Document No.
IM-2015-000152 (Non-Proprietary)

Response to the Action Items from January 28, 2015 Meeting on Toshiba FPGA LTR

(Non-Proprietary)

Note :
This document provides responses from Toshiba to the U.S. Nuclear Regulatory Commission (NRC) related to the action items from the January 28, 2015 meeting on the Toshiba Field Programmable Gate Array (FPGA) Licensing Topical Report (LTR).

001	Mar 23, 2015	Revision with identification of proprietary information and update of responses to the action items.	T.Tamba Mar 23, 2015	T. Hayashi Mar 23, 2015	T.Miyazaki Mar 23, 2015
000	Mar 3,2015	Initial Issue	T.Tamba Mar 3, 2015	T.Hayashi Mar 3, 2015	T.Miyazaki Mar 3, 2015
Revision	Date	Contents	Approved by	Reviewed by	Prepared by

Nuclear Energy Systems & Services Division
Instrumentation & Control Systems Design and Engineering Dept.

1 Purpose

This document provides responses from Toshiba to the U.S. Nuclear Regulatory Commission (NRC) related to the action items from the January 28, 2015 meeting on "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 0.

2 Reference

(1) Toshiba Field Programmable Gate Array (FPGA) Based Safety Related I&C Platform, IM-2014-001298 Rev.0

(2) SUMMARY OF JANUARY 28, 2015, MEETING on "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 0 (TAC NO. ME9861)

(3) Proprietary Handouts used at January 28, 2015 Meeting, TOS-CR-FPG-2015-0001

3 Response to the Action Items

3.1 Response to Action Item 1

Action Item 1

Check whether Toshiba is still on the Approved-Supplier List for South Texas Project Units 3 & 4.

Toshiba Response to the Action Item 1

Toshiba confirmed with NINA that all divisions of Toshiba remain on the Approved Supplier List for South Texas Project Units 3 & 4. NINA last audited the Toshiba Nuclear Instrumentation & Control Systems Department (NICSD) in 2011, when NINA slowed down the South Texas Project Units 3 & 4 Project.

3.2 Response to Action Item 2

Action Item 2

Confirm that a Commercial Grade Dedication (CGD) report was prepared for the old design process. Provide that report or its equivalent report.

Toshiba Response to the Action Item 2

A CGD report for Oscillation Power Range Monitor (OPRM) was prepared under the new process and documents the acceptance of Critical Characteristics for Acceptance (CCA). For the PRM, the old design process used an Acceptance Checklist to document the acceptance of CCAs and is equivalent to the CGD report for the OPRM. Toshiba provided the Acceptance Checklist for the Power Range Monirot (PRM) units (ACLFPG-JOS-C51-0001-01 Rev.0) on the Toshiba Document Portal (TDP) on March 6, 2015.

3.3 Response to Action Item 3

Action Item 3

Provide a formal response that the CGD process is looking at all requirements as critical characteristics in the Equipment Requirement Specifications (ERS).

Toshiba Response to the Action Item 3

Attachment-1 provides an explanation of the method Toshiba used to identify the critical characteristics (CCs) listed in Appendix A of the PTER, and how the Acceptance Plan was prepared. Attachment-1 only provides an explanation for a selection of some CCs. Toshiba will supply an explanation for all CCs in Appendix A of the PTER in the RAI response.

3.4 Response to Action Item 4

Action Item 4

Provide more information on the discussions related to critical characteristics.

Toshiba Response to the Action Item 4

See response to 3.3 above (Action Item 3).

3.5 Response to Action Item 5

Action Item 5

Explain how the critical characteristics in Appendix A of the PTER relate to the information in the Toshiba Acceptance Plan.

Toshiba Response to the Action Item 5

See response to 3.3 above (Action Item 3).

3.6 Response to Action Item 6

Action Item 6

Explain what activities Toshiba did for the CGD in the Preliminary Technical Evaluation Report and Oscillation Power Range Monitor.

Toshiba Response to the Action Item 6

In the Preliminary Technical Evaluation Report (PTER) for the PRM, the following activities were conducted for the CGD;

- Identify the source of Critical Characteristics for Design (CCDs) and Critical Characteristics for Acceptance (CCAs)
- List all the sections of the source documents where requirements are described. The list is provided in Appendix A of the PTER.
- Determine which requirements will be confirmed during procurement of Commercial Grade (CG) Items, performance of CG Services, Qualification Analysis, Qualification Tests, or Software Qualification.
- For items to be confirmed during procurement of CG Items, the CCDs and CCAs are identified and the applicable method to confirm the CCs are identified in PTER Appendix A.
- For items to be confirmed during procurement of CG Services, the applicable method to confirm each CC is identified in PTER Appendix A.

In the PTER for the OPRM, the following activities were conducted;

- Identify the requirements for the OPRM unit and document them in PTER Section 4.
- List the functions of the OPRM unit and service (e.g. qualification testing service, calibration service) and document them in PTER Section 5.
- Identify which items will be verified during procurement of CG items and which services will be verified during CG services and document in PTER Section 5.
- Develop an outline of CCAs and verification methods for CG Items and CG Services, and document them in PTER Section 8.

3.7 Response to Action Item 7

Action Item 7

Create a table comparing the old and new design process for CGD.

Toshiba Response to the Action Item 7

Table 3.7-1 on the next page provides a comparison of the old (original) and new (current) design process for CGD. This figure corresponds to slides 8 and 12 of the "Toshiba Field Programmable Gate Array (FPGA) Based Safety Related I&C Platform", IM-2014-001298 Rev.0 (Reference (1)) presentation provided to the NRC prior to the January 28 2015, NRC meeting.

Table 3.7-1 Comparison of the Old (Original) and New (Current) Design Process for CGD

Current Process		Original Process	
Document	Responsible	Document	Responsible
System Design Description (SDD) Instrument Equipment Diagram (IED) Interlock Block Diagram (IBD)	NED	Equipment Requirement Specification (ERS)	NED
Equipment Design Specification (EDS)	NICSD	Equipment Requirement Specification (ERS)	NED
CGD Plan	NICSD	Qualification Plan[Note)]	NED
Preliminary Technical Evaluation Report (PTER)	NICSD	Preliminary Technical Evaluation Report (PTER)	NED
Commercial Dedication Instruction (CDI)	NICSD	Acceptance Plan for CGI/CGS	NED
Procurement Document to the module supplier and commercial suppliers	NICSD	Procurement Specification to NICSD	NED
		QA Specification to NICSD	NED
Job Order to Commercial Vendor	NICSD	Job Order to NICSD	NED
Vendor Documents for CG Item/Services	Commercial Vendor	Vendor Documents for CG Item/Services	NICSD
Acceptance Records for CGI/CGS	NICSD	Acceptance Records for CGI/CGS	NED
CGD Report	NICSD	Acceptance Checklist	NED
Final Technical Evaluation Report (FTER)	NICSD	Final Technical Evaluation Report (FTER)	NED

Note) Elements of the CGD Plan is included in the Qualification plan.

3.8 Response to Action Item 8

Action Item 8

Describe and clarify how validation and verification tests are used in the equipment qualification testing.

Toshiba Response to the Action Item 8

Section 5.1 of the PRM System Qualification Test Summary Report, FPG-TRT-C51-0101, Rev.0, describes the system set-up and check-out test for pre-qualification and the burn-in testing that was performed as a part of the system validation test for Verification and Validation (V&V) activities. V&V activities took credit for the system setup and burn in testing. V&V did not take credit for the qualification testing. The Equipment Qualification (EQ) engineer examined the system validation test plan, procedure, and results and concluded that the system set-up and checkout test was sufficient and acceptable, and these tests did not need to be repeated before qualification testing.

3.9 Response to Action Item 9

Action Item 9

Provide the picture of module and middle-plane communication on slide 42.

Toshiba Response to the Action Item 9

The picture on slide 42 of the "Toshiba Field Programmable Gate Array (FPGA) Based Safety Related I&C Platform," IM-2014-001298 Rev.0 (Reference (1)) presentation will be added in the next revision of the LTR.

3.10 Response to Action Item 10

Action Item 10

Confirm the communication link between the front and back middle planes.

Toshiba Response to the Action Item 10

The front and rear middle planes are connected by [ ]a,c connectors. Figure 3.10-1 shows a drawing of the Local Power Range Monitor (LPRM) unit viewed from above. The blue arrows denote the flow of LPRM data from the LPRM modules to the TRN module through the communication links.

[ ]a,c

Power line connector

Rear Middle Plane

Power line connector

Front Middle Plane

← Flow of LPRM data through communication links

Figure 3.10-1 Drawing of the middle planes viewed from above the LPRM unit

Figure 3.10-2 and Figure 3.10-3 are photographs of the LPRM unit. The photographs were taken from the bottom of the chassis to provide better views of the middle planes and their connections.

a,c

Rear
Middle Plane

Front
Middle Plane

Figure 3.10-2 LPRM unit viewed from below

a,c

Rear
Middle Plane

Front
middle plane

[ ] a,c
connectors

Figure 3.10-3 Close View of the Connectors (red rectangle in Figure 3.10-2)

3.11 Response to Action Item 11

Action Item 11

Describe the middle plane configuration for each chassis (unit).

Toshiba Response to the Action Item 11

The configurations of the middle planes for the LPRM, LPRM/ Average Power Range Monitor (APRM), FLOW and OPRM modules are shown in Figure 3.10-1, Figure 3.11-1, Figure 3.11-2, and Figure 3.11-3. Signal connections are not shown for clarity. More data on connections and data flow is provided in Section 3.14 (Toshiba Response to the Action Item 14).

Figure 3.11-1 Drawing of the middle plane configuration for the LPRM/APRM unit

a,c

Rear
middle plane

Front
middle plane

Figure 3.11-2 Drawing of the middle plane configuration for the FLOW unit

a,c

Rear
middle plane

Front
middle plane

Figure 3.11-3 Drawing of the middle plane configuration for the OPRM unit

3.12 Response to Action Item 12

Action Item 12

Confirm the use of time out failure and how you switch to a secondary link for data.

Toshiba Response to the Action Item 12

Switching from the primary link to the secondary link is based on timeout monitoring of the primary link in the following communication links:

(1) Multiplexed data from the [ ]a,c module to the [ ]a,c module in the LPRM/APRM unit
(2) Multiplexed data from the [ ]a,c module to the [ ]a,c module in the LPRM/APRM unit
(3) Multiplexed data from the [ ]a,c module to the [ ]a,c module in the OPRM unit

For these links, the receiver ([ ]a,c module) uses data from the primary link when the primary link is active. The receiver switches to the secondary link only after [ ]a,c consecutive errors of the primary link are detected, which causes the primary link to be marked as inactive. The receiver returns to the primary link [ ]a,c pulses are detected by the [ ]a,c module or normal data is detected by the [ ]a,c module.

Note that for Case (2), [ ]a,c communication is somewhat unique, as shown in Figure 3.12-1.

[ ]a,c

Figure 3.12-1 Functional Block Diagram of TRN module and Data Flow

3.13 Response to Action Item 13

Action Item 13

Confirm the new version of the TRN and RCN modules can be used in the Power Range Monitor.

Toshiba Response to the Action Item 13

The new version of the TRN and RCV modules are common modules that can be used in the PRM and OPRM. The new TRN and RCV module hardware used in the OPRM are the same as the old TRN and RCV modules used in the PRM qualification except grounding lines were added to the printed circuit boards to improve electrostatic discharge withstand capabilities.

Another difference between the new and old TRN and RCV modules is that a portion of the logic implemented in the FPGAs has been revised to support the calculation of CRCs.

Figure 3.13-1 shows a function block diagram of the old TRN module. The old TRN module uses the following three types of FPGAs:

a,c

[ ]

The new TRN module uses the same [ ] a,c FPGAs as the old TRN module. The [ ] a,c FPGA, marked in red in the figure below, is replaced with the [ ] a,c FPGA used in the new TRN module. Changing the [ ] a,c FPGA to the [ ] a,c FPGA was accomplished by revising the FPGA code only. The same type of FPGA is used as on the original module. The [ ] a,c FPGA calculates a [ ] a,c CRC, and attaches the CRC to the end of the data frame before converting the data to Manchester code.

[ ]a,c

Figure 3.13-1 Function Block Diagram of TRN module used in the Power Range Monitor

Likewise, the old RCV module uses[ ]a,c types of FPGA, called the[ ]a,c These FPGAs were re-coded and are designated as[ ]a,c in the new RCV module. The difference between the functionality of the old and new FPGAs is that the new FPGAs uses the CRC code for error checking in addition to parity check.

[ ]a,c

Electrical Signal
Optical Signal

Figure 3.13-2 Function Block Diagram of RCV module used in the Power Range Monitor

Either the old TRN and RCV modules or the new TRN and RCV modules can be used in both the PRM and the OPRM, provided an old TRN is paired with a old RCV or a new TRN is paired with a new RCV. An old module cannot be paired with a new module.

3.14 Response to Action Item 14

Action Item 14

Clarify what type of diagnosis is done for communication and what modules are using them. (See item 21 below)

Toshiba Response to the Action Item 14

Table 3.14-1 shows the type of diagnosis for communication in the LPRM unit. For the communication path 1 numbered in Table 3.14-1, see Figure 3.10-1.

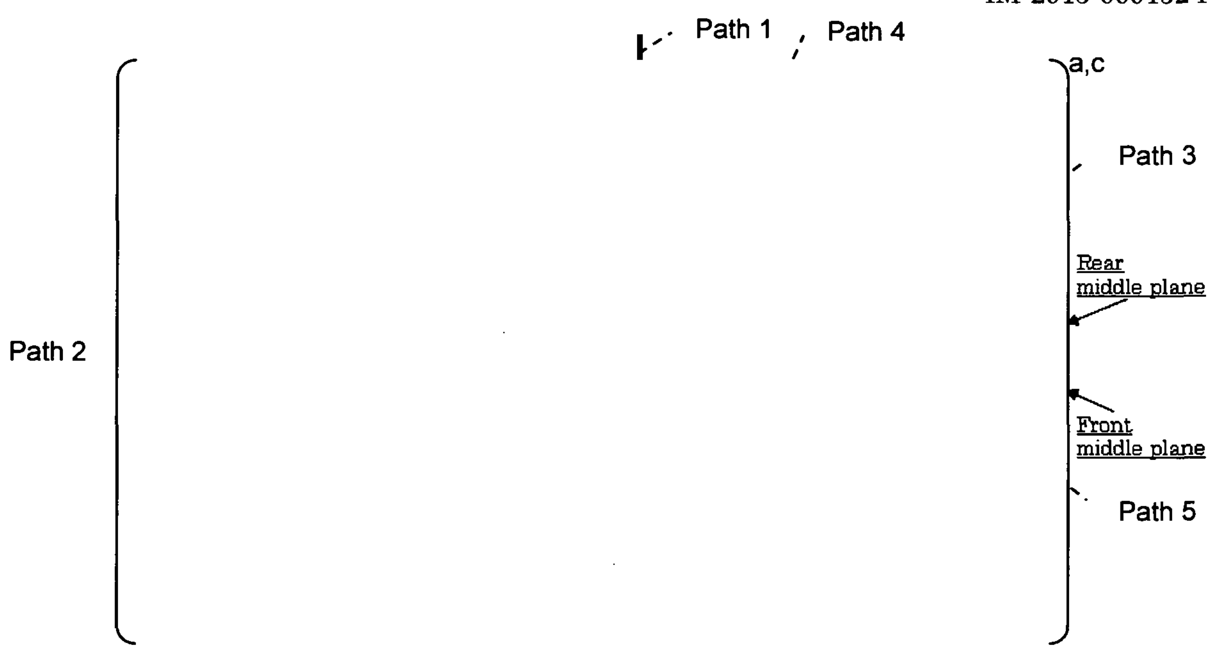
Table 3.14-1 Diagnoses for Communication in the LPRM unit

Path	Communication	Diagnoses			
		Parity error	Timeout error	Refresh Count	CRC
1	[ ]a,c to [ ]a,c	[			]a,c

Table 3.14-2 shows types of diagnosis for communication in LPRM/APRM unit Figure 3.14-1 shows the communication paths numbered in Table 3.14-2.

Table 3.14-2 Diagnoses for Communication in the LPRM/APRM unit

Path	Communication	Diagnoses			
		Parity error	Timeout error	Refresh Count	CRC
1	[ ]a,c to [ ]a,c	[			]a,c
2	[ ]a,c to [ ]a,c				
3	[ ]a,c to [ ]a,c				
4	[ ]a,c to [ ]a,c				
5	[ ]a,c to [ ]a,c				



Drawing of the middle plane configuration for the LPRM/APRM unit

Figure 3.14-1 Communication Paths in the LPRM/APRM unit

Table 3.14-3 shows the types of diagnosis for communication in the FLOW unit. Figure 3.14-2 shows the communication paths numbered in Table 3.14-3.

Table 3.14-3 Diagnoses for Communication in the FLOW unit

Path	Communication	Diagnoses			
		Parity error	Timeout error	Refresh Count	CRC
1	[ ]a,c to [ ]a,c	[			]a,c
2	[ ]a,c to [ ]a,c				
3	[ ]a,c to [ ]a,c				]

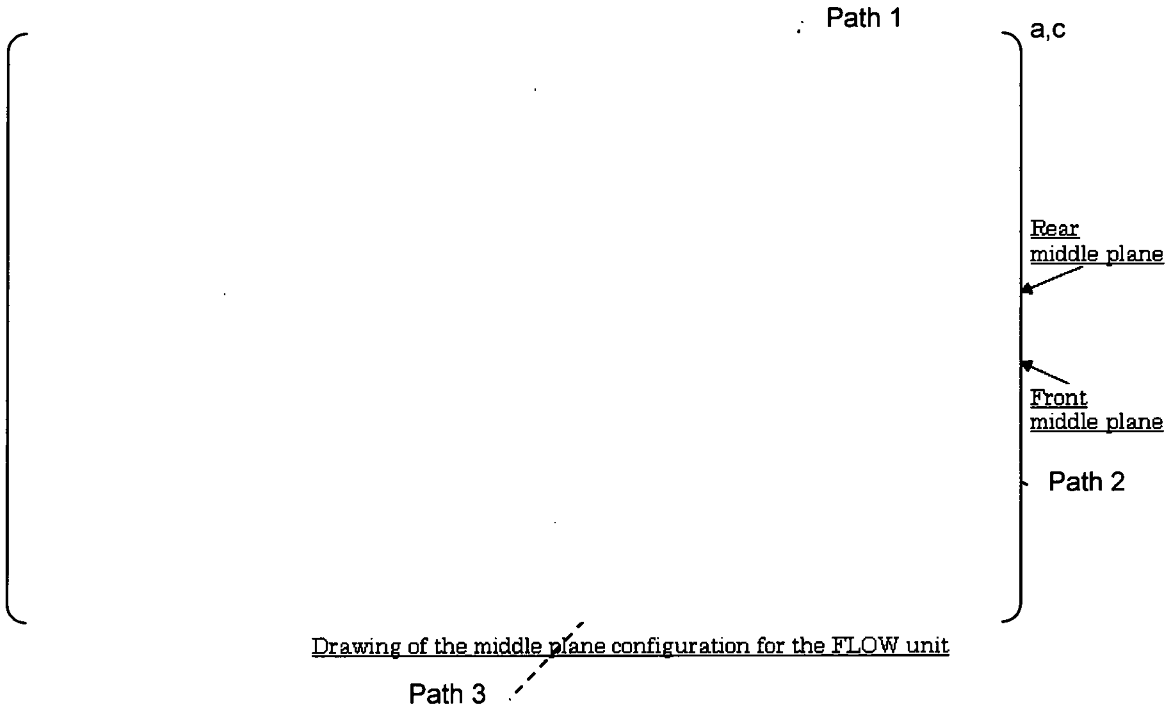


Figure 3.14-2 Communication Paths in the FLOW unit

Table 3.14-4 shows the types of diagnosis for communication in the OPRM unit. Figure 3.14-3 shows the communication paths numbered in Table 3.14-4.

Table 3.14-4 Diagnoses for Communication in the OPRM unit

Path	Communication	Diagnoses			
		Parity error	Timeout error	Refresh Count	CRC
1	[ ] a,c to [ ] a,c				a,c
2	[ ] a,c to [ ] a,c				
3	[ ] a,c to [ ] a,c				
4	[ ] a,c to [DAT/ST] a,c				
5	[ ] a,c to [ ] a,c				
6	[ ] a,c to [ ] a,c				
7	[ ] a,c to [ ] a,c				

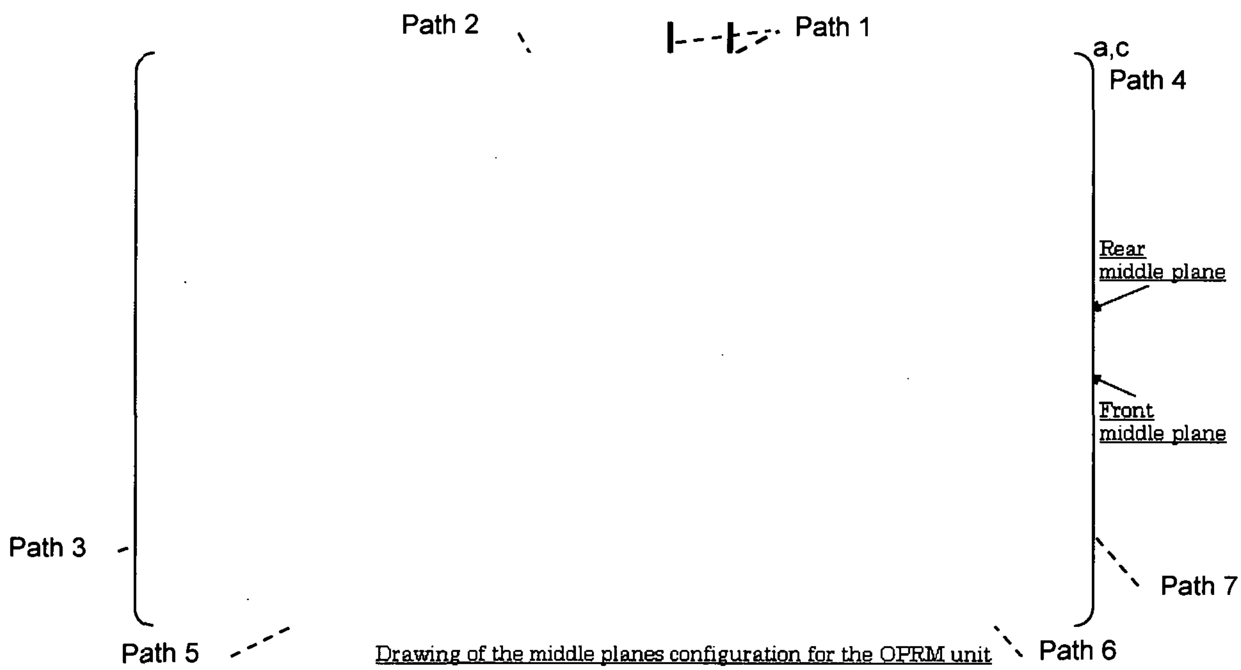


Figure 3.14-3 Communication Paths in the OPRM unit

3.15 Response to Action Item 15

Action Item 15

Provide justification and explain how the ERS has high-level requirements for communication, and what other documents provide detailed design information.

Toshiba Response to the Action Item 15

Section 5.2.2 of ERS describes the unit input/output requirements. This section specifies data to be transmitted as follows:

- Section 5.2.2.1 specifies the signals that the LPRM unit sends to the LPRM/APRM unit and external equipment.
- Section 5.2.2.2 specifies the signals that the LPRM/APRM unit receives from the LPRM and FLOW units, and the signals that the LPRM/APRM sends to external equipment.
- Section 5.2.2.3 specifies the signal that the FLOW unit sends to the LPRM/APRM unit.

ERS Section 5.2.3, "Module Requirements," includes the following subsections that describe the communication requirements for the TRN and RCV modules. Although the "communication requirements" are not completely defined for the PRM as a whole, the ERS specifies that the PRM includes two communication modules, i.e., TRN and RCV modules, and defines the requirements for the modules as follows:

ERS Sections 5.2.3.8 and 5.2.3.9 describe high-level requirements for the TRN and RCV modules, which perform communication between units or external equipment.

ERS Section 5.2.3.8 describes the TRN module, in Subsections 5.2.3.8.1, 5.2.3.8.2, and 5.2.3.8.3 state that the TRN module is mounted in the LPRM, LPRM/APRM, and FLOW units, and transmits the data described in Sections 5.2.2.1, 5.2.2.2, and 5.2.2.3 through fiber optical cables.

ERS Section 5.2.3.8 includes a watchdog timer requirement to monitor the periodic operation of the FPGA.

RS Section 5.2.3.9 describes the RCV module. The RCV module is mounted in the LPRM/APRM unit, receives serial data transmitted every [ ]a,c millisecond through each fiber optic cable, checks for periodic data transmission, and checks for the parity bit on every [ ]a,c word.

Communication self-diagnostic requirements are summarized in ERS Section 5.1.6 (e) and (f).

The Unit Equipment Design Specifications for the LPRM, LPRM/APRM, and FLOW units decompose high-level requirements for the PRM. These unit equipment design specifications include the following decomposed communication requirements for the TRN and RCV module:

- Data frame format
- Use of Manchester coding

Toshiba will make these Unit Equipment Design Specifications available by mid-April 2015 on the TDP.

The communication requirements for the TRN and RCV modules are defined further in the TRN Module Design Specification (MDS) and the RCV MDS, and implemented in FPGAs in programmable logic.

3.16 Response to Action Item 16

Action Item 16

Address what happens when one of the communication buffers fails.

Toshiba Response to the Action Item 16

The RCV module has two rotating buffers, one of which is providing the previously accepted message to other data users (i.e., modules) and the other is receiving the next message. These rotating buffers are not a separate device, such as an SRAM chip, but realized as a set of cells placed in the [ ]a,c FPGA.

Figure 3.16-1 shows part of functional diagram of the [ ]a,c FPGA around the communication buffers. Note that the figure is functional diagram, and does not reflect the actual placement of cells in the FPGA.

[ ]a,c

Figure 3.16-1 Functional Diagram around Communication Buffers

The [ ]a,c receives messages from [ ]a,c FPGA using a [ ]a,c One of the two [ ]a,c rotating buffers, Buffer 1 and Buffer 2, is selected at a time, and accepts the message from the [ ]a,c This buffer rotation is implemented in the FPGA by rotating [ ]a,c to the two buffers, instead of switching the signal paths to the buffers. That is, the [ ]a,c always sends the messages to the two buffers. The [ ]a,c in [ ]a,c generates a [ ]a,c [ ]a,c for one of the two rotating buffers at a time, to enable [ ]a,c of the received data. After the buffering of one message is completed, and when a next message comes from the [ ]a,c FPGA, the [ ]a,c switches the [ ]a,c from the current buffer to the other buffer. Both the buffers send [ ]a,c channel [ ]a,c according to the [ ]a,c [ ]a,c signal which specifies a channel number. The [ ]a,c selects one of the two data buffers according to the [ ]a,c

Since data always arrives at the two buffers, and rotation of the buffers is performed by rotating the [ ]a,c [ ]a,c generated in the same [ ]a,c FPGA, Toshiba considers that the possibility of one buffer failure without any failure of the other parts of the FPGA, such as [ ]a,c [ ]a,c or clock line, to be minimal and unlikely. If any of the programmable logic fails, the FPGA is likely to fail, which will result in a failure of the RCV module. The following discussion addresses what happens if one of the communication buffers fails:

If one of the two buffers, say Buffer 1, fails, the data from the failed Buffer 1 becomes corrupted. The RCV module provides the data to other modules, in a manner as: Buffer 1 data (corrupted), Buffer 2 data (uncorrupted), Buffer 1 data (corrupted) , Buffer 2 data (uncorrupted), ... The modules that receives above data are the [ ]a,c and [ ]a,c modules. Both modules perform parity checks of each data, and discard all corrupted data. The modules do not generate any alarm because the corrupted data is not received consecutively. As a result, the [ ]a,c and [ ]a,c modules accept uncorrupted data every two cycle times, [ ]a,c milliseconds, compared to the normal [ ]a,c milliseconds.

For the APRM module, this failure increases the time required for receiving uncorrupted data [ ]a,c milliseconds as illustrated in Figure 3.16-2.

a,c

[ ]

[ ]a,c Hence, the worst case trip signal is delayed by an additional [ ]a,c milliseconds. There is a case in which the APRM module could catch the data indicating the need for a trip at the same timing even with a single buffer failure.

[ ]a,c

Figure 3.16-2 Timing charts when both buffers are healthy (upper) and one buffer fails (lower)

Toshiba considers that a[ ]a,c ms delay is small when compared with other delays in the NMS and Reactor Protection System (RPS), and can be absorbed in the design or implementation of the other part of NMS or RPS.

The CELL module receives two types of data from the RCV module, data originated from the LPRM unit and data originated from the APRM unit, through separate three-wire electrical communication links. The cycle time of data is[ ]a,c milliseconds for the data from the LPRM unit, and[ ]a,c millisecond for the data from the APRM unit.

In the case of failure in the data from LPRM unit, the cycle time for receiving uncorrupted data increases from [ ]a,c milliseconds to[ ]a,c milliseconds. Since the execution cycle of the CELL module is[ ]a,c milliseconds, this small increase is within the timing margins and does not affect the safety function of

CELL module. Also, the increase in response time is small when compared to the expected response time for the OPRM which is in the order of seconds.

In the case of failure in the data from the APRM unit, the CELL module continues to use the last uncorrupted data that is received before the buffer fails. The data from the APRM unit includes the core power and flow to determine the automatic bypass of the OPRM. The OPRM is bypassed in the region where the core power < 30% or the core flow > 60%.

If the OPRM buffer fails while in the unbypassed region, the OPRM unit will not be bypassed when the core enters in the bypass region since new data will not be provided. Conversely, if the buffer fails in the bypass region, the OPRM unit will continue to be bypassed even when the core enters in the unbypassed region.

The OPRM system consists of four safety channels, each of which includes a separate OPRM. If one of the OPRM units fails to perform its safety function, the remaining three OPRM units can maintain the safety function performed by the OPRM system. The bypassed state of each OPRM is indicated to the operators.

3.17 Response to Action Item 17

Action Item 17

Provide a self-diagnostic summary table.

Toshiba Response to the Action Item 17

The self-diagnostic summary table on slide 57 of the "Toshiba Field Programmable Gate Array (FPGA) Based Safety Related I&C Platform", IM-2014-001298 Rev.0 (Reference (1)) presentation was added in the LTR revised in February as Table II-A-2-1.

3.18 Response to Action Item 18

Action Item 18

Provide diagrams for signal processing of watch-dog timers.

Toshiba Response to the Action Item 18

The watchdog timers of the CELL module are explained as an example. The CELL modules has two watchdog timers, one for FPGAs performing HMI function, and the other for FPGAs performing signal processing. Figure 3.18-1 is a diagram the signal chain of HMI FPGAs of the CELL module. The watchdog timer monitors the End of Processing (EOP) signal when it is passed from the [ ]a,c [ ]a,c FPGA to the [ ]a,c FPGA. The watchdog timer generates a minor failure alarm if the timer expires for the HMI FPGA signal chain.

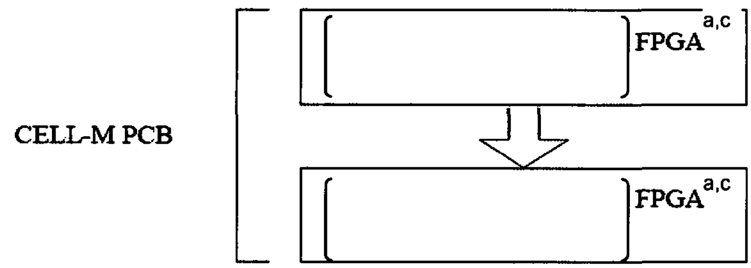


Figure 3.18-1 Signal Processing of Watchdog Timer for CELL module HMI FPGAs

Figure 3.18-2 is a diagram for signal chain of the FPGAs performing the signal processing. The watchdog timer monitors the EOP signal when it is passed from [ ]a,c through [ ]a,c The signal path branches at [ ]a,c to [ ]a,c and [ ]a,c and merges at [ ]a,c The watchdog timer generates an inoperative alarm if the timer expires.

[ ]a,c

Figure 3.18-2 Signal Processing of Watchdog Timer for CELL module Inoperative

Toshiba's design philosophy is to provide two individual watchdog timers to monitor:

- Signal processing FPGAs (i.e., for safety function), whose failure leads to an inoperative alarm, and

- HMI FPGAs, whose failure leads to a "Minor Failure."

Note that a failure of the [ ] a,c FPGA in an LPRM module leads to an inoperative alarm, since the [ ] a,c FPGA samples the module's mode switch, which makes the LPRM module inoperative if a mode other than OP(eration) is selected.

For modules other than the LPRM, the safety function is operable even if the HMI is inoperable, since the HMI logic is not required to pass signals to the next module.

In the CELL, AGRD, PBD, and LPRM modules, the signal processing FPGAs and HMI FPGAs have using separate signal chains. Each signal chain passes EOP signals to the next FPGA every time the FPGA completes its processing. The watchdog timer or one-shot retriggerable multi-vibrator accepts the EOP signal at the end of the chain, and resets itself. If the EOP is not accepted in a predetermined time, the watchdog timer expires, and generates an alarm.

In the APRM module, SQ-ROOT module and FLOW module, the signal processing FPGAs and HMI FPGAs are connected by the same signal chain. Even if HMI FPGAs cannot detect the EOP signal from the signal processing FPGAs within the predetermined period, the HMI FPGAs continue their operation to maintain HMI functions not being affected by failures of the signal processing FPGAs, which perform the safety functions.

3.19 Response to Action Item 19

Action Item 19

Describe how failures detected by and failure of the safety function watchdog timers can affect the safety function. Include the HIS watchdog timers in this discussion.

Toshiba Response to the Action Item 19

Effects on the safety function depend on the type of the module. The table shows maximum effects.

Watchdog Timer	Failure mode	Method of Failure Detection	Effect on the safety function
The Safety function watchdog timer	Generate a false alarm		
	Fails to generate an alarm		
The HIS watchdog timer	Generate a false alarm		
	Fails to generate an alarm		

a,c

FPG-DRT-C51-001 "Requirements Definition Phase Hazard Analysis Report" and FC51-3704-1101 "Software Safety Analysis Report for Safety-Related Oscillation Power Range Monitor (OPRM) (Design Phase" provide detailed analysis regarding watchdog timers for PRM and OPRM. Table 3.19-1 is part of the analysis for the LPRM unit.

Table 3.19-1 FMEA for LPRM Unit (Part)

No	Component or Function Description	Failure Mode	Cause	Local Effects Including Dependent Failure	Method of Detection	Inherent Compensating Provisions	Effect on the RPS or the OPRM	Comments

a,c

3.20 Response to Action Item 20

Action Item 20

Describe the watchdog timer Light Emitting Diodes.

Toshiba Response to the Action Item 20

The actions of Light Emitting Diodes (LED) on the module's front panel for watchdog timer timeout are shown in following table.

Module	Watchdog timer for signal processing FPGAs	Watchdog timer for HMI FPGAs
LPRM module	INOP LED on the front panel turns on.	INOP LED on the front panel turns on.
APRM module	INOP LED on the front panel turns on.	FAIL LED on the front panel turns on.
SQ-ROOT module	INOP LED on the front panel turns on.	FAIL LED on the front panel turns on.
FLOW module	INOP LED on the front panel turns on.	FAIL LED on the front panel turns on.
STATUS module	FAIL LED on the front panel turns on.	
TRN module	LINE STATUS LED on the front panel turns off.	
RCV module	LINE STATUS LED on the front panel turns off.	
CELL module	INOP LED on the front panel turns on.	FAIL LED on the front panel turns on.
AGRD module	INOP LED on the front panel turns on.	FAIL LED on the front panel turns on.
PBD module	INOP LED on the front panel turns on.	FAIL LED on the front panel turns on.
DAT/ST module	FAIL LED on the front panel turns on.	

3.21 Response to Action Item 21

Action Item 21

Provide communication diagnostics for the modules discussed on slide 61 (proprietary) of the presentation.

Toshiba Response to the Action Item 21

See response for Section 3.22, Action Item 22.

3.22 Response to Action Item 22

Action Item 22

Correct the last bullet on slide 61 before submitting to NRC.

Toshiba Response to the Action Item 22

Error on the last bullet on slide subtitled "c. Communication Diagnosis (Fiber Optic Link)" (actually slide 60) has been corrected in the "Toshiba Field Programmable Gate Array (FPGA) Based Safety Related I&C Platform", IM-2014-001298 Rev.0 (Reference (1)) and submitted to the U.S NRC by the letter "Proprietary Handouts used at January 28, 2015 Meeting", TOS-CR-FPG-2015-0001 (Reference (3)).

3.23 Response to Action Item 23

Action Item 23

Grant access to the Sharepoint site to additional NRC staff.

Toshiba Response to the Action Item 23

Access granted to Mr. Jack Zhao for the Sharepoint (Toshiba Document Portal (TDP)) on the end of January 2015.

3.24 Response to Action Item #24

Action Item 24

Identify several potential weeks for conducting the regulatory audit.

Toshiba Response to the Action Item 24

This item should be discussed after the schedule for RAIs is determined.

Attachment-1

Explanation for Appendix A of PRM PTER (FPG-DRT-C51-0001) Rev.10

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
			ERS/PQAM Requirement to be confirmed by											
EPRI TR-107330 CTM ITEM NO.	Document	SECTION of ERS or PQAM	Procurement of the CG Items	Procurement of the CG Services	Qualification Analyses	Qualification Tests	Software Qualification	Post-Qualification Activities	Remarks on selection of Methods for Ensuring ERS/PQAM requirements are satisfied	CCDs for CGI	CCAs for CGI	Applicable Method to Confirm Critical Characteristics (Acceptance Method and/or Qualification Test)	Required Frequency for Applying Acceptance Method	Explanation how to develop this Appendix A
	E05R-001-R0	Observation No.5 of CG Survey Report	X	—	—	—	—	—	Procurement of the CGI provides reasonable assurance that the requirements is satisfied.	X	Verification of design tool	Acceptance Method	Recuring	In column B and C, the observation No.5 from the CG Servey Report (E05R-001-R0) is identified as Critical Characteristics (CCs) to be confirmed. Requirements from the observation No.5 is as follows: "NICSD shall perform verificatio such as in-use-test for design tool. Moreover, when NICSD received notification of errors from tool vendor, NICSD shall implement evaluation of impact reviews/verification." Column D to H show how to confirm the CCs. As shown in column D, Toshiba determined that NED's evaluation of NICSD as part of the "Procurement of the CG Items" provides reasonable assurance to the CCs In column L, Verification of design tool is identified as Critical Characteristics for Acceptance (CCA) for CG Items. For verification of design tool, assessment of software tools was conducted in the V&V activities and described in the Implementation and Integration Phase V&V Report (FPG-DRT-C51-0014 Rev.0 Section 3.5 (Attachment-4 of UTLR-0020P Part V Rev.1)).
4.2.1.A 4.3.4.1 4.3.4.3.F	ERS	5.1.3.1 Response Time Requirements	X	—	—	X	—	—	Qualification testing provides reasonable assurance that the total system response time requirement (from the ERS) is satisfied. CGI procurement acceptance includes activity to reasonably assure that all other ERS response time requirements (except total system response time) are satisfied.	X	Unit Model Numbers Configuration Identifications of Units Quality of Design and Manufacture Total system response time for trip signal	Acceptance Method Qualification Test	Recurring (Acceptance Method) at Qualification Test (Qualification Test)	In column B and C, the response time requirements described in the ERS Section 5.1.3.1 are identified as Critical Characteristics (CCs) to be confirmed. In column A, sections of EPRI TR-107330 that could be related to the requirements described in the ERS Section 5.1.3.1 are listed. Column D to H show how to confirm the CCs. As shown in column D and G, Toshiba determined that NED's evaluation of NICSD as part of the"Procurement of the CG Items", and "Qualification Test" provide reasonable assurance to the CCs. In column L, "Unit Model Numbers", "Cofigurations of Units", "Quality of Design and Manufacture", and "Total system response time for trip signal" are identified as Critical Characteristics for Acceptance (CCA) for CG Items. An acceptance plan was prepared as separate documents. The acceptance plan identifies acceptance method to the CCA identified in column L of this Appendix A. Followings are identified in the Acceptance Plan for Test Specimen Units, Interconnecting Cables (FPG-PLN-C51-0008 Rev.1). -Source verification (Method 3) is identified as acceptance method for "Unit Model Numbers" and "Configuration Identifications of Units". -Commercial Grade Survey (Method 2) is identified as acceptance method for "Quality of Design and Manufacture" "Total system response time for trip signal" was confirmed during the qualification test.
4.2.3.6 4.2.3.7.A 4.3.4.7.B 4.3.4.7.C 4.4.1.2.G 4.4.6.1 4.4.6.1.1 4.4.6.1.5 4.4.6.1.8 4.4.6.1.9 4.4.6.1.10 4.4.6.1.11 4.4.6.1.12 4.4.6.1.13 4.4.6.1.14 4.5.6.E	ERS	5.1.6 Failure Detection and Self Test Requirements	X	—	—	X	—	—	CGI procurement acceptance includes activity to reasonably assure that this performance/design requirement is satisfied. Qualification Testing provides reasonable assurance that the requirements are met.	X	Unit Model Numbers Configuration Identifications of Units Quality of Design and Manufacture Fault condition signal generated during faults	Acceptance Method Qualification Test	Recurring (Acceptance Method) at Qualification Test (Qualification Test)	In column B and C, the failure detection and self test requirements described in the ERS Section 5.1.6 are identified as Critical Characteristics (CCs) to be confirmed. In column A, sections of EPRI TR-107330 that could be related to the requirements described in the ERS Section 5.1.6 are listed. Column D to H show how to confirm the CCs. As shown in column D and G, Toshiba determined that NED's evaluation of NICSD as part of the "Procurement of the CG Items", and "Qualification Test" provide reasonable assurance to the CCs. In column L, "Unit Model Numbers", "Cofigurations of Units", "Quality of Design and Manufacture", and "Fault condition signal generated during faults" are identified as Critical Characteristics for Acceptance (CCA) for CG Items. An acceptance plan was prepared as separate document. The acceptance plan identifies acceptance method to the CCA identified in column L of this Appendix A. Followings are identified in the Acceptance Plan for Test Specimen Units, Interconnecting Cables (FPG-PLN-C51-0008 Rev.1) -Source verification (Method 3) is identified as acceptance method for "Unit Model Numbers", "Configuration Identifications of Units", and "Self Test Functions and Surveillance Testing Capability for Modules". -Commercial Grade Survey (Method 2) is identified as acceptance method for "Quality of Design and Manufacture". The failure detection and self test functions were also confirmed during the qualification test.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
			ERS/PQAM Requirement to be confirmed by											
EPRI TR-107330 CTM ITEM NO.	Document	SECTION of ERS or PQAM	Procurement of the CG Items	Procurement of the CG Services	Qualification Analyses	Qualification Tests	Software Qualification	Post-Qualification Activities	Remarks on selection of Methods for Ensuring ERS/PQAM requirements are satisfied	CCDs for CGI	CCAs for CGI	Applicable Method to Confirm Critical Characteristics (Acceptance Method and/or Qualification Test)	Required Frequency for Applying Acceptance Method	Explanation how to develop this Appendix A
4.2.3.2 4.2.3.3 4.2.3.4 4.2.3.5 6.4.1	ERS	5.1.7 Availability/Reliability Requirements	X	–	X	–	–	–	CGI procurement acceptance includes activity to reasonably assure that the MTBF requirement is satisfied. Qualification analysis will address the availability/reliability analysis requirement (from the EPRI TR).	X	Unit Model Numbers Quality of Design and Manufacture	Acceptance Method	Recurring	In column B and C, the availability/reliability requirements described in the ERS Section 5.1.7 are identified as Critical Characteristics (CCs) to be confirmed. In column A, sections of EPRI TR-107330 that could be related to the requirements described in the ERS Section 5.1.7 are listed. Column D to H show how to confirm the CCs. As shown in column D and F, Toshiba determined that NED's evaluation of NICSD as part of the"Procurement of the CG Items", and "Qualification Analysis" provide reasonable assurance to the CCs. In column L, "Unit Model Numbers" and "Quality of Design and Manufacture" are identified as Critical Characteristics for Acceptance (CCA) for CG Items. An acceptance plan was prepared as separate document. The acceptance plan identifies acceptance method to the CCA identified in column L of this Appendix A. Followings are identified in the Acceptance Plan for Test Specimen Units. Interconnecting Cables (FPG-PLN-C51-0008 Rev.1) -Source verification (Method 3) is identified as acceptance method for "Unit Model Numbers". -Commercial Grade Survey (Method 2) is identified as acceptance method for "Quality of Design and Manufacture" The availability/reliability requirement described in the ERS Section 5.1.7 was confirmed through the availability/reliability analysis.
4.2.2 4.4.5.2.E 7.2.G 7.4 7.5.2 7.5.3 7.7.3 8.7.E	ERS	5.3 Software Requirements	X	–	–	–	X	–	Software qualification by NED provides reasanable assurance that the requirement is satisfied. Procurement of the CGI provides reasonable assurance that the requirements is satisfied., including providing necessary V&V information from vendor.	X	Quality of Design and Manufacture Documentation that work is performed in accordance with a program that has: – Lifecycle V&V requirements (documents such as FE specs, FPGA design specs, Implementation records, testing records, etc.) – Traceability Requirements (of the boards, etc.) – Document and Coding Control Requirements – Configuration Control requirements – Change Control Requirements – Design Language and Tool Control Requirements – Labelling requirements for logic revision number on chips Design Requirements – Synchronous design – Modular design using completely tested FEs – Lengths of train of the FEs FPGA model number (for size, non-rewritable, retention capability)	Acceptance Method	Recurring	In column B and C, the software requirements described in the ERS Section 5.3 are identified as Critical Characteristics (CCs) to be confirmed. In column A, sections of EPRI TR-107330 that could be related to the requirements described in the ERS Section 5.3 are listed. Column D to H show how to confirm the CCs. As identified in column D and H, Toshiba determined that NED's evaluation of NICSD as part of the "Procurement of the CG Items", and "Software Qualification" provide reasonable assurance to the CCs. In column L, "Quality of Design and Manufacture" is identified as Critical Characteristics for Acceptance (CCA) for CG Items. An acceptance plan was prepared as separate document. The acceptance plan identifies acceptance method to the CCA identified in column L of this Appendix A. Commercial Grade Survey (Method 2) is identified as acceptance method for "Quality of Design and Manufacture" in the Acceptance Plan for Test Speciment Units, Interconnecting Cables (FPG-PLN-C51-0008 Rev.1). The software requirements described in ERS section 5.3 was confirmed through the V&V activities.
6.2.3	ERS	7.3.1.3 Test Support Equipment Requirements	–	X	–	X	–	–	Procurement for CG services provides reasonable assurance that the requirements are met. Control of test equipment is part of the qualification testing scope.	–	–	Acceptance Method Qualification Test	Recurring (Acceptance Method) at Qualification Test (Qualification Test)	In column B and C, the test support equipment requirements described in ERS Section 7.3.1.3 are identified as Critical Characteristics (CCs) to be confirmed. In column A, section of EPRI TR-107330 that could be related to the requirements described in ERS Section 7.3.1.3 is listed. Column D to H shows how to confirm the CCs. As shown in column E and G, Toshiba determined that NED's evaluation of NICSD as part of the "Procurement of the CG Services", and "Qualification Test" provide reasonable assurance to the CCs. In Section 4.3.3 and 4.3.4 of mainbody of the PTER, Critical Characteristics for Acceptance (CCA) of the CG Services are described. For example, type of relay applied to the trip auxiliary unit as test equipment is provided as Critical Characteristics for Acceptance (CCA) in Section 4.3.4.1 of mainbody of the PTER. An acceptance plan was prepared as separate document. The acceptance plan identifies acceptance method to the CCA identified in Section 4.3.3. and 4.3.4 of mainbody of the PTER. For example, in the Acceptance Plan for Test Support Services (FPG-PLN-C51-0010 Rev.5), Source Verification (Method 3) is identified as acceptance method for the type of relay described in Section 4.3.4.1 of mainbody of the PTER. The test support equipment requirements described in ERS 7.3.1.3 was also confirmed during the qualifation test.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
			ERS/PQAM Requirement to be confirmed by											
EPRI TR-107330 CTM ITEM NO.	Document	SECTION of ERS or PQAM	Procurement of the CG Items	Procurement of the CG Services	Qualification Analyses	Qualification Tests	Software Qualification	Post-Qualification Activities	Remarks on selection of Methods for Ensuring ERS/PQAM requirements are satisfied	CCDs for CGI	CCAs for CGI	Applicable Method to Confirm Critical Characteristics (Acceptance Method and/or Qualification Test)	Required Frequency for Applying Acceptance Method	Explanation how to develop this Appendix A
7.2.F	PQAM	6.4 Critical Digital Review	—	—	—	—	X	—	Software qualification by NED provides reasonable assurance that the requirement is satisfied	—	—	Acceptance Method	Recurring	In column B and C, the requirements for critical digital review described in the Project Quality Assurance Manual (PQAM) (FPG-PLN-A70-0001) Section 6.4 are identified as Critical Characteristics (CCs) to be confirmed. In column A, section of EPRI TR-107330 that could be related to the requirements described in the PTER Section 6.4 is listed. Column D to H show how to confirm the CCs. As shown in column H, Toshiba determined that "Software Qualification" provides reasonable assurance to the CCs. This CCs were confirmed by the cirtical digital review of NICSD and Actel.