C51-0001, Software Quality Assurance Plan FPG-PLN-C51-0002, Master Configuration List FPG-CFM-C51-0001, Verification and Validation Plan FPG-PLN-C51-0006 and the Project Planning and Concept Definition Phase Requirement Traceability Matrix Report FPG-DRT-C51-0010). In addition, it includes documentation requirements, nonconformance requirements, and spare and replacement part requirements.

The Acceptance Checklist for Commercial Grade Item (ACLFPG-JOS-C51-0001-01) identified the PRM system as acceptable and referenced the Product Quality Certificate for the PRM system (PQC-FPG-JOS-C51-0001-01 Rev.0). The Acceptance Checklist also identifies the Quality Record List, QRL-05001 Rev. 2, which also identified the PRM as acceptable. There were no VNNR, NNR or CAR issued for this item. The PRM system was deemed acceptable and an NED QA Engineer signed off on the document. The Revision block contained signatures from the Preparer, Reviewer and Approver within the Project QA group. Finally, the attachment identified all the parts received and the associated item ID numbers, and quantities. NRC staff confirmed that the equipment being tracked through the CGD process was included. Therefore, NRC staff were able to successfully complete this audit activity.

1.4.2 Failure Detection and Self-Test Requirements Item C – Watchdog Timers (ERS Section 5.1.6):

Section 5.1.6(c) of the ERS states: “Monitoring of the FPGAs with a watchdog: A watchdog timer shall monitor each FPGA that operates periodically. [A group of FPGAs that operates serially may be monitored by [ ] watchdog timer, as long as the watchdog timer can detect the [ ]. If a [ ], the module containing the FPGA shall generate an inoperable signal. The failure of the [ ] shall not generate an inoperable signal, but a Minor Failure Alarm, except for the LPRM module. The watchdog timers shall be external, and not built into the FPGA logic, nor shall the watchdog timer depend on the clock signal used by the FPGA.”

For the Failure Detection and Self-Test Requirements, the CCAs were identified in the FTER as: unit model numbers, configuration identifications of units, quality of design and manufacture, and fault condition signal generated during faults. These were verified by Commercial Grade (CG) Survey Checklists (E05SC-001 Rev. 0 and E06SC-001 Rev. 0), Source Verification Check Sheet and Record for Commercial Grade Dedication (FPG-06-ESVR-0001, Rev. 0), the Qualification Test Summary Report (FPG-TRT-C51-1001, Rev. 0), and the System Validation Test Record (FPG-06-ETR-001, Rev. 3). NRC staff reviewed these documents and found that the CCAs were appropriately addressed. Other documents reviewed that were identified in the “Summary of Document Relationship (IM-2014-001106)” provided by Toshiba include: the

Procurement Planning Sheet, Technical Procurement and QA Specifications, and Job orders to NICSD.

The Procurement Planning Sheet (PP-FPG-IM001 Rev. 1) provides a plan including schedule for use in preparation of the PRM equipment. It identifies the various stages in the process from Preparation of a Dedication Plan all the way to Packing Inspection & Shipping Inspection along with proposed schedules.

The Procurement Specification for Test Specimen Units, Interconnecting Cables (PN-0020614 Rev. 3) identifies in Appendix A the design requirements that are applicable, along with the conditions, exemptions, modifications and clarifications as specified. Appendix A identifies that the requirements in 5.1.6 of the ERS for Failure Detection and Self-Test are required in full.

The Quality Assurance Specification for Test Specimen Modules (FPG-RQS-A70-0006, Rev. 0) defines the QA requirements necessary for design of the PRM modules. These quality assurance requirements include quality assurance program requirements, submittal documents, right of access, nonconformance and corrective action, extent and frequency of monitoring and source surveillance and inspection, QA Record requirement, Pre-fabrication meeting, identification and certification of material, acceptance, notification procedure, QA/QC interface, past nonconformance reflection, change request from vendor, special process, prevention of contamination, spare and replacement parts, process control, dimensional inspection, translation control and special mention matter.

The Job Order Sheet (FPG-JOS-C51-0001, Rev. 7) identifies the components being ordered, the boundary of the order (design, material procurement, fabrication, examination, and testing), the requirements imposed on the vendor (Procurement Specification PN-0020614, Equipment Requirement Specification FPG-RQS-C51-0001, Software Quality Assurance Plan FPG-PLN-C51-0002, Master Configuration List FPG-CFM-C51-0001, Verification and Validation Plan FPG-PLN-C51-0006 and the Project Planning and Concept Definition Phase Requirement Traceability Matrix Report FPG-DRT-C51-0010). In addition, it includes the documentation requirements, nonconformance requirements, and spare and replacement part requirements.

The CG Survey Checklist E05SC-001, Rev. 0 includes the following sections: organization and planning ([ ] observation found), design control, procurement control ([ ] observations found), material identification and control, manufacturing process ([ ] observation found), inspection and test control, measuring and test equipment control, and software control ([ ] observations were found). Toshiba prepared E05SR-001 R1 CG Survey Report which contains a more detailed breakdown of the observations. This document is reviewed below.

CG Survey Checklist E06SC-001 was also reviewed to ensure CGD was appropriately addressed. It describes the following areas: organization and planning, design control, procurement control, material identification and control, manufacturing process, inspection and test control, measuring and test equipment control, software control. It also included confirmation of supplementary requirements, which were found at the previous CG survey (E05SC-001). It identified [ ] observations in the Organization and Planning section. After further evaluation by Toshiba personnel, [ ] observation was removed and the remaining [ ] observations were addressed.

CG Survey Report E05SR-001 Rev. 1 records the results of the CG Survey Checklist E05SC001 Rev. 0. The audit scope was to: 1) evaluate selected processes to determine whether the QA Program and its implementation of the CG Vendor provides reasonable assurance that CC are adequately controlled. This CG Survey was performed to accept commercial grade items for safety-related application in the commercial grade dedication. 2) Evaluation of CG Vendor performance. As a result of the evaluation, the draft PTER identified CCs that needed to be added and included in the verification process. 3) Procurement source evaluation for registration of a prospective vendor for commercial grade items and/or services used for safety-related application. The Survey Report identified [ ] observations. Of the [ ] observations, the PTER incorporated [ ] of them as additional CCs.

NRC staff reviewed FPG-06-ESVR-0001, "Source Verification Check Sheet and Record for Commercial Grade Dedication" (also called Witness Inspection Record) as part of the audit. Since the watchdog timer is an internal feature, it is included in the CCA for fault condition signal generated during faults. There is a sub-item for self-test functions and surveillance testing capability for modules. The NRC staff's review of FPG-06-ESVR-0001 determined the watchdog function was addressed.

As part of the audit, NRC staff reviewed the final validation test results. FPG-TPRC-C51-0001 identifies the system validation test requirements for the PRM equipment. FPG-06-ETR-001 is the system validation test record for the PRM. FPG-06-ETR-001 included the testing of the watchdog function for the various modules. Each module was tested to confirm the watchdog function and to ensure an alarm resulted when the watchdog function was tested. The alarm cleared when the watch dog function test was completed. Test personnel initialed and identified the results as SAT. The test sheets were also marked SAT and signed in the 'Recorded by' box and 'Reviewed by' box with a review date marked. The review by NRC staff determined the watchdog timer function was addressed.

FPG-PLN-C51-0003, "Qualification Plan" references the following documents and therefore they were reviewed.

NRC staff reviewed AS-200A110 the "Procedure for Commercial Grade Items and Services". The purpose of AS-200A110 is to describe how NED applies the appropriate elements of the 10CFR50 Appendix B program to commercial grade items and services when they are procured for use in applications where Appendix B requirements apply. There is a statement in Section 8.1 of the qualification plan that identified three criteria for using CGD for procurement taken from AS-200A110. NRC staff confirmed the revision of AS-200A110 in effect for the PRM project does include the three criteria discussed in the qualification plan. The NRC staff noted that later revisions of AS-200A110 removed these criteria. Section 9 of the qualification plan included a statement that identified a process in Figure 1 of AS-200A110 that was used to perform the procurement and qualification of the PRM test system. Staff reviewed Figure 1 of AS-200A110 during the audit and compared to the document relationships identified in Figure 91 of the qualification plan. The review determined that all of the aspects identified in Figure 1 of AS-200A110 were incorporated into the qualification plan.

Section 9.2 of the qualification plan identified an NED test control procedure. During the audit NRC staff questioned Toshiba staff to determine what document this actually referred to. Toshiba's response was that the NED test control procedure is actually FPG-TPRC-C51-0001, "PRM System Validation Test Procedure". NRC staff reviewed the test procedure during the audit and identified that it defines the instructions for the test setup and testing performed on the PRM test system for the PRM system qualification project. It also includes the instructions for verification of the software tools used in the qualification testing of the PRM system.

Section 9.2 of the qualification plan discusses hold points and other special requirements that would be identified in the technical procurement specification as needed to permit acceptance of the items. The technical procurement specification was reviewed and the test specimens did not require any special requirements or hold points for procurement and therefore none were included.

Section 9.2 of the qualification plan also discussed source verification. During the audit the NRC staff reviewed source verification checklists FPG-06-ESVR-0001 and FPG-06-ESVR-0003 for the test unit and associated packaging. Both documents identified the required activities by NED. In addition, they identified that in-process source verification was performed and the results were document in the source verification record. In addition, CCAs were identified and marked as either acceptable or unacceptable. For the test unit, all CCAs were identified as acceptable.

Finally, the Qualification Plan requested a review of the commercial grade survey of the Fuchu complex. The staff reviewed survey checklist E05SC-001 and the associated survey report E05SR-001. The results of the review can be found earlier in this section.

NRC staff were able to successfully complete this audit activity.

Attachment 2 – OPRM Unit Audit

Quality Assurance

The NRC staff met with NED and NICSD QA groups to discuss QA programs and procedures used by NED and NICSD. The Power Systems Company Nuclear Energy (PSNE) QA Program Description (QAPD) establishes the QA program for Toshiba. The NRC staff reviewed Nuclear Energy QA Program Description, Procedure 44014, Rev. 10. This document describes how the QA program meets all applicable regulatory, codes and standards requirements of 10CFR50, Appendix B, and 10CFR21. This QA program controls the design and procurement of items and services that prevent or mitigate the consequences of postulated accidents that are supplied to overseas nuclear facilities. This document defines the organization, roles and responsibilities, and identifies the AS standard procedures that are part of the QA process. In addition, the project QA manual could be created to supplement the QA programs and provide specific contractual requirements.

Toshiba prepares its "Common Quality Assurance Specification for NRW-FPGA-based I&C System Qualification Project." This document provides the QA specification to be included in the job order from NED to NICSD for each project.

The QAPD includes AS standards. For each site, the companies identify what AS procedures applied to them depending of the scope of work. So for NICSD, The NICS-QA defines which AS procedures applied to NICSD. The applicable AS procedures are identified in NQ-1003. NQ1003 also identifies if an AS procedure is replaced by another procedure (e.g., NQ procedure) and recent modifications to AS procedures, and whether they are applicable to NICSD. NICSD has created its own specific QA procedures to complement AS standards. These are identified as NQ standards.

The NRC staff noted that the software plans do not identify the revision of the AS and NQ procedures used. So it is not clear how someone knows what QA procedure was used, especially when significant modifications were made or AS procedures were replaced by NQ procedures. To address this, Toshiba provided a mapping that identified the software plan, project document identification (PDI) number, filing number, revision, date issued, and the standards referenced (both AS and NQ). The following examples were observed:

> Equipment Design Specification, PDI number: FC51-3002-1000, filing number: 5B8K0029, Revision: 4, Date issued: 21-jan-14, standards used: AS500A007, NQ-2004, NQ-2030, NQ-2036, NQ-2037, NQ-5001, NQ-5003, NQ-5004.
>
> NICSD RTM, PDI number: FC51-3704-1004, filing number: RTM-JHS-000039, Revision: 4, Date issued: 12-nov-13, standards used: NQ-2015 rev 5.
>
> NICSD Software Configuration Management Plan, FA-32-3708-1000, 5B8K0036, Revision: 1, Date issued: 7-may-12, standards used: NQ-2024, 2033, 2035, 3006, 3019, 4001.

The NRC staff mentioned that Toshiba should consider including the revision of the

QA procedures referenced in its documents. The NRC staff asked for clarification of the roles and responsibilities for the NICS-QA and NICS-QC because the descriptions in the SQAP (FA32-3701-1001) were not clear. Toshiba explained the NICS-QA is responsible for issues related with the QA procedures and audits. NICS-QC is more directly involved with testing and validation. NICS-QA uses CAR to identify nonconformances and problem. NICS-QC uses NNR. Toshiba noted that their roles are described in NQ-3019. However, when the NRC staff reviewed NQ-3019, we found the descriptions provided for NICS-QA and NICS-QC were similar. To clarify the role of these organizations, Toshiba issued SCAR-16-012.

As part of the QA program, NED and NICSD performed audits and surveillances of their supplier. The NRC staff reviewed the QA procedures that describe the process, as well as examples of surveillance reports prepared. NICSD uses its NQ-3022, Internal Audit Procedure, which describes the method to perform internal audits and how to report the results. This procedure is used to verify compliance with the QA program. NICS-QA is responsible for this audit. The NRC staff's observation regarding survey reports are included in the description of commercial grade dedication (CGD).

The NRC staff also reviewed NQ-3005, "Procedure for Evaluation of Suppliers," which describes the method of the evaluation and qualification of suppliers for procured items and services. NICS-QA is responsible for this evaluation. Qualification of suppliers requires performing a commercial grade survey for non-Appendix B grade items or services. When the evaluation result is acceptable, the manufacturer is registered on the qualified vendor list (QVL) with critical characteristics. Further descriptions of vendors' evaluations and surveys are provided in the section that covers CGD.

The Toshiba software plans referenced several QA procedures that were not docketed. The NRC staff reviewed these procedures for further clarification of the processes followed. Below are summaries of the QA procedures reviewed.

AS-300A005, "Preparation Procedure of Source Verification Report." This procedure describes preparation process, contents and form for Source Verification Report in order to document the results of the source verification.

AS-200A110, "Procedure for Commercial Grade Items and Services." This procedure describes how NED applies the appropriate elements of the 10CFR50, Appendix B QA Program when commercial grade items (CGIs) and services are procured and accepted for use in applications where the requirements of 10CFR50, Appendix B apply. This procedure states the Engineering/Design Group performs an initial evaluation of the commercial grade item/service to confirm that the CGI/service has the potential to satisfy the safety functions and design requirements. Then they develop a dedication plan for the evaluation, procurement and dedication of commercial grade items or services.

NQ-4001, "Commercial Grade Dedication." This procedure describes the process for the dedication of CGI intended for use in safety-related applications. This procedure also

explains how to prepare a Commercial Dedication Instruction (CDI). The CDI identifies CCs of the item and the dedication method(s) to be used to verify the critical characteristics. The CDI also identifies the function and determine the functional mode and the functional classification of components or parts. Identify Critical Characteristics for Design (CCD) and CCAs. At the completion of verifying all CCA, a CGD report should be prepared.

NQ-2034, “Procedural Standard for Control of Software Tools Used with FPGA Based Systems.” This procedure describes the software tool control process to be followed by NICSD for development of safety related FPGA-Based Systems, or for qualification activities for such products. Tools are controlled by the Software Tool Information Sheet. Software Tools are validated to demonstrate that they produce the intended results. The identification of the Software Tools used for the development are recorded in the Master Configuration List (MCL)

NQ-2025, “Preparation Procedure for Procurement Document for CG Items & Services.” This procedure describes the development of NICSD procurement documents especially to be applied for CGIs (parts, materials and equipment) and services.

NQ-2030, “Procedural Standard for FPGA Products Development.” This procedure describes the development process of FPGAs, including design, IV&V integration and testing.

NQ-2031, “Procedural Standard for FPGA Device Development.” This procedure describes the development process for FPGA devices, which includes logic programmed by VHDL to perform the required functions. In particular, it describes development and configuration of FPGA devices, and the integration of these FPGAs into modules and units for the system-based units.

NQ-2032, “Procedure Standard for FE Development.” This procedure describes the process to develop FEs to be used in safety related FPGA products. This procedure also describes the lifecycle for the development of the FEs, including, design, testing IV&V, integration in FPGAs, and modifications. This procedure must conform to NQ-2030.

NQ-3016, “Software Test.” This procedure describes activities and responsibilities to establish the software test for safety-related items, including test plan, test specification, QC test plan, test procedure, configuration management, problem reporting and corrective action, and preparation of test reports and records.

E-68007, “Design Review Control Procedure.” This PPDD procedure describes the design review meeting to determine if the product meets quality requirements. The procedure describes the type of meeting, participants required and the items to be confirmed. After the meeting, a meeting minutes report should be written identifying open items. During the audit Toshiba showed a design process flowchart for the FPGA-based system that illustrates when these meetings are required. The design process cannot continue if these meetings are not held. For example, in the design phase there are two design review meetings, DRB2 and DR-C. DR-B2 occurs after the module design specification is created, and DR-C occurs

after the FPGA is designed. An NICSD inspector is required to attend both meetings for oversight of PPDD activities.

The NRC staff reviewed training records for NED and NICSD personnel involved in the design and testing of the OPRM unit. The following examples show the information observed:

Personal training record PIR-13-88025810. NICSD IV&V team
Identifies courses required and when they were taken.
Approval of this form was performed by a senior manager.

Personal training record PIR-05-83011510. NED Nuclear QA department.
Identifies courses required and when they were taken. It also identifies training to be taken and the due date.
Approval of this form was performed by a senior manager.

Non-conformance Control and Corrective Action

The NRC staff met with NED and NICSD QA groups to discuss the process followed to identify and control non-conformance notices and corrective action reports. Nonconformances are used to identify non-conforming items and documents for safety related items and services. Corrective action reports are used to identify conditions adverse to quality. Toshiba explained NED uses Nonconformance Notice Reports (NNRs) in accordance with AS-300A008 and Corrective Action Requests (CAR) in accordance with AS-300A009. NICSD uses Site (S)NNR in accordance with NQ-3019 and Site (S)CAR in accordance with AS-300A009.
However, the NED IV&V plan (FA10-3709-0001) identifies AS-300A008 for the process for NICSD to follow to control its nonconformances, and the NICSD IV&V plan (ADAMS Accession No. ML15261A655) identifies NQ-3019. Toshiba explained that this was a modification made to the NICSD QA program, and NQ-3019 is the correct procedure to use. Toshiba opened SCAR16-018 to review its documents and identify the correct procedure for NICSD to identify nonconformances.

NQ-3019 Rev. 7 describes the process to control non-conforming items and documents for safety related items and services at NICSD. The manager of NICS-QA has overall responsible for these activities. The manager of NICS-QC is responsible for control and verification of disposition results. When a non-conformance is identified, NICS-QC must be notified. NICS-QC will determine if following NQ-3019 or NQ-3006. Specifically, if the nonconformance occurred in NICSD, then Toshiba used NQ-3019 (SNNR). If the nonconformance occurred in the supplier, then Toshiba used NQ-3006 (VNNR). For non-conformance originating in PPDD, NICSD uses the term VNNR, in which the ‘V’ indicates a vendor. In addition, this procedure states that NICSQA should prepare a SNNR-I for items related to QA program, and NICS-QC should prepare a SNNR-I for items related to project activities. This procedure also defines the criteria for determining if a non-conformance affect quality and then perform a root cause analysis. In this case, Toshiba prepare s SNNR-II corrective action. This also includes evaluation of the corrective action to determine if report in accordance with 10CFR21 is necessary. SNNR-I should include the disposition and completion date. If a SNNR-II is issued, then NICS-QA manager will approve disposition. In addition, NQ- 3019 refers to AS-300A009 for classification of conditions adverse to quality. However, the NRC staff found in NQ-1003 Rev. 20 that

AS300A009 was replaced by NQ-3009. Toshiba issued SCAR-16-010 to correct that for classification conditions adverse to quality refer to NQ-3009.

NQ-3006 Rev. 3 describes how to control and disposition non-conformance of items and services procured by NICSD to produce a safety related product. The manager of NICS-QC is responsible for these activities. This non-conformance is identified as a VNNR. The VNNR includes recommended disposition and technical justification. The VNNR is evaluated to see if they should be made into a corrective action. If so, they should follow the process described in NQ-3009. NICSD logs VNNR in the vendor-NNR log. The NICS-QA showed this log to the NRC staff.

The NRC staff reviewed NQ-3009, “Corrective Action Request Application Procedure.” This procedure describes methods and responsibilities to address conditions adverse to quality and control of corrective action for safety related items at NICSD. This procedure states NICS-QA is responsible for this activity.

The NRC staff requested examples of nonconformances and corrective action reports created for the OPRM unit. These are the examples reviewed during the audit:

SNNR-I-13-002
Insufficiency of FPGA test cases to verify connections between FEs.
Solution identified: perform additional FPGA testing.
This required revision of FPGA test procedure, test reports and module MCLs
It didn’t require SNNR-II.
The attachment identified the required modifications to address this issue. For example test more patterns for every channel to check the independence of each channel. This includes the FPGA test report that confirms these issues were addressed and tested.

SVNNR-11-001
Generated by PPDD to describe that the result of FPGA timing evaluation was not documented, even though the evaluation was complete and no problem was found.

SVNNR-11-002
PPDD submitted this report to describe that FPGA timing evaluation was not performed by dynamic simulation. This report provided explanation and proposed resolution – include timing requirement in the standard.

SCAR-12-005
NICS-QA issued this CAR to identify that the sub-supplier did not include the required information. The corrective action was to provide the information required.

In addition, the NRC staff reviewed AS-300A006, “Nonconformance Control Procedure for Procured Items and Services,” which describes the process to control procured items that do not meet NED procurement documents or approved documents. However, for PPDD activities, NICSD used the process described in NQ-3006. AS-300A006 defines nonconformances as deficiencies in characteristics, documentation, or procedures that render the quality of items or activities unacceptable or indeterminate. This procedure also describes the process for

evaluation and disposition of the VNNR. When a disposition is determined to not meet the original requirements, the impact to the related documents will be evaluated. After the responsible organization Manager approves the VNNR, it is transferred to the Project QA Manager for approval.

Regarding 10CFR21, Toshiba uses its Procedure 4810, "Reporting Procedure for Defects and Non-Compliances under USNRC 10CFR21." The NRC staff reviewed Rev. 4. This procedure describes activities for ensuring compliance with the requirements of 10CFR21, "Reporting of Defects and Noncompliance". Specifically, Toshiba evaluates non-conformances to determine if the defect could create a substantial safety hazard exists. This procedure also describes the procedure for reporting of defects and noncompliance under 10CFR21 and notification to the NRC

Commercial Grade Dedication

Because part of the OPRM unit development process was performed by PPDD (in accordance with its QA program), the NRC staff reviewed the CGD process used. The NRC staff selected the AGRD module and traced its development and dedication to observe the process followed. The NRC staff reviewed the information provided in the FTER.

The FTER explains that before placing a purchase order to PPDD, NICSD performed a preliminary evaluation of PPDD and TDMS. This evaluation included CG surveys of PPDD, which were summarized in Survey/Audit Report Nos. SE09SR-001 R0, SE10SR-001 R0, and SE10SR-001a R0. The NRC staff reviewed these reports. The Survey/Audit Report SE09SR001 described PPDD QA capabilities. The SE10SR-001 R0 describes the evaluation of PPDD testing process for the modules. The SE10SR-001a R0, describes the 2010 survey of Fuchu Complex, in particular FPGA and FE development. The survey team accepted the module after resolution of findings, which were resolved later in 2010. These survey reports list all findings and recommendations with any associated CARs, if identified, and then how and when the issues were resolved.

In addition, NICSD evaluated the PPDD QA process to work with TDMS, its sub-supplier for printed circuit boards (PCB). This evaluation was recorded in the Survey/Audit Report SE09SR002. The NRC staff observed this report summarizes the evaluation and lists all findings and recommendations.

The modules used FPGAs purchased from Microsemi SoC (formerly Actel). Therefore, NICSD performed a survey of Actel in November 2009, which was recorded in the Survey/Audit Report SE09SR-002. The NRC staff observed this report summarizes the evaluation and lists all findings and recommendations.

NICSD QA process requires them to audit or evaluate PPDD every year and perform CG survey every 3 years. The NRC staff reviewed several examples of survey reports. When performing this activity, the NRC staff noted that audits were not performed every year as required by NQ3022. Toshiba explained that it was an error in the SQAP (FA32-3701-1001), that in reality they do not perform an evaluation the year they performed the CG Survey. Toshiba issued SCAR16-0015 to correct the description in the SQAP.

The NRC staff reviewed the following survey reports: SAER-10-004, annual evaluation of Actel; SAER-10-002, annual evaluation of TDMS; SAER-11-002, annual evaluation of TDMS; SE12SR-004, 2013 commercial grade survey of Microsemi; SE15SR-001, most recent CG survey of PPDD to evaluate its manufacturing process of I&C equipment. The NRC staff observed these survey reports includes documents reviewed, checklists and results.

During the preliminary evaluation of PPDD, NICSD requested information about the modules to be purchased for the OPRM unit. This information is summarized in FTER, Table 9-1. Specifically, this table lists the FPGA control sheet for the FPGAs that constitute the module. For the AGRD module, the NRC staff selected [ ], FPGA control sheet: FDFG-10-0011M. This FPGA control sheet was reviewed during the audit. This control sheet included the following information, among other:

FPGA code name: [ ]
Number of code: FPC-09-0001-M
Checksum: 87CF
Fusemap registration in NICS-QA: NB1081-01-001-C
FPGA specification: 5G8HB793, Rev. 5
FPGA test procedure: 8T8H3614, Rev. 3
FPGA test report: 9H8H1085, Rev. 0
FPGA media no. (DVD): FPGA-12-0069-M, date 2012.7.18
This sheet Identifies tools used and their version. For example, Synplify for Actel Version 8.2b. It also identifies the source code for each component.

The NRC staff reviewed the following documents referenced in the control sheet:

- FPGA Design Specification 5G8HB793, Rev. 5. It defines the scope and applicable documents, including PPDD's E procedures, FPGA code (i.e., FPC-09-0001-M) and type, flow diagram for module, pin assignments, functional description, I/O signal assignment, and block diagram.

- FPGA Test Procedure 8T8H3614, Rev. 3. It defines the scope, reference documents, code number, type, testing environment (identifies software, controlling division, equipment control number), test tools, input signals and simulation items, and input signals for testing serial output.

- FPGA Test Report: 9H8H1085, Rev. 0. It shows the completed test procedure. The NRC staff confirmed the number of code: FPC-09-0001-M and FPGA type A54SX72A was the same as the one identified in the FPGA design specification. The NRC staff observed each step had a pass or fail note, who did the test, and when it was done.

After completing the preliminary evaluation, NICSD issues a job order to PPDD, procurement planning sheets and procurement documents. For the OPRM unit, NICSD issued job order Engineering Communication Sheet (ECS)-JHS-015392 (Rev. 4) for the purchase of OPRM modules from PPDD. This sheet references another job order sheet that provides the detail

technical description (MEM-JHS-000025, Rev. 2). The NRC staff reviewed these sheets and found them consistent with the documents listed above.

Job order MEM-JHS-000025 Rev. 2 from NICSD to PPDD provides technical specification for the parts requested, in this case the modules for OPRM. For the AGRD module, this job order identifies the following information:

- Module details - equipment no. (type): HNS0420B00000, quantity, Procurement specification, device order no. 9P04482PB2113B302, tools and their versions (e.g., VHDL simulator, ModelSim, version 6.0b), Safety class 3, Quality group class: Class C, Electrical classification 1E.
- References - purchase specifications for each module (e.g., Purchase Specification for AGRD Module (5Q8K0020 Rev.3)) and the RTM for the OPRM (RTM-JHS-000045 Rev.0)) and Compliance traceability matrix (CTM) for NQ-2037 (FDS-JHS-000175, Rev. 0, which identifies general requirements in NQ-2037 and specific requirements from NICSD to PPDD.)
- Supplier's document list. For example: FPGA Implementation Evaluation Report (including STA evaluation, netlist confirmation results, source code confirmation results), which should conform to E6817 (PPDD procedure). Submittal category for IR (independent review) review. Document to be submitted electronically using NUPDM 2 system.

In addition to the job order sheet, NICSD prepared the procurement planning sheets, identified in Table 9-2 of the FTER, and the purchase specification for each modules, identified in Table 93 of the FTER. The NRC staff reviewed the Procurement Planning Sheet, FC51-3611-1000 Rev. 0, for the procurement of modules from PPDD for the OPRM equipment. This planning sheet identified the commercial grade modules to be purchased, specifically, the HNS series for the LVPS, DIO, RCV, TRN, CELL, AGRD, PBD, DAT/ST. This planning sheet also defined: the procurement activities to be used (e.g., evaluation of vendors), AS/NQ standards (e.g., NQ3005), description of activities (e.g., evaluation of unqualified vendors), group responsible (e.g., NICS-QA), date, remark (e.g., the vendor is listed in the qualified vendor list. The annual evaluation was performed). The NRC staff also reviewed the purchase specification for the AGRD Module, procurement document 5Q8K0020. This purchase specification identified: the approved manufacturer (PPDD), product, conforming standard, shape, dimension, performance, characteristics, components, testing and inspection (tests and inspections shall be performed by PPDD), and special requirements (for testing and inspection PPDD shall prepare and submit the test procedure which indicates: applicable standards and test methods, inspection items, records, and judgment conditions.

To support the activities required for CGD of the modules purchased from PPDD, NICSD prepared Commercial Dedication Instructions (CDIs) for each module. The CDI for the AGRD module, document No. 9B8K0048, identifies the technical evaluation and acceptance criteria for the module. The results from the acceptance activities were summarized in the CGD reports, which are listed in Table 10-6-1 of the FTER. For the AGRD module, Toshiba prepared the Commercial Grade Dedication Report No. 5B8K0084. This report documents CGD results for

the AGRD in accordance with NQ-4001 procedure. NICSD found all critical characteristics for acceptance were confirmed. For example, this report identifies the following:

> Supplier: PPDD. Sub-supplier: TDMS
> Job order ECS- JHS-015392, Rev. 4
> Order no. for PPDD 9P04482 PB 2113 B302
> Product: AGRD module/ HNS0420
> CDI for module: 9B8K0048
> Proc doc. No. 5Q8K0020 (same that is identified in CDI and FTER)
> Identifies FPGAs in the module. The NRC staff confirmed [ ] is listed
> Traveler No. TUSER2113013
> Product description, safety related function, functional classification.
> Critical characteristics for acceptance (same that those identified table 5-1 of CDI). This identifies the acceptance records for each verification method.
> For example:
> 1) Performance characteristic
> Acceptance records
> C of C – from PPDD COC12004, rev. 0; from TDMS HNS1208-002, rev. 2
> Check list/report: SQIR-JHQ-000007
> Supplier's test: Module Design Verification Report for the AGRD design module specification (Document No. 5G8HC105, Rev 1); Design Verification Report No. DVRJHS-000272, which describes items reviewed during the design verification of the AGRD module design specification.
> FPGA design specification (Doc. No. 5G8HB794, rev. 4; DVR No. DVR-JHS-000345)
> FPGA test procedure (Doc. No. 8T8H3614, Rev 4; DVR No. DVR-JHS-000622)
> FPGA test report (Doc No 9H8H1085, rev 1; DVR-JHS-000630, rev. 0)
> Module test procedure (5T8H7621, rev 2; DVR-JHS-000455, rev. 0)
> Module test report (ATC-103666; DVR-JHS-000520, rev. 0)
> NICSD IV&V report: 5B8K0031, rev. 11
> 2) Build in quality
> Commercial grade survey SE12SR-001a, Rev. 0
> Source verification report – for example, for FPGA implementation: SVR-12003, Rev. 0
> Source verification check sheet (for example FPGA implementation SVCGD-12002, Rev. 0)
> FPGA logic implementation request/record sheet ([ ]): FDIM-12-0011-KM
> Vendor non-conformances: SVNNR-11-004, status closed, issued by PPDD
> Includes non-conformance notice report SVNNR-I-13-02. SCAR-12-013, issued by NICSD IV&V team, responsible PPDD. SCAR-12-013 reports that the VHDL source code was not designed in accordance with procedure E-68017, and this required a modification to the PPDD procedure.

The NRC staff reviewed the procedures and reports referenced in the CGD report for the AGRD module. The following are summaries of the information observed:

- Module test procedure (5T8H7621)
  Describes the module validation testing for AGRD module (HNS0420 series), specifically it identifies items to be confirmed prior to testing, including applicable documents

(schematic diagram and assembly drawing), test setup, test file, instructions, settings, and testing procedure.

- Receiving Inspection checklist/report (SQIR-JHQ-000007)
  Identifies the record No. for the test/inspection required by NICSD. In this case it references: ATC-103666, Rev. 1.

- Module test record ATC-103666
  Test record for the AGRD Module. This record identifies the manufacturing No. 9P04482PB2113, module type HNS0420B0000, who witnessed the test, test confirmation and results. The test was performed confirmation and setup as described in the procedure. The report also identifies measuring instruments used, with its calibration due date, calibration cycle, manufacturer, model, Toshiba control No., test item No.

The job order also specified the software development tools, which are identified in Table 9-2 of the FTER. As part of the CGD survey of PPDD, NICSD evaluated the process to control software development tools. Results from this evaluation were recorded in SE10SC-001a. In the FTER, Table 10-4-3, as well as in purchase document (e.g., job order to PPDD ECS-JHS015392) Toshiba identified the software tools and their version to be used by PPDD. The NRC staff verified the information identified in Table 9-2 of the FTER and purchase document for ModelSim matched the Software tool information sheet FDTC-05-0015-M Rev. 2, such as Modelsim version used (6.0b).

In the FTER, Toshiba explained that after the modules for the OPRM were qualified, they decided to modify the TRN and RCV modules to better meet the guidance in ISG-04. Specifically, Toshiba included Cyclic Redundancy Check (CRC) functions in these modules. Toshiba followed its process to perform dedication activities in the same manner that were followed for the original TRN and RCV modules. The NRC staff reviewed job order ECS-JHS017582 for the procurement of the modified TRN and RCV modules with the CRC function. This job order refers to MEM-JHS-000062, Rev. 3, for the technical details for these modules. The NRC staff reviewed Job order MEM-JHS-000062 Rev. 3. This other job order identified the procurement items (RCV module and TRN module), procurement specification (5Q8K0015 Rev.4), Device order number (9P04482PB2119B351), if oversight of the design review is required (NICSD to carry out DR oversight to DR-C and DR-F2. Therefore, PPDD can't skip DRC and DR-F2. (DR-C is performed after FPGA design. DR-F2 is performed after module testing)), software tools, QA procedures, and the design technical report (with the modifications for CRC).

Thread Requirements Traceability

For this activity, the NRC staff selected two requirements for the OPRM unit to trace form the system design description down to validation testing. As part of the LTR review, Toshiba docketed its System validation Testing Phase Requirements Traceability Matrix (RTM) (FC513704-1112) and the Equipment Design Specification for Power Range Neutron Monitor (FC513002-1000). Using this information the NRC staff selected the following requirements to trace:

SDD Requirement: R06-150 (this ID is assigned by NED and it refers to the requirement in the Neutron Monitoring System Design Description (SDD) documented in FC51-1001-0001).
EDS ID: FC51-3002-1000-426 (during the audit Toshiba explained that -426 is a number assigned by DOORS to each paragraph in the documents used for requirements traceability).
EDS Description: 5.2.1.3.0-12. (1) Input. The OPRM unit shall receive signals listed in table 5-7-1, unit input list.
Unit DDS ID: FC51-3702-1000-1004, FC51-3702-1000-227, FC51-3702-1000-1003, FC513702-1000-996, FC51-3702-1000-990, FC51-3702-1000-989, FC51-3702-1000-233, and
FC51-3702-1000-982
Validation Testing and Remark: Validated in the Module validation

SDD Requirement: R37-YYY.
EDS ID: FC51-3002-1000-1117.
EDS Description: 5.5.7.1.0-4. The communication data links to be provided for external systems have a one-way communication…
Unit DDS ID: FC51-3702-1000-823 and FC51-3702-1000-798
Validation Testing and Remark: Not a functional requirement, but a design and fabrication requirements

The NRC staff asked why the RTM does not trace all requirements identified in the EDS. Toshiba explained that the EDS includes requirements for multiple units in the Power Range Neutron Monitor (PRNM), and therefore not all apply to the OPRM unit. Also, Toshiba noted that generic requirements, applicable to all units, were captured in the lower level requirements for the OPRM unit. For example, Section 4.3.1 of the EDS states: “The PRNM system shall adopt modular design and support module replacement as described in Section 2 of IEEE Std. 603.” This requirement was captured in Section 5 (for the OPRM unit) in the requirement “5.1.8. Failure Detection and Self-Test Requirements 2. Monitoring Low Voltage Supply to modules A) Adopting modular design, the PRNM system is decomposed into modules.”

Toshiba prepared a mapping (cross reference) of the design criteria in Section 4 and its implementation in Section 5 of the EDS. In this map Toshiba identified requirements applicable to the OPRM unit as “OPRM Requirements” or “Common Requirements.” The NRC staff reviewed this information and confirmed the NICSD SD team verified all requirements for OPRM unit in the EDS had been incorporated in the OPRM Unit DDS.

For the OPRM unit, Toshiba created a RTM which was updated during each of the life cycle phases. Because Toshiba traced the requirements not only to the design documents, but also to its test procedures and test reports, Toshiba created different RTMs to trace the requirements.

To trace the requirements from the SDD to the EDS, Toshiba used RTM-JHS-000039. The NRC staff confirmed EDS ID: FC51-3002-1000-426 and FC51-3002-1000-1117 were traced in this RTM. Also, the NRC staff confirmed the information for these requirements provided match the information in the documents docketed. Then Toshiba prepared RTM-JHS-000045 to trace requirements from the EDS to the OPRM Unit DDS (FC51-3702-1000). The NRC staff

confirmed FC51-3002-1000-426 and FC51-3002-1000-1117 were identified and the information listed matched the information in the previous RTM and in the design documents. For FC513002-1000-426, this RTM identifies FC51-3702-1000-233 and FC51-3702-1000-982 in the OPRM unit DDS. To continue the traceability to the module design specification, the NRC staff selected FC51-3702-1000-233 (ID used for tracing other RTMs). For FC51-3002-1000-1117, this RTM identifies FC51-3702-1000-798 and FC51-3702-1000-823 in the OPRM unit DDS. Because these requirements are implemented in hardware (e.g., optical inputs), these requirement could not be traced to the level of system test procedures.

The requirements from the EDS and Unit DDS are traced to the system validation test procedure in RTM-JHS-000049. In the example being traced, the NRC staff observed the information matched the data in previous RTMs. For example:

EDS: 5.2.1.3.0-12
SDD-ID: FC51-1001-0001-1751
SDD Requirements: R06-150
ID EDS ID FC51-3002-1000-426 5.2.1.3.0-12

EDS: 5.5.7.1.0-4
SDD-ID: R37-YYY
SDD Requirements: FC51-3002-1000-1117 5.5.7.1.0-4

After tracing the requirements in the Unit DDS, Toshiba created a RTM for each module. For the example selected, the NRC staff used ID FC51-3702-1000-233, which corresponds to FC513002-1000-426 (signals that the OPRM should receive). This requirement was traced in the module design specification's RTM-JH8-000007. The NRC staff observed the information in the matrix matched the information in the Unit DDS. For example:

EDS: 5.2.1.3.0-12
UDDS ID FC51-3702-1000-233
OPRM Unit DDS Section 5.1.3.0-8
OPRM Unit Detailed Design Specification: The OPRM unit shall receive APRM Level, Core Flow Level, and APRM Unit Data from an APRM unit via the RCV module.
Object Identification: OPRM Unit
MDS (Module Design Specification): -

Requirements in the module were then traced to the RTM associated with the FPGA design specification (RTM-JH8-000059). The NRC staff observed that the information in RTM-JH8000059 matched the previous description and identified the next step. For example:

MDS (Module Design Specification): 5G8HC109-66
5G8HC109 Rev.3 RCV Module Design Specification: 5.1.1 Optical Data Interface
Object identification: RCV
5G8H6382 Rev.1 [ ] FPGA Design Specification: -
5G8H6383 Rev.1 [ ] FPGA Design Specification: -

In addition, Toshiba created a RTM to trace requirements from the module design specification to the module test procedure, RTM-JH8-000054. The NRC staff reviewed the information listed in the RTM Specifically,

MDS (Module Design Specification): 5G8HC109-66
RCV Module Design Specification: 5.1.1 Optical Data Interface Object identification: RCV RCV Module Test Procedure:
5T8H7022-17
5.1 Signal Continuity Test (APRM Data Continuity)
5T8H7022-18
5.2 Anomaly Action Check
5T8H7022-19
5.3 Unit Type/ Unit Number Detection Check
5T8H7022-37
5.8 CRC Error Check

Lastly, Toshiba created RTM-JHS-000049 to trace the requirements from the EDS and Unit DDS to System validation test procedure. This RTM included the following information:

EDS: 5.2.1.3.0-12
SDD-ID: FC51-1001-0001-1751
SDD Requirements R06-150
ID EDS ID FC51-3002-1000-426 5.2.1.3.0-12
EDS Description
1. Input
The OPRM unit shall receive signals listed in Table 5-7-1.
Table 5-7-1 OPRM unit Input List (1/2)
Unit DDS ID: For example, FC51-3702-1000-1004
Validation Testing and Remark
Validated in the Module validation

Toshiba provided copies of the test procedure (FC51-7101-1000) and test records (FC51-75131002) for the EDS ID: FC51-3002-1000-426 and the test records (FC51-3002-1000-1117) for the EDS ID: FC51-3002-1000-1117. The NRC staff confirmed these items were successfully tested.

Verification and Validation

The NRC staff met with Toshiba's IV&V group to discuss the IV&V process followed by NED and NICSD. Specifically, NICSD performed the majority of the activities, which were summarized in IV&V reports (VVR), which then NED incorporated in its VVR (FC51-3704-0001). In addition, NICSD prepared Software Safety Analysis Reports (SSARs) for each lifecycle, and summarized them in FC51-3704-1000. These reports were reviewed by NED, which summarized the results in FC51-3704-0004.

The NRC staff reviewed the software development process and IV&V activities to confirm that IV&V processes are implemented per its documentation and that the general requirements of current industry standards are being followed.

The IV&V team performed review of the documents created during the lifecycle in accordance with AS-200A002 “Design Verification Procedure.” AS-200A002, describes the method for design verification required by regulation, code and standards. In particular, this document states that design verification is performed to ensure adequacy of the design in accordance with the methods described in this procedure (e.g., design reviews) before the product is released. The results of document reviews are recorded in the design verification reports (DVR) or IM reports for NICSD IV&V reports. Problems discovered during the design verification are recorded in the DVR, where the resolution and approval are also recorded. The NRC staff reviewed the following:

DVR No. FC51-0904-0001 for the System Design Description Neutron Monitoring Systems (FC51-1001-0001). The document references the design input sheet FC51-0901-0001, Rev. 0, “Design Input Sheet for NMS.” The DVR identified that plant specific documents should be removed. This was then verified. Since FC51-0901-0001 Rev. 0, Design Input Sheet, was referenced in the DVR, the NRC staff also reviewed this document. The design input sheet includes a checklist of the design input to be included and whether necessary or not. This document is prepared in accordance with AS2000A014. For example, for environmental conditions, it identifies EPRI TR-107330 for specific requirements. If this changes, the preparer would need to identify the reason for changing it.

IM-2012-000152, Project Planning and Concept Definition Phase NICSD VVR Review Report. This NED report documents the result of the review and evaluation performed of NICSD IV&V Report (VVR) for the OPRM. For the Project Planning and Concept Definition Phase NICSD prepared FC51-3704-1001 “Nuclear Instrumentation & Control Systems Department Verification and Validation Report for OPRM of FPGA-based Safety-Related Systems,” Rev.0. This NICSD VVR was updated in consequent phases. It describes the activities performed during that phase, as well as their review and evaluation, and findings. NED found the activities were satisfactorily performed.

If open items are identified in the DVR, NICSD IV&V team uses verification follow sheet (VFS) for the design team to resolve them, in accordance with AS-200A002. For example, the review of the EDS (FC51-3002-1000) was accompanied by VFS-JHS-000064. The IV&V report summarizes the issues identified and how they were resolved.

In addition to DVRs, NED used a vendor generated checklist (VDCL) for review of certain documents, such as the NICSD IV&V plan. NICSD uses a Project Control Document List (PCDL) to control the documents created in accordance with AS-200A010. The NRC staff noted that the NED IV&V Plan (FA10-3709-0001) does not describe the VDCL, but this is mentioned in the IV&V report (FC51-3704-0001). In addition, the NICSD IV&V plan does not describe the PCDL either. The NRC staff also noted that Toshiba documents do not provide clear description of the different reports and means used to record reviews. To address this gap, Toshiba issued CAR-16-073 and SCAR-16-016 to address these issues. The NRC staff reviewed the following VDCLs:

VDCL-IM-0103, Vendor Generated Document Checklist
Vendor: NICSD
Product: OPRM
Documents checked: NICSD IV&V Report for the OPRM (after module validation testing phase)
The reviewer concluded the document was acceptable with exception to the issues identified in the attachment. Evaluation of this report was summarized in the NED IV&V report (FC51-3704-0001).
The attachment describes the findings and how they were resolved and their status (open/close).

VDCL-IM-0114, Vendor Generated Document Checklist
Vendor: NICSD
Product: OPRM equipment
Documents checked: NED approved EDS for the PRNMS (FC51-3002-1000, Rev. 4). The reviewer verified the requirements for the PRNMS.

The NRC staff reviewed an example of a design input sheet, which identified the requirements for the NMS.

Design Input Sheet FC51-0901-0001
This input sheet was used in the design verification of FC51-1001-0001, System Design Description Neutron Monitoring System. Specifically, the input sheet identified the source for the inputs used in the creation of the SDD for the NMS.

As part of the IV&V activities, the IV&V team participated in design review meetings. NQ-2001, “Process Review Meeting,” describes the process for this meeting. A meeting is requested by the Manager of the Design Group. The Process Review Meeting (PRM) is a non-mandatory review measure to assess the status of the project at the end of each lifecycle phase. This document describes the different categories for the PRM. For example, PRM category C: Software, Hardware and Interface Review Meeting - This PRM is a review meeting to confirm the interface between software and hardware, detailed design specification, performance, operability, maintainability, etc. in the stage of specific design. The NRC staff reviewed the following example:

PRM-JHS-000019
Design phase process review meeting (CRC function development)
Category PRM-C2
Date and location, attendance list
Summary of items discussed: design phase activities, items not yet completed, document configuration control status
Comments from NED to NICSD were recorded in ECS-IM-062457. Specifically, ECS-IM062457 communicated comments as a result of IV&V activity. In this case, IV&V spot checked of FPGA design specification and test procedure and identified comments to add additional items (e.g., test patterns) to cover requirements that were not sufficiently covered.
NICSD prepared ECS-JHS-017840 for disposition. Specifically, ECS-JHS-017840

Engineering letter from NICSD to PPDD, with copy to NED, asking PPDD to add additional testing pattern to address comments identified in the appendix of this document.

NICSD and PPDD performed “Design Review” meetings in accordance with “Design Verification Procedure” (AS-200A002) during the design phase. These meetings were used to discuss design issues and confirm PPDD activities. The NRC staff reviewed the following:

DR-16292, Design Review (C-5) Record
Meeting to discuss how to obtain acceptance from the NRC, regarding communication requirements. Specifically, the document describes modifying the RCV and TRN to include this function. It also requires creation of a new job order to NICSD to perform this. It identifies the document that should be modified to add this modification, such as RTM, module procurement specification, SDD, etc. (Later, NED issued job order C51-3612-0001 to request this modification to the RCV and TRN modules).

The software plans docketed do not provide clear descriptions of the processes to identify, report, and track non-conformances or problems during the design review, testing and source code review. Toshiba issued SCAR 16-018 to resolve this gap (Open Item). TheToshiba explained how anomalies and non-conformances were identified depending on the IV&V activity performed. For example, for problems identified during source code review, PPDD used an anomaly list, which was then included in the source code review sheet. During the audit the NRC staff reviewed the anomaly list for the software validation report, FC3704-1103. The NRC staff also confirmed that this list was referenced in the source code review. In addition, Toshiba prepared a table identifying IV&V activities and means to identify anomalies and nonconformances. In addition, Toshiba walked the NRC staff through this process using information for the AGRD module, which was used for the review of the CGD process described before. In particular, the design team created the module design specification (5G8HC105). This document was internally reviewed, and anomalies were reported in a comment list, which also described resolution and approval. Once the anomalies are resolved, the document was sent to the IV&V team for their review. The module design specification was accompanied by DVRJHS-000112, including comment list 5G8HC105. After IV&V performed its review, IV&V issued DVR-JHS-000272 summarizing its evaluation. If the DVR identifies open items, they would be discussed in the baseline review meeting.

Since PPDD was responsible for the design of the FPGAs and the modules, NICSD reviewed PPDD’s documents (e.g., module design specification) and VHDL source code. For document review, NICSD performed DVR process described above. For review of VHDL source code, the IV&V team held a review meeting and then created a source code review sheet. The NRC staff reviewed:

Source code review 5B8K0058 (for software validation report, FC51-3704-1103). This document records the source code review performed to detect and identify anomalies in software product that will be incorporated into FPGA logic for the Oscillation Power Range Monitor (OPRM)
Identified code reviewers and their roles.
Identified FPGA reviewed. (For example, [ ] was listed)
Listed documents and tools required

> The following is information from the media, which includes the VHDL source code and related electronic files.
> - FE Files (Media No. FE-12-0001-M, FE-12-0002-M)
> - Source Code Files (Media No. FPGA-12-0034-M, FPGA-13-0005-M, FPGA-13-0006-M, FPGA-13-0007-M)
> VHDL source code using the tool (spyglass – synopsys software tool)
> Describes review meetings, including problems, and completed tests.
> Includes review sheet for each FPGA (for example, Review Sheet for [ ])
> Code Number FPC-09-0001-M
> FPGA Design Specification (Document number and revision): [ ] FPGA Design Specification (5G8HB793 Rev.4)
> Other information such as media number that contains software products to be reviewed as necessary: FPGA-12-0034-M Documents the review results
> Anomaly List Item No.: 7, 8, 9, 10, 11, 12, 13, 14, 15, 16. The list includes disposition and justification for each item.

After the code was verified, and as part of the CGD activities, NICSD witnessed implementation of the FPGA. This activity is recorded in a source verification report. During the audit the NRC staff reviewed: SVCGD-12002, which recorded witnessing FPGA implementation, associated with Job order sheet ECS-JHS-015392, and with CDI: 9B8K0057 Rev. 1. In addition, NICSD prepared its IV&V report (FC51-3704-1001) for this phase. NED reviewed this report and summarizes the results in VDCL-IM-0103, which was described previously.

The IV&V team is also responsible for reviewing and confirming how PPDD used the software tools used for the design and testing of the OPRM unit. The NRC staff confirmed that NICSD and PPDD identified the tools used, and these tools were controlled in accordance with E68020, “PPDD Procedural Standard for Control of Software Tools Used with FPGA Based Systems.”

Once the modules were tested, they were integrated into the OPRM unit. The next step performed was system validation testing. NICSD IV&V team prepared the System Validation Test Specification (FC51-7101-1001) for the System Validation Testing Phase. The NRC staff reviewed this plan and observed the following:

> This document describes the system test specification for OPRM, including test requirements, conditions, and methodologies for the hardware test conducted in the system validation testing of the OPRM. Test requirements, conditions, and methodologies for the software validation test conducted in the system validation testing are described in the Software Validation Test Plan (SVTP). This specification defines the hold points, witness points and review points to be performed by NED. It also describes applicable documents, test system description and configuration, test system features, test equipment, Standard Settings and Default Statuses (normal operation) of OPRM Unit, test requirements (test conditions, environment), special test (including acceptance criteria for each item), confirmation items before test, hardware test, software validation test, prudency test, operability test, shipment settings. This specification identifies how to address nonconformances, specifically it requires using NQ-3019 and NQ-2024.

NICSD IV&V team also prepared the System Validation Test Procedure (FC51-7101-1000). The NRC staff reviewed this document and observed that it describes the instructions for the system validation test for the OPRM to demonstrate that the unit performs the functions specified in the EDS and OPRM unit detailed design specification. This procedure identifies the steps for hardware testing, burn-in test, operability test, software test, and prudency test.

As part of the system validation, NICSD performed software validation testing. The Software Validation Test Plan (SVTP) (FC51-7012-1003) describes the test requirements conditions, and methodologies for the software validation test conducted in the system validation testing of the OPRM unit. After testing, NICSD prepared a software validation test report (FC51-7513-1002). During the audit the NRC staff reviewed this report and observed the following:

> This report describes test system description, M&TE, test equipment software, test results, test anomaly reporting, and conclusions. This also includes the validation of the software after the changes to include CRC in the RCV and TRN modules. The report describes evaluation of the test equipment software, generation and evaluation of test patterns created by NICSD IV&V team. The test was performed in accordance with System Test Specification (FC51-7101-1001), which includes the special test for commercial grade items, FAT, and software validation testing.
>
> This report includes brief description of each test and summaries of the test results. Anomalies found during the system validation test were recorded in the test log of the system validation test record. No SNNRs were issued (for software errors or equipment malfunction).
> Document changes requested are also described. Document changes were documented in Document Change Request (DCR) in accordance with NQ-2024. These modifications are explained in the NICSD IV&V report.
>
> The IV&V team concluded that the test was successfully performed and met the acceptance criteria.

After the system validation is performed the IV&V team prepared a system test validation report. A summary of this report is provided in the IV&V report. In addition, NED Quality Assurance Department (NQAD) witnessed the system validation, and summarized its observation in the "System Validation Test Record," ATC-103584. This document is an inspection record for the validation testing (factory test) of the OPRM unit.

This report identifies the items witnessed during the test, such as hardware test (measurements), operability test, burn-in test, software validation test, and prudency test. These tests were passed satisfactorily. This report identifies reference documents required, including receiving inspection checklist/report (e.g., SQIR-JHQ-000007 for the AGRD module). The report includes the checklists used to perform these tests, with their results. NQAD concluded that validation testing passed satisfactorily. The results of the system validation were used in the CGD of the OPRM (i.e., special test method).

In addition to participating in the PRM, NICSD performed software QA reviews at the end of each lifecycle phase. These reviews were conducted to confirm the adequacy of IV&V activities

performed by NICSD, and to determine if these activities were performed in accordance with the IV&V plan. The results of this review were summarized in the Software Surveillance Report (FC51-7021-1001). The NRC staff observed that the Software QA team verified the following:

- Design verification reports
- Software safety analysis report
- Security review
- RTM
- Baseline review report

Functional Elements (FE)

Because Toshiba develops its system using FEs, the NRC staff reviewed the process used to design and develop them. Toshiba treats the FEs as commercial off the shelf (COTS), and therefore they were part of the CGD process. As part of the CGD, NICSD evaluated PPDD processes associated with FPGA logic and FEs. In addition, NICSD evaluated the procedures followed, which are identified in the FTER, Section 9.1.1. During the audit the NRC staff reviewed the following QA procedures, which are associated with the development of FEs.

NQ-2030, “Procedural Standard for FPGA Products Development.” It describes the development process of FPGAs, including design, IV&V integration and testing.

NQ-2031, “Procedural Standard for FPGA Device Development.” It describes the development and configuration processes of FPGA devices, including logic programmed by VHDL to perform the required function. It also includes the process for integration of these FPGAs into modules and units for the system-based units. This procedure must conform to the higher level procedure NQ-2030, “Procedural Standard for FPGA Products Development”.

NQ-2032, “Procedure Standard for FE Development.” It describes the process to develop FEs to be used in safety related FPGA products. This procedure also describes the lifecycle for the development of the FEs, including, design, testing IV&V, integration in FPGAs, and modifications. This procedure must conform to NQ-2030.

E-68016, “PPDD Procedural Standard for FPGA Products Development.” It describes the process to be followed by PPDD for development of units for use in safety related FPGA products, or to be used in qualification activities for such products when NICSD requests to use this procedure. This procedure applies to PPDD activities related to design, integration, testing or modification of FPGA products provided by PPDD to NICSD when NICSD requests use of this procedure. These activities include development of FPGA-based modules and integration of these modules into FPGA-based units.

E-68018, “PPDD Procedural Standard for Functional Element Development.” It describes the process to be followed by PPDD for development of FEs for use in safety related FPGA products, or to be used in qualification activities for such products when NICSD requests the

usage of this procedure. These activities include development and configuration of FEs and the integration of these FEs into FPGAs, and eventually into modules for the system-based units. This procedure must conform to the higher-level procedure E-68016. This procedure describes the activities required in each phase of a FE's life cycle.

E-68019, "PPDD Procedural Standard for FPGA Configuration Management." It describes the configuration management process to be followed by PPDD for development of safety related FPGA products, or for qualification activities for such products when NICSD requests to use this procedure.

For CGD of the FE, NICS-QA verified that PPDD's 'E' procedures were equivalent to and complied with NQ-2032. Results of this review were recorded in the NICSD IV&V report. In addition, NICSD IV&V team verified documentation and configuration control of the FEs. The NRC staff reviewed examples of the information evaluated by NICSD. In particular, the NRC staff observed the following information:

FE Requirement Specification
5G8HA703, Rev 2
This document provides the functional requirements for the FE, I/O signals, and Interface/Interaction with other FEs

Requirement specification for FEs
5G8HB647
Adder, substrate, multiplier, comparer, flip-flop, counter, selector.

FE Design Specification
Edge detector 5G8HA723
Describes the FE with logic diagram and time requirements

FE Test Specification
8T8H3371
Identifies the test device: hardware and software, and the test specification for each case, rising and falling bit.

FE Test Record
9H8H0259
Describes the test bench and FPGA used for testing, RTL simulation test results, and pinport test results for the rising edge.

FE Control Sheet
FDFE-05-0056M
Name of Code [ ]
FE Specification 5G8HA723
Test procedure 8T8H3371
Test report 9H8H0259
FE source code [ ]
Edf file [ ]

For the audit, Toshiba held a demonstration of a FE and an FPGA logic using approved FEs. During this demonstration, PPDD showed the stand-alone PCs and software tools used, as well as the stand-alone PCs and software tools used for testing.

During the FE demonstration, the NRC staff observed how PPDD created the source code for the FE, the netlist, I/O and test source code for testing, and the fuse map. Then PPDD moved the fuse map to the testing PC and performed simulation testing using the test source code created with the FE. After the simulation was completed, the NRC staff reviewed the test report and test results. PPDD also performed a demonstration of hardware testing using PinPort. Both the simulation and hardware testing met the test acceptance criteria. Once an FE is tested, it is registered in the FE library. The PTER and FTER identified the FEs used for the development of the OPRM unit.

To develop the FPGA logic, PPDD uses the FEs in the FE library. The PPDD made a demonstration of how this process is performed. In particular, PPDD showed the NRC staff how they obtain the DVD that contains the FEs to be used in the FPGA. Using the DVD, PPDD demonstrated how they use the logic synthesis tools, perform place and route, and generate the fuse map. Once the fuse map is created, PPDD tested it using simulation software. During the demonstration, the NRC staff observed that the FPGA was successfully tested (i.e., toggle coverage equal to 100%). After testing, the information is registered in a DVD and the FPGA is stored in a locked cabinet. At this point the FPGA can be burned in the chip. FPGA burning is performed in TDMS. The NRC staff observed the DVD containing the FPGA contains the following information:

PPDD information (when the DVD is created)
Media No. FPGA-13-0004-2-M
File Name NB111200.afm
Code file FPC-12-0003-M
Rev. 0, Date 13/01/16
Signature of configuration manager

NICSD information (after registration)
Media No NB111*200-001-C-KM
Fuse map file name NB111200.afm
FPGA code name [ ]
Date 16/01/13
Signature of configuration manager

Toshiba also provided a tour of the TDMS facility. During this tour, the NRC staff observed how circuit boards are assembled, as well as the process to burn the FPGA in the chip using Silicon Sculptor II. To burn the FPGA, PPDD received the DVD with the FPGA logic implementation request/record sheet. During the demonstration, the NRC staff reviewed the following record sheet:

No. FDIM-12-0035-KM
Signature of approver

NICSD order No. 9P04482 PB2119 B352
FPGA device – Actel FPGA type A54SX72A
Fuse-map [ ]
File name NB111200.afm
Check sum DA75
Security fuse – security fuse shall not be processed
Implementation tool Silicon Sculptor V.5.14.2
PC Control number

TDMS follows procedure WDR-L-R002 to burn the FPGA in the chip. This procedure requires the tool is tested before it is used, then it describes the steps to burn the chip. After the FPGA is burned, TDMS verifies the correct FPGA logic was burned by checking the checksum and device sum. After the FPGA is burned, TDMS fills out the bottom portion of the FPGA logic implementation request/record sheet. The NRC staff observed the following information:

Manufacturer: TDMS
Fuse-map [ ]
File name NB111200.afm
Check sum DA75
Security fuse not processed
Worker name
Implementation tool used: Silicon Sculptor V.5.14.2
PC Control number used

The FPGA chip is stored in a locked cabinet. After this the FPGA is sent to manufacturing facilities to be placed in the circuit board.

Attachment 3 – Configuration Management

The NRC staff reviewed the Configuration Management activities established for the PRM system and the OPRM unit. For this audit activity, the NRC staff reviewed NED, NICSD and PPDD documents that describe configuration management, document control, design change control, and nonconformance control procedures. The NRC staff also observed how these procedures have been implemented, and interviewed Toshiba personnel.

3.1 Configuration Management

The configuration management procedures and standards used by NED and NICSD vary between the original process and the current process. For both the original process used to develop the PRM system and the current process used to develop the OPRM unit, NED implemented configuration management procedure AS-200A131, "Digital System Configuration Management Procedure." For the development of the PRM system, NICSD used E-68019, "PPDD Procedural Standard for FPGA Configuration Management." After completion of the PRM system development project, NICSD prepared NQ standard NQ-2033, "Procedural Standard for FPGA Configuration Management." For the development of the OPRM unit, NICSD used the NQ-2033 standard, and PPDD used the E-68019 standard. These documents were reviewed by the NRC staff as described below.

NED Configuration Management

The NRC staff reviewed NED document AS-200A131, "Digital System Configuration Management Procedure," Rev. 1, which describes the configuration management process to be applied to all digital system and documentation for the design or modification of safety related products to be sold to commercial US nuclear power plants, or to be used in qualification activities for such products. This procedure details the responsibilities for the Configuration Management Plan, the Master Configuration List (MCL), and the Software Baseline. It identifies the configuration management activities for the software lifecycle phases, which include developing a project-specific Configuration Management Plan, developing and updating a MCL, developing and updating a Software Baseline, and maintaining Change Control documentation.

The procedure states that Configuration Control requires maintaining control of document revision levels in accordance with AS-100A004, "Document Control Procedure" and using the Change Control Process as described in AS-200A015, "Design Change Control Procedure." Additionally, all test deficiencies and/or deviations are to be documented in accordance with Procedure AS-300A008, "Nonconformance Control and Corrective Action Procedure."

Toshiba uses the configuration status accounting to identify and update the configuration items which comprise the software baselines and the MCL, and to establish a system to track the status of system change requests or change control documentation. This allows NED to

monitor problems or errors found during the design and manufacture of the product, as well as monitor user requests and problems. Additionally, use of the MCL ensures that project personnel are aware of, have access to, and are using the current version of each controlled document.

Toshiba uses Configuration Records to maintain electronic copies of all documents (or components) needed to regenerate a specific document (e.g., software baselines), and to update the MCL to record the latest version of a revision-controlled document. It also requires maintaining changes/deviations and test deficiencies/deviations along with the resolution and the completed documentation.

Change Control Documentation requires documenting and reviewing changes to controlled documents of configuration items using NED procedure AS-200A015. The Design Change Notice (DCN) must be reviewed and approved. The DCN specifies the unique change identified number, change description, new and previous code version, implementation date, affected documentation, required validation activities resulting from the change, signature of the preparer and reviewer, reference to a validation test procedure document and step which failed (if applicable), and reference to a Nonconformance Notice Report (NNR) form (if applicable). The DCN and any other change documentation is to be retained, and no change request should be discarded.

Appendix A of this procedure contains the activities and requirements for the Configuration Management Plan, while Appendix B describes the requirements for configuration status accounting of the software baselines.

NICSD Configuration Management

The NRC staff reviewed NICSD document NQ-2033, “Procedural Standard for FPGA Configuration Management,” Rev. 4, which provides the method to establish a baseline at completion of FPGA logic development, control configuration items by registration, control change of the registered FPGA logic, and release the registered FPGA logic for manufacturing of a module. The procedure specifies that CIs for each FPGA device are to be identified and controlled by the FPGA Control Sheet, in accordance with NQ-2031. The CIs for each FPGA includes the fuse-map, VHDL source code, FE files, and all the documentation applicable as a baseline. The FEs to be used for the FPGA logic are identified and controlled by the FE Control Sheet, in accordance with NQ-2032.

The procedure discusses the naming and numbering rules for the FPGA CIs. For the VHDL source code that goes into the deliverable product, a new FPGA code number is assigned. To identify the FPGA in the field, a 6-digit ID number, which is a part of the fuse-map registration number, is printed on a label affixed to the FPGA device. The checksum value to be confirmed at implementation into an FPGA device is described on the FPGA Control Sheet. The NRC staff’s review of an FPGA Control Sheet is contained in the Commercial Grade Dedication section of Attachment 2 to this audit report.

The FPGA configuration management activities include approving for use the FEs used for FPGA logic design, and performing the necessary V&V activities for the FEs, before they are incorporated into the FPGA logic. The baseline is established when the FPGA testing is finished and the review of configuration records is completed at the implementation phase. After the baseline has been established, the change control for the FPGA is performed in accordance with the formal change control process. For FPGA logic modifications, the configuration management activities include verifying the existing baseline prior to modification, and identifying the portion of the documents to be modified.

NQ-2033 discusses control of configuration records in electronic media. For example, the responsible design group stores a duplicate electronic copy of all the necessary configuration items to reproduce the baseline, and stores the FPGA files, including VHDL source code and fuse-map, in one-time writable electronic media (e.g., CD-R, DVD-R). The procedure also discusses the control of media which stores the FEs and software tools. This includes using one-time writable electronic media to store the FE files that include VHDL source code, and using Form 8, "FE Documents/Media Check Sheet," to confirm the contents of related documents and electronic media that store the FE files.

PPDD Configuration Management

The NRC staff reviewed PPDD procedure E-68019, "PPDD Procedural Standard for FPGA Configuration Management," Rev. 7, which describes the configuration management process to be followed by PPDD for development of safety related FPGA products. This procedure applies to activities related to design, integration, testing or modification of FPGAs to be used in FPGA products provided by PPDD to NICSD, or for qualification of such products when NICSD requests to use this procedure.

The procedure states that for each FPGA product produced by PPDD (e.g., FPGA device, FE files, or other FPGA product), configuration items (i.e., all of the data required to reproduce the system and development environment) is to be maintained. The configuration items to be controlled are grouped by the following categories: Requirement Documents (e.g., Procurement Specification), Design, (e.g., FPGA Design Specification), Program (e.g., FE Source Code), Procurement (e.g., Procurement Planning Sheet), Manufacturing (e.g., Parts List), Test (e.g., Module Test Procedure), Record (e.g., Environment Assessment Report), Nonconformance Control (e.g., NNR), and Development Environment (e.g., Software Tool Validation Report).

The procedure discusses Configuration Status Accounting using Software Baselines at the end of testing in the FPGA implementation phase. The Software Baseline includes electronic copies of the fuse-map, VHDL Source Code, FE files, development environment, tools, and all documentation applicable to that baseline. Software baselines are identified with each document number and unique sequential revision number assignments. The CIs that are part of each Software Baseline are maintained and the following information for each CI is documented as a MCL: Configuration identification (e.g., revisions, file names, file sizes, etc.),

issue date, a brief description, checksums for fuse-map indicated in the implementation tool, software tool configuration information (e.g., tool name, version, tool settings, etc.), and development platform information (such as operating system version) if relevant. Additionally, electronic copies of all components needed to regenerate a Software Baseline are maintained.

A design change of the CIs is documented and reviewed in accordance with E-68001, "Design Change Control Procedure," and by using the Change Control Sheet. The information contained in the Change Control Sheet includes: a unique change identification number, the background and purpose for the change, the specific code changes implemented, new and previous code version and/or revision numbers, affected documentation, and required validation activities resulting from the change. If applicable, a reference to a validation test procedure document and step which failed, and reference to a Nonconformance Notice Report (NNR) should also be included.

When a modification is made to the product configuration items, the FPGA designer updates the MCL and the Software Baseline. The MCL is then reviewed and approved by the configuration manager. The Software Baseline change is to be identified in the history column of the updated MCL and then it is stored as a quality record. After approval by the configuration manager, the FPGA designer sends a control copy of the updated MCL to the responsible NICSD division.

Appendix A of E-68019 discusses the media, tool and Control Sheet storage. Electronic files of the configuration items in the project are stored in the [ ] media management system. Optical media (i.e., CD-R, DVD-R) may also be used for storage and for transfer to other departments.

3.2 Document Control

NED Document Control

The NRC staff reviewed NED document AS-100A004, "Document Control Procedure," Rev. 17, which describes the responsibilities and defines the measures for control, preparation, review, revision, release, issuance, disposition, and storage of a Project Control Document (PCD). PCDs include purchase orders, specifications, design calculations, procedures and drawing which describe activities affecting quality for a project.

The NRC staff reviewed NED document FA10-0301-0001, "Project Specific Document Control Procedure," Rev. 0, which describes the process for preparation and control of PCDs for the NRW-FPGA-Based I&C System Qualification Project. This process includes preparation (e.g., document format, numbering and other requirements), transmittal, and revision of PCDs. It references NED documents AS-100A004 and AS-200A015.

PCDs include documents which are issued or used for the NRW-FPGA-Based I&C System Qualification Project and specify quality requirements or prescribe activities affecting quality, such as instructions, procedures and drawings; and documents such as System Design Descriptions, Piping and Instrumentation Diagrams, piping and valve design documents, documents for testing, inspection, plant operations, and maintenance, and instruction manuals.

FA10-0301-0001 describes the PCD numbering rules. Toshiba assigns a unique Project Document Number to each PCD and a list of Toshiba document codes applicable to the FPGA project is provided. Examples of some document codes are: '0301' for Project Requirements Document, '1505' for Design Study Report (Evaluation Report), '3702' for Software Requirement Document, and '3704' for Software Validation Report. FA10-0301-0001 also describes the document revision guidelines for PCDs, which include attaching an associated DCN when a document is revised.

NED uses the NUPDM2 electronic document control system for storing electronic versions of controlled documents. NUPDM2 is located within the NED [ ] software. An ID and password are required to log into the [ ] software, from which the NUPDM2 system is accessed. Documents are prepared in Microsoft Word, printed, signed, scanned, and then reviewed and approved in NUPDM2. When a new document is created, the user selects the document type, and the system assigns the document filing number. The document control procedure describes the project document numbering scheme. The paper hardcopy becomes a quality record and it is stored in a controlled area. Once the project is completed, NICSD will send the baseline documents electronically to NED. There, the documents will get signed and reviewed, an NED cover will be added to the front, and then the document will be added to NUPDM2.

There is a separate electronic document storage for AS-procedures, but the document control is only done with the hardcopy documents.

NICSD Document Control

The NRC staff reviewed NICSD document NQ-2024, "Document Control Procedure," Rev. 11, which specifies the control responsibilities and methods for preparation, review, approval issuance, distribution and revision of documents that specify quality requirements for the safety-related items and services produced by NICSD.

Toshiba explained the use of the electronic document control systems. NICSD and PPDD use the [ ] document control system. This system requires a user ID and password for access. When a new document is created, an attributes menu allows the user to select the document number type. [ ] is used for electronic document storage, and to assign document and filing numbers when creating new documents. Although [ ] maintains a record of the document version changes, NICSD and PPDD only use the hardcopy versions of the documents for document control. When a document is created or revised, a hardcopy is printed out and hand carried for signatures. Then it gets scanned and approved electronically

by the manager so that it can be added to the [ ] system. The reviewer and approver need to make an electronic approval of the document on the system.

Document access rights are controlled in [ ], as approved by the project manager, to select which groups issued the document, and which groups have write or read-only access. If a document is selected for which access is not granted, an error message appears and the contact information for the organization who owns the document is displayed. The NRC staff was given a demonstration of how the NICSD PM performs the registration of users to the electronic document control system, and performs supervision of access control to the documents.

The NRC staff was given a tour of the QA Records Storage Room which contains the hardcopy versions of the project QA documents. The room is locked and a form needs to be signed in order to enter. The room contains locked, fireproof cabinets which contain the hardcopy QA documents. A Transmittal Control Slip is attached to every product that NICSD delivers to NED. Once NED receives a product from NICSD, it signs the Transmittal Control Slip and sends it back to NICSD. The NRC staff was shown the Transmittal Control Slip for the OPRM project that was sent back NED after the product was delivered. The slip is dated January 15, 2015.

3.3 Design Change Control

NED Design Change Control

The NRC staff reviewed NED document AS-200A015, “Design Change Control Procedure,” Rev. 6, which describes the process for controlling and authorizing changes to the design. The design change process consists of the change proposal, the design change evaluation, the change authorization, and the retention of QA records.

The design change proposal activities include: defining the change and identifying the scope and impact; defining the reason(s) for the change; identifying the design document(s) to be changed, and those affected by the change; and classifying the Design Change Class for the change.

The design change evaluation process includes: evaluating the technical, quality, safety, schedule and cost impacts of the design change; evaluating if acceptance by organizations other than NED is necessary; and concurring with the Design Change Class. An evaluation is also made to determine whether the proposed change is the result of an inadequacy in the original design which could create a substantial safety hazard for safety-related activities, using procedure 4810, “Reporting Procedure for Defects and Noncompliance under USNRC 10CFR21.”

The design change authorization process includes documenting the result of the Design Review Meeting and distributing the results to the concerned organizations, in accordance with document AS-200A005, "Design Review Meeting Convening Standard." The revised design documents are then prepared and issued.

The retention of QA records process includes collecting, storing and maintaining the design output documents and the documents providing evidence that the design change processes were performed in accordance with the NED QA record control program. This control program is described in AS-300A010, "Preparation Procedure for QA Record Control Procedure," AS300A011, "QA Record Validation Procedure," and AS-100A007, "Filing Procedure for Quality Assurance Records."

NICSD Design Change Control

The NRC staff reviewed NICSD document NQ-2035, "Procedure for Design Change Control," Rev. 4, which describes the design change control activities to be performed by the NICSD Design Group for the identification, evaluation and implementation of a safety-related item design change. There are three classes of design changes performed by NICSD: -A, -B and None.

For a "Design Change Class-A," NED must review and approve the change request. After receiving approval from NED, the preparer assigned by the Design Group manager prepares a Design Change Technical Report (DCTR). After the evaluation of the design change is reviewed and approved, the design change is implemented, reviewed, approved and verified.

For a "Design Change Class-B," the design change is evaluated and performed by the Design Group. The preparer assigned by the Design Group manager prepares a DCTR based on the evaluation of the design change, and following the evaluation results. After the Design Group manager approves the DCTR, the design change is implemented, reviewed, approved and verified.

For a "Design Change Class-None," the design change is identified with the DCN and change history, and authorized through the DCN review/approval process.

The DCN should specify the item to be changed, current design, previous design, Design Change Class, reason of the change, and verification of the change. The DCN is reviewed by the Design Engineer and approved by the Design Group manager.

The DCTR is used for evaluation of the design change and includes the Job Number, Customer Name, Item/System Name, Reference System Name, Document Number, and the Design Change Class. The DCTR should include the circumstances that lead to the design change, and the impacts of the change, including technology, quality, safety and project risks.

The NRC staff reviewed the DCTR for a proposed change that resulted in a design change for the OPRM unit. The NRC staff reviewed DCTR-FC51-3002-1000-02, Rev. 0, which was originated by NED and proposed to modify the TRN and RCV modules to add a [ ]-bit Cyclic Redundancy Check to the integrity check function for data transmission. This design change makes the units that consists of TOSDIA series modules capable of detecting multi-bit errors on transmission data, thus making the transmission more dependable. The DCTR change evaluation states that the design change does not affect the OPRM unit's functional specifications. The NICSD SD Team evaluated the impact of this design change and determined the design control activities and life cycle activities as required.

3.4 Nonconformance Control

NED Nonconformance Control

The NRC staff reviewed NED document AS-300A006, "Nonconformance Control Procedure for Procured Items and Services," Rev. 8, which describes the responsibilities and the measures for control and disposition of nonconformances for items and services that do not meet the requirements of procurement documents issued by NED or documents approved by NED. This procedure defines nonconformaces as deficiencies in characteristics, documentations, or procedures that render the quality of items or activities unacceptable or indeterminate. A nonconformance is to be reported to NED when: a technical or material requirement is violated; a requirement in vendor documents, which has been approved by the NED, is violated; a nonconformance cannot be corrected by continuation of the original manufacturing process; the item does not conform to the original requirement even though the item can be restored to a condition such that the capability of the item to function is unimpaired; there are counterfeit, fraudulent or suspicious items; or a nonconformance is related to customer property.

The procedure describes the process for evaluation and disposition of a Vendor-NNR (VNNR). After the VNNR is received, the Project QA Manager assigns the organization that prepared the Procurement Specification for the nonconforming item or service as the responsible organization for review. The assigned personnel will review the VNNR, and evaluate the recommended disposition and the technical justification. When a disposition is determined to not meet the original requirements, the impact to the related documents is to be evaluated. After the responsible organization manager approves the VNNR, it is transferred to the Project QA Manager for approval. If it is required in the contract with the customer, the Project QA group is to submit the VNNR to the customer for approval.

The VNNR is to be retained by NED for the retention period applicable to the item the nonconformance report affects. The VNNR is to be registered on a computer nonconformance information sharing database named "Integrated information Management system with Prevention/Accumulation/Correction process of Trouble (IMPACT)". This database is populated by NNR and VNNR data, as well as other sources of information, and the data is used for the Lessons Learned program. The IMPACT database was developed by NED and is controlled by NED QA. The database is found under the NED [ ] system. The IMPACT main page contains the latest updated nonconformances. Input information required

for the IMPACT database is described in AS-300A008, “Nonconformance Control and Corrective Action Procedure.” The database allows searching for nonconformances by plant code, project name, system name, equipment name, responsible group for the nonconformance, or date of the nonconformance. The information contained in the database includes the plant, nonconformance title, date, cause, corrective action, preventive action, and QA information.

The NRC staff reviewed NED document AS-300A008, “Nonconformance Control and Corrective Action Procedure,” Rev. 17, which describes the responsibilities and measures to control nonconformance items and documents at NED, and describes corrective actions to prevent recurrence. The nonconformance items addressed in this procedure include:

a. Nonconforming items manufactured by Toshiba Shop Organizations using inadequate NED specifications, or those manufactured by vendors by use of the inadequate procurement documents issued by NED.
b. Nonconforming documents (such as specifications, instructions and drawings) and data generated by NED.

The process for disposition of a nonconformance starts with detection and notification. The responsible QA staff is to describe the following Nonconformance Notice Report Phase-I (NNRI) information: identification number of the NNR-I, issue date, customer name, date of occurrence (or detection), plant (and/or project) name, item name, item number, outline of the nonconforming conditions, details of the nonconforming conditions, responsible organization within NED, and required date for replying. The NNR-I is then forwarded to the responsible organization to establish the disposition. The manager of the responsible QA group instructs the Toshiba Shop Organization or the vendor, as applicable, that is manufacturing the item to stop work related to the nonconformance. The item related to the nonconformance is then identified and segregated. The manager of the responsible organization assigns the personnel performing evaluation to determine disposition and technical justification. The nonconformance is to be categorized as either a Category A nonconformance that needs customer’s approval before disposition or a Category B nonconformance that may be disposed of at the discretion of NED. The disposition is then recorded in the NNR-I.

The conditions adverse to quality identified on the NNR-I are to be classified to determine if a corrective action is necessary. For significant conditions adverse to quality, the root cause(s) is determined and documented on the Nonconformance Notice Report Phase-II (NNR-II), and the impact of such conditions on completed and/or related items and activities are to be evaluated and documented on the NNR-II. An evaluation is also made to determine whether the significant conditions adverse to quality are reportable in accordance with 10 CFR Part 21 by using procedure 4810, “Reporting Procedure for Defects and Noncompliance under USNRC 10CFR21.” If a condition adverse to quality is detected during the investigation, disposition and corrective action process, it is to be documented and separately controlled by using a CAR in accordance with AS-300A009.

The NRC staff reviewed Toshiba document AS-300A009, "Corrective Action Request Application Procedure," Rev. 18, which describes the responsibilities and measures established to assure that conditions adverse to quality are promptly identified, documented, and corrected. For significant conditions adverse to quality, this procedure also describes the responsibilities and the measures for identification, documentation of the cause and corrective action taken to preclude recurrence, reporting to the appropriate level managers, and follow-up action taken to verify implementation of corrective action.

Conditions adverse to quality include failures, malfunctions, quality system deficiencies, defective items, out of control processes, documentation, procedures, and nonconformances including unacceptable and indeterminate activities. Documents that identify conditions adverse to quality include the VNNR, External Audit Report, Internal Audit Report, Source Verification Report, Test Record and the Design Verification Report.

The responsible organization for the required corrective action (RORC) performs a root cause analysis and the determined cause(s) are to be documented by the CAR. The analysis to determine the action(s) to be taken may include studies, simulations, investigations, experimentation, trending, and interviewing personnel.

The RORC is responsible to document the proposed disposition, corrective action, and due date of the corrective action on the CAR. This includes performing an evaluation to determine whether the conditions adverse to quality are reportable in accordance with 10 CFR Part 21, by using procedure 4810, "Reporting Procedure for Defects and Noncompliance under USNRC 10CFR21." The responsible management person at the RORC reviews and approves the CAR. Upon the receipt of the approved CAR, the CAR owner instructs the RORC to implement the approved disposition and corrective action.

NICSD Nonconformance Control

The NRC staff reviewed NICSD document NQ-3006, "Procedure for Control of Nonconforming Procurement Items and Services," Rev. 3, which describes how to control and dispose nonconformance of items and services procured by NICSD to produce a safety related product. The manager of NICS-QC is responsible for these activities. This non-conformance is identified as a VNNR. The VNNR includes recommended disposition and technical justification. The VNNRs are evaluated to see if they should be made into a corrective action. If so, they should follow the process described in NQ-3009. NICSD logs VNNRs in the VNNR log. NICS-QA showed this log to the NRC staff.

The NRC staff reviewed NICSD document NQ-3019, "Procedure for Control of Nonconformance and Corrective Action," Rev. 7, which describes the process to control non-conforming items and documents for safety related items and services at NICSD. The NICS-QA manager has overall responsibility for these activities. The NICS-QC manager is responsible for control and verification of disposition results.

When a non-conformance is identified, NICS-QC must be notified. If the nonconformance occurred in NICSD, then Toshiba uses procedure NQ-3019 (SNNR). If the nonconformance occurred in the supplier, then Toshiba uses procedure NQ-3006 (VNNR). For a nonconformance originating in PPDD, NICSD uses the VNNR.

In addition, this procedure states that NICS-QA should prepare a SNNR-I for items related to QA program, and NICS-QC should prepare a SNNR-I for items related to project activities. This procedure also defines the criteria for determining if a non-conformance affects quality, and then a root cause analysis is performed. In this case, Toshiba prepares a SNNR-II corrective action. This includes an evaluation of the corrective action to determine if reporting in accordance with 10 CFR Part 21 is necessary.

Attachment 4 - Secure Development Environment

The NRC staff verified that the secure development environment established at the Toshiba Fuchu Complex for the PRM system and OPRM unit conforms to the requirements of RG 1.152, Revision 3. For this audit activity, the NRC staff reviewed Toshiba, NED, NICSD and PPDD procedures and guidelines that describe the secure development environment controls, observed how these security controls have been established, and interviewed Toshiba personnel.

4.1 Toshiba Information Security Rules and Guidelines

Section 8.3, "Secure Development and Operational Environment," of NED document FA323702-0005, "Software Management Plan," Rev. 2 (ADAMS Accession No. ML14225A054), for the OPRM unit project, states that design documents are to be protected in accordance with the Toshiba Information Security Rules and Guidelines (ISRGs) in a manner that does not compromise the security of the digital systems, other systems, or the plant. The NRC staff reviewed the following Toshiba ISRGs, which provide high level policies for protecting Toshiba information and products:

SEC 1-01, Basic Regulation for Information Security Management
This document establishes the Toshiba policies for protecting proprietary information retained by Toshiba, ensuring the proper management of information from the perspective of information security, and to reduce information-related risks.

The document identifies the relevant regulations, describes the Toshiba information security management structure and provides requirements for education and training, conducting selfaudits, protecting the confidentiality of corporate information, prohibiting unauthorized access to or use of corporate information, and the actions to be taken in case of an incident.

SEC 1-02, Information Security Standard
This document establishes the standards for implementing information security in accordance with SEC 1-01. These include development of information handling standards, development of an organizational management system, internal audits, virus protection, security patches, measures to be taken when bringing devices out of the office, prevention of improper use, network measures, ID/password settings and management, and physical measures for information devices.

Information Security Guidelines
This document provides the measures required to comply with the regulations found in SEC 102. These include virus protection, security patches, measures to be taken when bringing devices out of the office, prevention of improper use, network security measures, ID/password settings and management, and physical measures for information devices. The document also discusses incorporation of security requirements, and physical measures for servers.

Information Security Handbook
This information security handbook is intended for Toshiba employees and provides explanations of the rules and key points to be observed in conducting day-to-day operations. There is also a separate, but similar Information Security Handbook intended for TANE employees.

Information Security and Handling Policy
This document is the TANE policy for information security for the company and its employees designed to prevent information-related risks and to safeguard information. It contains security measures for information devices such as PCs, smart phones, and USB flash drives.

4.2 NED Secure Development Environment

NED Secure Development Environment Procedure
The NRC staff reviewed document D-81018, "Information Security Criteria of Control for Toshiba Fuchu Complex Power Systems Segment," Rev. 2, dated June 30, 2008. Revisions 0 and 1 of this document were effective at the time the PRM system was being developed. Although this document was later voided and superseded by PG-C-2502, "Security Guide for Information Devices," – also later voided and superseded by PG-C-2303 – the Toshiba LTR still references D-81018 and the Toshiba NRW-FPGA-based I&C System project is still using it.

Toshiba performed a gap analysis between D-81018 and PC-C-2303 and found that D-81018 contains information that was not included in PC-C-2303. Toshiba expressed that it will work with the Information Technology (IT) group in charge of the newer documents to add the information found in D-81018 to PG-C-2303. For the FPGA-based safety-systems, Toshiba will continue to use D-81018, as identified in the LTR. At the request of the NRC staff, a Toshiba interpreter translated portions of D-81018.

The document provides criteria for controlling information devices like laptop and desktop PCs. For example, only software that is required for business operation and that has been previously approved is to be installed in information devices. Any other software is not to be installed without permission. Approval is also required for performing hardware changes on information devices. Information devices are to be used at predetermined locations, and they are not to be moved without permission.

D-81018 describes measures for protecting information from theft and/or loss. These include securing PCs [
] that require access control. Additionally, no documents are to be left on a desk when leaving the office. Locked cabinet/drawers are to be used as needed.

The keys used for security control are to be controlled by [

].

Information devices are to be registered and controlled with the Fuchu Software & Information Device Central Control System, regardless of connection to the Toshiba Network. D-81018 describes the security controls to be placed on laptop and desktop PCs. Such controls include [

]. D-81018 also describes training and education requirements, actions to take in the case of theft or loss, and disposal of information devices.

Attachment 1 of D-81018 contains a list of security measures for information devices. These include [

]. Attachment 2 contains a table identifying [
] physically securing laptop and desktop PCs.

4.3 NICSD Secure Development Environment

NICSD Secure Development Environment Procedure

The NRC staff reviewed NQ-2037, "Cyber Security Procedure of Safety Related System," Rev. 3. This procedure is based on RG 1.152, Rev. 3, to ensure that safety-related digital systems manufactured by NICSD (including FPGA-based products) do not include any potential susceptibility against inadvertent access and/or undesirable behaviors from connected systems. This procedure is also applicable to software tools – and computers used to run those software tools – that are used during production and development of the systems, storage media which are used to store electronic files of the safety-related digital systems or are used during development and production of the systems.

NQ-2037 identifies the general controls performed by NICSD to address identification and mitigation of potential vulnerabilities of the digital safety systems throughout the software life cycle phases. These include protection of the design documents, code, records and all other work products associated with digital safety systems; protection of all QA records by storing in an access controlled location; and storage of software products in one-time writable media which is off-line and physically protected. Additionally, the V&V team ensures that the requirements for software security are properly implemented and undocumented functions are avoided from the implementation, perform security assessment for each life cycle phase, and document the assessment results.

The procedure identifies the secure development activities that are to be performed for each of the software lifecycle phases, in accordance with RG 1.152, Revision 3. These include performing a security assessment to identify the digital safety system's potential weaknesses and vulnerabilities, ensuring there is no capability for remote access, ensuring the development systems are isolated from external networks, ensuring that the safety system does not include undocumented code, and establishing physical and logical access controls.

The procedure requires ID and password controls for computers where the development activities for digital safety systems are implemented, in accordance with Toshiba ISRGs SEC 101 and SEC 1-02. It also calls for physical protection to be applied to the development work area and the storage area for the documents and software products, and for appropriate controls to be employed in the testing area.

Regarding storage media control, the procedure states that electronic files prepared as system configuration items are to be stored and controlled in non-rewritable storage media such as a CD-R. To prevent information leakage, unauthorized modification or damage, the storage media is to be kept in [

].

The procedure calls for an incident response and recovery plan to be developed in case of a security incident or compromised computer. Awareness, training, configuration management controls, and security audits are also discussed.

Regarding control of software tools, the procedures states that qualified software of software tools are to be maintained as the registered software, stored in non-rewritable storage media, and are to be controlled by the Configuration Manager (for FPGA software tools) or the Tool Master (for software tools except for FPGA software tools).

Security Review Activities (PRM system)

Toshiba explained to the NRC staff that because the PRM system was developed before there were stringent security controls and procedures implemented, the security review for the PRM system was performed only at the Module Validation Testing Phase. The security review activities for the PRM system are described in section 3.6, “Configuration and Security Issues,” of FPG-DRT-C51-0016, “PRM Unit/Module Validation Testing Phase V&V Report,” Rev. 1. This document is included as Attachment 5 of Part V of the LTR, Rev. 3 (ADAMS Accession No. ML15246A176).

Security Assessment Meeting Minutes (OPRM unit)

NICSD conducted several Security Assessment Meetings to identify and evaluate secure development vulnerabilities throughout the lifecycle phases of the NRW-FPGA-Based I&C System Qualification Project (OPRM unit). The NRC staff reviewed the Security Assessment Meeting Minutes for the following lifecycle phases:

A. Project Planning and Concept Definition Phase, January 13, 2012, REC-JHS-000344, Rev. 1

The meeting minutes discuss the security of servers and PCs used in the development of digital safety systems, and the secure operational environment features of the safety system. It concludes that there is no remote access to the safety system, confirms one directional data transfer from safety to non-safety, and no non-safety to safety data transfer for the OPRM unit. Regarding the secure development environment features, it lists the following:

1. The development network is isolated from external network.
2. PCs require a user ID and password for login.
3. PPDD uses a standalone development environment for FPGA logic synthesis and place and route.
4. Development systems are located in an isolated room.
5. Servers are controlled.
6. Individual PCs are in offices with security doors.

B. Requirements Definition Phase, May 31, 2012, MOM-JHS-000015, Rev. 0

During this meeting, various security control activities were confirmed as having been implemented. These include performing the security assessment for the Requirements Definitions Phase in accordance with the V&V Plan, and that the security requirements have been incorporated into the procurement documents issued for PPDD.

The meeting minutes contains a list of the NQ-2037 security requirements and how they were addressed by NICSD and PPDD. An open item for applying the newest security patch to the PCs is identified as 'Closed'.

The meeting minutes also contains a list of the Appendix-B workers in the Nuclear Instrumentation Systems Development & Design Group, along with their employee identification number. A separate list contains the Server Access Control List (or Authorized Personnel List), which identifies the employee name, employee identification number and organization.

C. Design Phase, September 12, 2012, MOM-JHS-000046, Rev. 0

During this meeting, various security control activities were confirmed as having been implemented. These include performing the security assessment for the Design Phase in accordance with the V&V Plan, checking that software tools have been controlled with the software tool information sheet in accordance with E-68020, "PPDD Procedural Standard for Control of Software Tools Used with FPGA Based Systems," and confirming that Fuchu's security measures have been taken for computers used by PPDD developers involved in safety-related developments.

Two security assessment open items are identified. One open items request checking the latest registration information to verify that inappropriate personnel have not been registered through the access control in the project management system and the Fuchu PS file server. The second open item explains that the security control state in TDMS could not be checked, and therefore requests checking the TDMS control standards.

D. Implementation and Integration Phase, Module Validation Testing, October 11, 2012, MOM-JHS-000052, Rev. 0

During this meeting, various security control activities were confirmed as having been implemented during the Implementation and Integration phase. These include performing the security assessment for the Implementation Phase and Integration Phase in accordance with the V&V Plan.

The NICSD IV&V Team confirmed that the security requirements from the Unit DDS (e.g., adoption of a key-switch, and disallowing remote access) have been adequately traced through the V&V activities for the Module Design Specification, the FPGA Design Specification, and the RTM. The NICSD IV&V Team also confirmed that the security countermeasures of the test environment were performed.

The PPDD engineer confirmed through FPGA Testing and Module Validation Testing that no irregular behavior occurred. The PPDD engineer also confirmed through source code review that it has not identified any hidden functions or vulnerable features embedded in the code.

Additionally, various security control activities were confirmed as having been implemented during Module Validation testing. These include performing the security assessment for the Module Validation Testing in accordance with the V&VP. After PPDD sent the Module Validation Test Records to NICSD, the NICSD IV&V Team confirmed the validity of the security requirements.

The following security countermeasures were also confirmed:

- NICSD personally delivered the fuse map on a CDR-R and/or DVR-R.
- Embedment of logic into FPGAs was performed in the TDMS room used exclusively for logic embedment, as witnessed by NICSD.
- The embedded FPGAs are kept in a key-locked cabinet in the room designated only for FPGA logic embedment.
- During module assembly, the type and serial number of FPGAs mounted into a module assembly were recorded for traceability.
- A module manufactured by TDMS is placed in the PPDD receipt inspection test area. After testing is completed, the module goes through NICSD receipt inspection and is inserted in a unit.

The meeting minutes include the status of the two security assessment open items identified in the Design Phase meeting minutes. The open item to verify that inappropriate personnel have not been registered through the access control in the project management system and the Fuchu PS file server is marked as still being 'Open' and is assigned to PPDD. The open item for checking the TDMS control standards is marked as being 'Closed'.

E. System Validation Testing Phase, November 9, 2012, MOM-JHS-000059, Rev. 0 During this meeting, various security control activities were confirmed as having been implemented during the System Validation Testing phase. The secure development environment activities performed by the NICSD IV&V Team include the following:

- Performed the security assessment for the System Validation Testing Phase in accordance with the V&V Plan.
- Confirmed that the NICSD Quality Control Group (NICS-QC) registers test results with the Fuchu Data Management System, and confirmed that a rule requires that hardcopy of quality records submitted to NED be temporarily kept in a safe in a locked storeroom.
- Confirmed that NICS-QC Test Personnel performed System Validation Testing using the OPRM Test Tool managed in accordance with NQ-2003 and that no other PCs or software tools were used.
- Confirmed that write-once media – on which test equipment software that is installed on OPRM Test Tool used for System Validation Testing is stored – is kept in [ ].
- Confirmed that System Validation Testing was performed in [ ].
- Confirmed that PCs used by NICS-QC Test Personnel at NICS-QC office to prepare test procedures are managed in accordance with SEC 1-02 and that the required security measures have been taken on the PCs.
- Confirmed that NICS-QC Test Personnel have gone through education and training on NQ-2037.

The NICSD IV&V Team also confirmed the following secure operational environment features:

- Checked that the key-switch operation, which was identified as a security measure of the OPRM unit identified in the EDS, and parameter setting functions of the OPRM unit were tested in the System Validation Testing.
- Confirmed that no behaviors other than those specified in the test procedures were observed in the System Validation Testing through the review of the System Validation Testing.

The NRC staff noted that the System Validation Testing Phase meeting minutes do not include the status of the security assessment open item that was identified as still being open in the Implementation and Integration Phase, Module Validation Testing phase

meeting minutes. This open item was to verify that inappropriate personnel have not been registered through the access control in the project management system and Fuchu PS file server. The NRC staff informed Toshiba that there is no document explaining how this item open item was closed. Toshiba NICS-QA opened SCAR-16-017 to address how this open item was resolved. NICSD V&V is identified as the responsible organization for the SCAR. The SCAR recommended Corrective Action is to check the project management system and the Fuchu PS file server access rights, and correct the meeting minutes. The NRC staff created open item 91 to review the resolution to SCAR-16-017.

Fuchu Complex Controls

Toshiba has implemented physical access controls over the development environment at the Fuchu Complex. For example, guards stationed at the Complex entrance only allow Toshiba personnel with identification badges to enter. Non-Toshiba personnel must wear a visitor badge and be escorted by a Toshiba employee within the Complex. The visitor badge must be returned to Toshiba when exiting the Complex.

Media Storage Room Controls

The NRC staff was given a tour of the Media Storage Room. [

].

Manufacturing, Assembly and Testing Facility Controls

The NRC staff toured the Manufacturing, Assembly and Testing Facility known as the [ ]. [ ]. The NRC staff was shown one chassis of the OPRM unit (1 division) and the PRM system.

Toshiba personnel opened the flow module and the NRC staff observed the rotary switches and the three FPGAs. The rotary switches are on the inside of the module, therefore, the module needs to be removed from the rack and opened in order to access the rotary switches and change the setpoint.

The LPRM modules have a key-switch to select between the Operating, Standby, or Bypass modes. The same key was used for each LPRM module within the two chassis in the rack. The NRC staff was informed that the same key would be used for all modules within the same division.

The NRC staff observed that the Appendix B area for parts storage (after receipt inspection), the US Safety-Related Warehouse storage, and the shipping area are locked. The temporary QA Records Storage Room is also locked, and the key is controlled by the [ ].

Fuchu Complex Information System Controls

The NRC staff interviewed the Fuchu Complex Engineering & Information System Department Senior Manager to discuss the security controls used on the Fuchu server and overall network infrastructure. The NRC staff was informed that the Fuchu server used to be owned and controlled by the Fuchu Complex IT department, but it is now owned and controlled by the

Toshiba corporate IT department. In 2008 a transition of the server was started and a backup server location was set up [ ]. After the 2011 earthquake, the main Fuchu server was moved to [ ] and ownership was transferred to the Toshiba corporate IT department.

The development network is isolated from the corporate network through the use of firewalls. All Toshiba PCs are encrypted, and the passwords must be changed [ ]. Unauthorized portable media is detected if plugged in to a PC. Additionally, all application software in monitored by [ ]. The IT department has a list of allowed software to be installed on the servers. The application software that does reside on the servers is tested by the IT department before installation. A Toshiba corporate-wide antivirus software is implemented, monitored and reviewed for warnings. A batch file scan of each PC is performed every six months. While daily file changes are capture through daily backups, a full server backup is performed once a week.

Toshiba uses the IBM® Rational® DOORS® management tool for requirement traceability. The tool keeps track of the changes made to the files via a change log. The application client is installed on a limited number of local PCs, and the application database is installed on a database server. Use of the application client requires a unique user login ID and password for access.

4.4 PPDD Secure Development Environment

PPDD Secure Development Environment Procedure

The NRC staff reviewed Toshiba document 9B8H3559, "NRW-FPGA-Based I&C System Qualification Project (Development Plan)," Rev. 6, which establishes the PPDD security measures for the design, test and programming PCs and firewall. This document references Toshiba documents NQ-2037, SEC 1-01, and SEC 1-02. The plan contains configuration management requirements for the software and tools installed on the PCs, including the software type, name, and version number.

Appendix A of this document contains the PPDD secure development measure procedures for the PPDD design and test PCs and Local Area Network (LAN). These include discussion on [ ]. Toshiba provided the NRC staff with a translation of Appendix A of 9B8H3559 and

gave it the document number MEM-JH8-000125. This appendix states that the [

]. If any abnormality is identified, both NCISD and PPDD are to valuate the severity and determine the measures to be taken.

The plan states that the security strength of [

].

The secure development settings for the development PCs include [

].

Appendix A identifies the secure development measures for the VHDL coding PC, the PC for logic synthesis (including place and route), the PC for FPGA testing, the PC for configuration management, and the PC for writing the FPGA. The security measures identifies that [

]. It also specifies that [ ] is to control the keys.

The appendix also identifies the secure development measures for the firewall equipment. It describes that [

]. [

] controls the login password.

There are self-check items for each of the controlled equipment identified to verify that the measures established have been incorporated and are still being implemented. These selfchecks are to be performed before and after each use, and once a month during the project.

PPDD Design and Testing Room Area Controls

The NRC staff observed the secure development measures implemented in the PPDD Design and Testing Room Area. This room requires [

].

The room contains two standalone desktop PCs ([ ]) used for FPGA design. On the back of one of these PCs, there is [

]. On the other PC, [

].

The room also contains three desktop PCs used for testing which also have [

]. These three PCs require the

use of testing software that is located in [
]. The unused Ethernet ports on the firewall are [
]. [ ] controls the keys and the
[ ]. The design and testing PCs require a user ID and password for

login. The unused PCs (one design PC, and two test PCs) have [
] showing the status of the PC.

The FE library does not reside in the design PCs. The FE library is contained in a DVD that is inserted to the design PC. Once the design file is ready for testing and burning, the DVD drive of the design PC is unlocked with permission of the PPDD Group Manager. A DVD-R (nonrewritable media) is then used to transfer the file to the test PC.

Once PPDD designs the FPGA and burns the image on a DVD, it writes the identification information on the DVD label. NICSD then checks the content of the DVD, adds identifiers to the label, prepares an accompanying information sheet, and stores the DVD in a locked safe. When the FPGA image is to be programmed, the DVD is transferred to TDMS via PPDD as witnessed by NICSD. TDMS then uses the DVD image to burn the FPGA in the TMDS FPGA Programming Room. NICSD has configuration control of the FPGA, while PPDD maintains Quality Control.

The NRC staff was given a demonstration of the simulation and stimulation test coverage tool which resulted in 100% coverage of the movable/changeable signals. Hardware testing was also performed. The test results are then burned into non-rewritable media and handed to NICSD.

TDMS FPGA Burning Room Controls

The NRC staff observed the secure development measures implemented in the TDMS FPGA Programming Room. TDMS is the vendor for printed circuit board (PCB) design and manufacturing. Inside the TDMS building there is a FPGA Programming Room which is [ ]. There are two stand-alone desktop PCs in this room, which also have [ ]. These PCs are controlled by PPDD. The software tool used for programming the FPGA is already loaded onto these PCs.

The NRC staff observed how the [ ] a DVD to be inserted and the FPGA to be burned. The NRC staff observed the following process for burning the FPGA:

1. A self-diagnostic test is performed on the software tool before burning. This is described in a procedure (in Japanese) which is stored in the same room.
2. The FPGA image DVD is loaded onto the PC.
3. The sheet that accompanies the DVD contains the tool configuration settings, and is used to verify the information on the DVD.
4. The checksum on the sheet is compared with the checksum on the tool.
5. The new FPGA is inserted into the programming tool.
6. Verification of the burn in process is performed using the checksum. In the demonstration given, the checksum matched the one on the sheet.
7. The FPGA is then removed and placed [
], awaiting installation into the PCB.

PPDD Quality Control Test Area Controls

The NRC staff observed the secure development measures implemented in the PPDD Quality Control Test Area. This room contains [

] used for Module Validation Testing. The [

].

4.5 Code Review Activities

Code Review Guide

The NRC staff reviewed Toshiba document 8M8K0000, "Code Review Guide," Rev. 1, which provides recommended practices for code review activities performed by NICSD in order to detect and identify software product anomalies. This document is a generic guide, and therefore it does not have a project-specific document number.

The NICSD code review process verifies that the software product satisfies its specifications and specified quality attributes, and conforms to applicable regulations, standards, guidelines, plans, and procedures. It also identifies deviations from standards and specifications.

The guide specifies that the NICSD IV&V Lead is responsible for source code review. Apart from this guide, input to the code review process includes the Source Code Review Plan (which describes the purpose and scope of the review), the software product to be reviewed, the Source Code Review Sheet, requirements specifications, and applicable VNNRs, SNNRs, and SCARs.

Attachment A of the guide discusses the necessary skill and qualification for code review activities. For example, the Code Review Lead is to have three years or more experience of FPGA circuit design or equivalent experience certified by the NICSD IV&V Lead. The Code Review Lead is also to be a NICSD Appendix-B QA Program Worker who is listed in "Personnel List for Performing Safety related Work", and must have completed the QA Program Course "Designed of FPGA" and the project specific training (i.e., Code Review Course).

The guide also includes discussions on activities such as Managerial Control, Planning, Plan Review Meeting, Entrance Meeting, Code Review, Exit Meeting, Rework and Follow-up. Attachment D contains a Compliance Traceability Matrix that shows how the code review guide conforms to Section 6 of IEEE Std. 1028-1997.

Source Code Review Sheet

The NRC staff reviewed FC51-3704-1103, "Software Validation Report: Source Code Review Sheet for NRW-FPGA-Based I&C System Qualification Project," Rev. 3. The purpose of this document is to detect and identify anomalies in the software product that will be incorporated into FPGA logic for the OPRM unit, and record the source code review activities performed by the Code Review Team in NICSD IV&V. The Code Review Team uses the Synopsys® SpyGlass Lint Very High Speed Integrated Circuit Hardware Description Language (VHDL) source code tool to analyze the structure of the register transfer level (RTL) and identify design issues.

Section 7 of this document contains the results and conclusions of the source code review activities. It states that the Code Review Team found [ ] anomalies, the majority of which do not require rework on the VHDL source code and are classified as either recommendations or

minor comments. [ ] anomalies were found that required rework on the VHDL source code.

Table 7-1, “Code Review Result (Anomaly Counts),” identifies which type of code anomalies (e.g., superfluous, inconsistent, not conforming to standards, etc.) were found in each of the FPGA codes. The table also identifies which FPGA codes had an anomaly which required rework on the VHDL source code, or anomalies which required revision of the FPGA Design Specification.

The [ ] anomalies found which required rework were on the [ ] FPGA and [ ] FPGA pieces of VHDL source code. These were found to not conform to mandatory-level coding rule A.4.1.d of E-68017, “PPDD Procedural Standard for FPGA Device Development” Rev. 9, which states that the code “shall not use the same name changing the capital letter/small letter of the English character.”

Sections 6.25 and 6.28 of FC51-3704-1103 contain the source code review sheets for [ ] and [ ], respectively. The code review sheets include the responsible code reviewer, the identification of the software product, the code review checklist, an anomaly list, the NICSD exit meeting information, and the conclusions. The identification of the software product includes the code name, the code number, the source code file information (i.e., file name, time stamp, file size), the code developer organization (in this case PPDD), the FPGA Design Specification (document number and revision), and the media number that contains the software product to be revised.

The source code review concluded that making a revision to use a consistent signal name in the VHDL source code and to perform the logic synthesis and place & route again would be needed to resolve the [ ] anomalies. FC51-3704-1103 states that PPDD corrected the internal signal in the VHDL source code in accordance with the coding rule, performed the logic synthesis and place & route again, confirmed that the time stamp was the only difference as the comparison result of output files, and confirmed the checksum of the fuse map after rework did not change. The document also states that PPDD checked the code again using the Synopsys® SpyGlass Lint VHDL source code tool and confirmed that the anomalies were resolved.