PSNN-2014-0870

Safety-Related

The use of the information contained in this document by anyone for any purpose other than that for which it is intended is not authorized. In the event the information is used without authorization from TOSHIBA CORPORATION, TOSHIBA CORPORATION makes no representation or warranty and assumes no liability as to the completeness, accuracy, or usefulness of the information contained in this document.
TOSHIBA CORPORATION
NUCLEAR ENERGY SYSTEMS & SERVICES DIV.

Toshiba Project Document No.	Rev. No.
FA32-3709-1000	7

Project	:NRW-FPGA-Based I&C System :Qualification Project
Contract No.	: ——

X	For Approval		For Information

Action		
A	X	Approved No Further Action
C		Approved with Comment Revised and Resubmit
D		Disapproved Revised and Resubmit
I		Accepted for Information Only □ Recommendation Included

Group Instrumentation & Control System Design & Engineering Dept

Approved by	Reviewed by
M. Tahira May. 23, 2014	T. Hayashi May 23, 2014

Approval by buyer does not release seller of his obligation to furnish all goods and services in strict conformance with all of the terms of the Purchase Order.

TOSHIBA CORPORATION
NED

Document Filing No.	Rev. No.
RS-5159214	6

NRW-FPGA-Based I&C System Qualification Project

Software Verification &Validation Plan

Title: Nuclear Instrumentation & Control Systems Department Verification and Validation Plan for FPGA-based Safety-Related Systems

Customer Name	None
Project Name	NRW-FPGA-Based I&C System Qualification Project
Item Name	None
Item Number	A32
Job Number	9P04482
Applicable Plant	None

TOSHIBA NICSD verified this Document;

Method : Design Review
Verification Report No. : FA32-0904-1015 Rev
Verification Results Acceptable
Verified by H. Kitazono
Group Name NICSD IV&V Team
Date Apr. 24, 2014

Rev.No	Issue Date	Description	Approved by	Reviewed by	Prepared by
7	Apr. 28, 2014	See DECN-FA32-3709-1000-07	A. Naka Apr. 28. 2014	H. Kitazono Apr. 24, 2014	K. Kasai Apr. 23, 2014

Initial Issue Date	Issued by	Approved by	Reviewed by	Prepared by	Document filing No.
Nov. 10, 2011	Nuclear Instrumentation & Control Systems Department	S.Totsuka Nov. 10, 2011	H.Kitazono Nov. 9, 2011	K.Kasai Nov. 9, 2011	5B8K0038

Record of Revisions

Rev No.	Date	Description	Approved by	Reviewed by	Prepared by
0	See Cover Page	Initial Issue	See Cover Page	See Cover Page	See Cover Page
1	Feb.21 ,2012	See DECN-FA32-3709-1000-01	S.Totsuka Feb.21 ,2012	H.Kitazono Feb.21 ,2012	M.Shirasaki Feb.21 ,2012
2	Mar.8 ,2012	See DECN-FA32-3709-1000-02	S.Totsuka Mar.8 ,2012	H.Kitazono Mar.8 ,2012	M.Shirasaki Mar.7 ,2012
3	Jun.26 ,2012	See DECN-FA32-3709-1000-03	S.Totsuka Jun.26 ,2012	H.Kitazono Jun.26 ,2012	K. Kasai Jun.26 ,2012
4	Sep.24 ,2012	See DECN-FA32-3709-1000-04	S.Totsuka Sep.24 ,2012	H.Kitazono Sep.21 ,2012	K. Kasai Sep.21 ,2012
5	Jan.11 ,2013	See DECN-FA32-3709-1000-05	A.Nakai Jan.11 ,2013	H.Kitazono Jan.9 ,2013	K. Kasai Jan.9 ,2013
6	Feb.26 ,2014	See DECN-FA32-3709-1000-05	A.Nakai Feb.26 ,2014	H.Kitazono Feb.19 ,2014	K. Kasai Feb.19 ,2014
7	See Cover Page	See Cover Page	See Cover Page	See Cover Page	See Cover Page

Table of contents

1 Introduction

1.1 Purpose

The Nuclear Instrumentation & Control Systems Department (NICSD) Verification and Validation (V&V) plan (NICSD VVP) is prepared for Non-Rewritable (NRW) Field Programmable Gate Array (FPGA)-based safety-related Instrumentation and Control (I&C) systems based on the Nuclear Energy Systems and Services Division (NED) V&V plan (NED VVP) (Reference (46)) to define the NICSD V&V activities.

The system design is determined by the Instrumentation & Control Systems Design and Engineering Department (ICDD) of Nuclear Energy Systems and Services Division (NED), and ICDD procures the FPGA-based equipment from Toshiba Fuchu Complex Power Systems Segment (Fuchu-PS) NICSD. NICSD procures major FPGA-based components, including modules with FPGA logic from the Toshiba Fuchu-PS Power Platform Development Department (PPDD) using a commercial grade dedication process.

For V&V of the FPGA-based safety-related I&C systems, ICDD and NICSD organize independent V&V (IV&V) Teams. The ICDD and NICSD IV&V Teams work together.

The software lifecycle process, including V&V, is defined in the project document "NICSD Software Management Plan for FPGA-based Safety-Related Systems" (NICSD SMP) (Reference (47)). This NICSD VVP covers the Section 4 "Software Verification and Validation Program Plan" of the project document "Software Program Plan" (SPP) (Reference (44)). This NICSD VVP is prepared by the NICSD IV&V Team in accordance with the following reference documents:

- NED, FA10-3709-0001 "Nuclear Energy Systems and Services Division FPGA-based Safety-Related Systems Verification and Validation Plan " (Reference (46))
- NED AS-200A130 "Digital System Verification & Validation Procedure" (Reference (12)), and
- NICSD NQ-2013 "Preparation Guide for V&V Plan" (Reference (17))

1.2 Scope

This NICSD VVP applies to the V&V activities for the FPGA-based safety-related I&C systems, which Toshiba will supply to US Nuclear Power Plants.

Section 4 of the project document "Software Program Plan," (SPP) (Reference (44)) establishes requirements and provides guidance and expectations for the V&V activities. This NICSD VVP complies with Section 4 of the SPP for the NICSD portions of the V&V activities. Table A shows compliance to Section 4 of the SPP.

2 Definitions and Abbreviations

2.1 Definitions

Functional Element (FE): A Functional Element is a component of digital logic that is completely verified and validated through full pattern testing, i.e. tests that are performed for all possible input combinations. An FE is written in Very High Speed Integrated Circuit Hardware Description Language (VHDL). All VHDL source codes for the NRW-FPGA-based System solely consist of FEs and interconnect between FEs.

Module: A part of a unit. Each module consists of one or more printed circuit boards, on which the FPGAs and other circuitry are mounted, and a front panel.

Netlist: Description of logics created by the logic synthesis tool. A design engineer describes FPGA logic in the form of VHDL source codes and FEs. The logic synthesis tool converts the VHDL source code into forms of digital circuits and outputs the resulting circuit in the form of a netlist. The layout tool transforms the netlist into physical placement of interconnects on the FPGA, which are represented as an FPGA fuse-map.

Unit: A major component of FPGA-based equipment. A unit is a chassis that has front slots and back slots to mount modules. Each unit consists of several modules. There is a vertical middle plane between the front and back slots in each unit. This plane consists of two circuit boards. These circuit boards provide backplanes for the front and rear modules. Modules plug into the backplanes using connectors. Once a module is plugged into the appropriate connector, it exchanges data with other modules in the unit, connects to other units and any external field equipment, and is powered.

Validation: Validation is used to ensure that the final product satisfies the user requirements. Validation shall be performed on the final product, although validation may be necessary or performed prior to the final code being produced. See Section 4.2 of the SPP (Reference (44)).

Verification: Verification consists of reviews performed on the results of each development phase to ensure the phase was completed appropriately and correctly. See Section 4.2 of the SPP (Reference (44)).

2.2 Abbreviations

BRR	Baseline Review Report
CAR	Corrective Action Request
CDR	Critical Digital Review
CFR	Code of Federal Regulation
CM	Configuration Management
CG	Commercial Grade
COTS	Commercial-Off-The-Shelf
DVR	Design Verification Report
ECWD	Elementary Control Wiring Diagram
EDIF	Electronic Design Interchange Format
EDS	Equipment Design Specification

ES	Engineering Schedule
FE	Functional Element
FPGA	Field Programmable Gate Array (a programmable logic device)
Fuchu-PS	Toshiba Fuchu Complex Power Systems Segment
I&C	Instrumentation and Control
IBD	Interlock Block Diagram
ICDD	Instrumentation & Control Systems Design and Engineering Department
IDE	Integrated Development Environment
IED	Instrumentation Electrical Diagram
IEEE	Institute of Electrical and Electronics Engineers
IR	Independent Reviewer
IV&V	Independent Verification and Validation
MCL	Master Configuration List
NED	Nuclear Energy Systems and Services Division
NICSD	Nuclear Instrumentation & Control Systems Department
NISD	Nuclear Instrumentation Systems Development & Designing Group
NICS-QA	Quality Assurance Group for Nuclear Instrumentation & Control Systems
NNR	Nonconformance Notice Report
NQ	Nuclear Quality (standards for NICSD)
PC	Personal Computer
PCDL	Project Control Document List
PDS	Previously Developed Software
PM	Project Manager
PPDD	Power Platform Development Department
PRM	Process Review Meeting
PRS	Problem Reporting Sheet
PSNE	Toshiba Corporation, Power Systems & Services Company, Nuclear Energy
QA	Quality Assurance
QAD	Quality Assurance Department
QC	Quality Control
RG	Regulatory Guide
RTIS	Reactor Trip and Isolation System
RTM	Requirements Traceability Matrix
SSAR	Software Safety Analysis Report
SCAR	Fuchu Site Corrective Action Request

SCMP	Software Quality Configuration Management Plan
SCSI	Small Computer System Interface
SD	Software Development
SDD	Software Design Description
SDL	Software Development Lead
SDOE	Secure Development and Operational Environment
SIL	Software Integrity Level
SM	Senior Manager
SMP	Software Management Plan
SQA	Software Quality Assurance
SQAP	Software Quality Assurance Management Plan
SRS	Software Requirements Specification
SPP	Software Program Plan
SVTP	Software Validation Test Plan
SVTR	Software Validation Test Report
V&V	Verification and Validation
VHDL	Very High Speed Integrated Circuit Hardware Definition Language (A hardware description language that defines the FPGA circuit)
VNNR	Vendor Nonconformance Notice Report
VVP	Verification and Validation Plan
VVR	Verification and Validation Report

Table 3-1 of the NICSD SMP is provided for a better understanding of terminological difference between the SPP and NICSD SMP. This NICSD VVP also uses Table 3-1 of the NICSD SMP.

3 Reference Documents

3.1 Code of Federal Regulations

This NICSD VVP does not refer to the Code of Federal Regulations (CFR) directly. The Toshiba internal standards in Section 3.4 are based on the CFR.

3.2 Regulatory Guides and NRC Documents

(1) Regulatory Guide 1.168
"Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." Rev.1, 2004

(2) Regulatory Guide 1.152
"Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Rev.3, July 2011

Other regulatory guides may be referred to indirectly through the Toshiba internal standards in Section 3.4.

3.3 Industry Standards

(3) IEEE Std. 1012-1998
"IEEE Standard for Software Verification and Validation"

(4) IEEE Std. 1028-1997
"IEEE Standard for Software Reviews"

3.4 Toshiba Internal Standards (NED, NICSD)

(5) Toshiba Nuclear Energy Systems and Services Division AS-100A004
"Document Control Procedure"

(6) Toshiba Nuclear Energy Systems and Service Division AS-100A012
"Preparation Procedure for Engineering Communication Sheet"

(7) Toshiba Nuclear Energy Systems and Service Division AS-200A002
"Design Verification Procedure"

(8) Toshiba Nuclear Energy Systems and Services Division AS-200A010
"Control Procedure of vendor generated documents"

(9) Toshiba Nuclear Energy Systems and Service Division AS-200A017
"Design Planning Procedure"

(10) Toshiba Nuclear Energy Systems and Service Division AS-200A128
"Digital System Life Cycle Procedure"

(11) Toshiba Nuclear Energy Systems and Service Division AS-200A129
"Digital System Development Procedure"

(12) Toshiba Nuclear Energy Systems and Service Division AS-200A130
"Digital System Verification & Validation Procedure"

(13) Toshiba Nuclear Energy Systems and Service Division AS-200A131
"Digital System Configuration Management Procedure"

(14) Toshiba Nuclear Energy Systems and Service Division AS-300A008
"Nonconformance Control and Corrective Action Procedure"

(15) Toshiba Nuclear Energy Systems and Services Division AS-300A009 "Corrective Action Request Application Procedure"

(16) Toshiba Nuclear Instrumentation & Control Systems Department NQ-2011 "Procedure for FPGA Test"

(17) Toshiba Nuclear Instrumentation & Control Systems Department NQ-2013 "Preparation Guide for V&V Plan"

(18) Toshiba Nuclear Instrumentation & Control Systems Department NQ-2014 "Preparation Guide for V&V Report"

(19) Toshiba Nuclear Instrumentation & Control Systems Department NQ-2015 "Preparation Procedure for RTM & RTM Report"

(20) Toshiba Nuclear Instrumentation & Control Systems Department NQ-2019 "Preparation Procedure for Test Specification"

(21) Toshiba Nuclear Instrumentation & Control Systems Department NQ-2024 "Procedure for Document Control"

(22) Toshiba Nuclear Instrumentation & Control Systems Department NQ-2030 "Procedural Standard for FPGA Products Development"

(23) Toshiba Nuclear Instrumentation & Control Systems Department NQ-2031 "Procedural Standard for FPGA Device Development"

(24) Toshiba Nuclear Instrumentation & Control Systems Department NQ-2032 "Procedural Standard for Functional Element Development"

(25) Toshiba Nuclear Instrumentation & Control Systems Department NQ-2033 "Procedural Standard for FPGA Configuration Management"

(26) Toshiba Nuclear Instrumentation & Control Systems Department NQ-2003 "Procedure for Control of Software Tools"

(27) Toshiba Nuclear Instrumentation & Control Systems Department NQ-2036 "Procedure for Design Control"

(28) Toshiba Nuclear Instrumentation & Control Systems Department NQ-2037 "Cyber Security Procedures of Safety Related Digital System"

(29) Toshiba Nuclear Instrumentation & Control Systems Department NQ-3005 "Procedure for Evaluation of Suppliers"

(30) Toshiba Nuclear Instrumentation & Control Systems Department NQ-3006 "Procedure for Control of Nonconforming Procurement Items and Services"

(31) Toshiba Nuclear Instrumentation & Control Systems Department NQ-3015 "Test Control Procedure"

(32) Toshiba Nuclear Instrumentation & Control Systems Department NQ-3016 "Software Test"

(33) Toshiba Nuclear Instrumentation & Control Systems Department NQ-3019 "Procedure for Control of Nonconformance and Corrective Action"

(34) Toshiba Nuclear Instrumentation & Control Systems Department NQ-3020 "Control Procedure of QA Records"

(35) Toshiba Nuclear Instrumentation & Control Systems Department NQ-4001
"Commercial Grade Dedication"

3.5 Toshiba Internal Standards (PPDD)

(36) Toshiba Power Platform Development Department E-67019
" PPDD Procedure for Operation for Problem Reporting Sheet"

(37) Toshiba Power Platform Development Department E-68016
"PPDD Procedural Standard for FPGA Products Development"

(38) Toshiba Power Platform Development Department E-68017
"PPDD Procedural Standard for FPGA Device Development"

(39) Toshiba Power Platform Development Department E-68018
"PPDD Procedural Standard for Functional Element Development"

(40) Toshiba Power Platform Development Department E-68019
"PPDD Procedural Standard for FPGA Configuration Management"

(41) Toshiba Power Platform Development Department E-68020
"PPDD Procedural Standard for Control of Software Tools for FPGA-based Systems"

(42) Toshiba Power Platform Development Department E-68027
"Standard for Preparation of the Test Specification"

Notice: Upon application of above NED, NICSD and other Toshiba internal standards, the latest version shall be used.

3.6 Project Documents

(43)NRW-FPGA-Based I&C System Qualification Project, FA10-0301-0001
"Project Specific Document Control Procedure," Rev. 0

(44)NRW-FPGA-Based I&C\System Qualification Project, FA10-0501-0024
"Software Program Plan," Rev. 1

(45)NRW-FPGA-Based I&C System Qualification Project, FA32-3702-0005
"Nuclear Energy Systems and Services Division FPGA-based Safety-Related Systems Software Management Plan," Rev. 2

(46)NRW-FPGA-Based I&C System Qualification Project, FA32-3709-0001
"Nuclear Energy Systems and Services Division FPGA-based Safety-Related Systems Verification and Validation Plan," Rev. 3

(47)NRW-FPGA-Based I&C System Qualification Project, FA32-3702-1000
"Nuclear Instrument & Control Systems Department Software Management Plan for FPGA-based Safety-Related Systems," Rev. 2

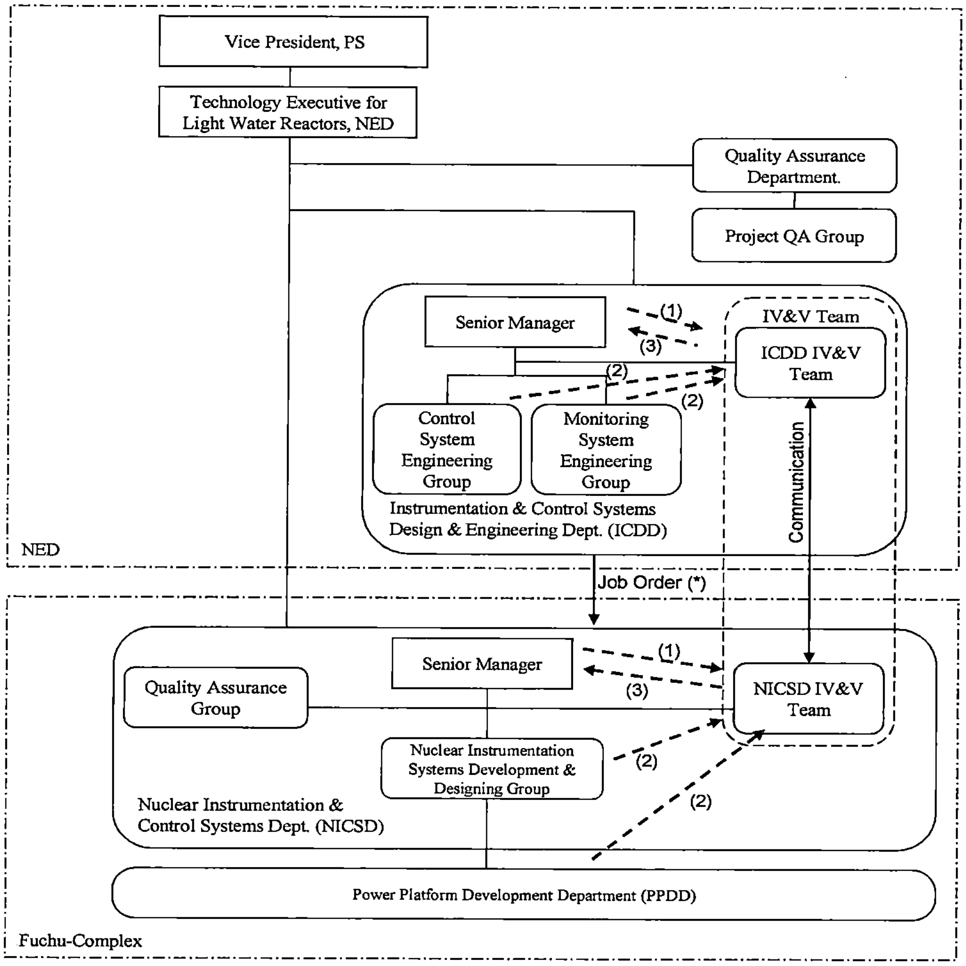
(48) NRW-FPGA-Based I&C System Qualification Project, FA32-3701-1001
"Nuclear Instrument & Control Systems Department Software Quality Assurance Plan for FPGA-Based Safety-Related Systems," Rev. 1

(49) NRW-FPGA-Based I&C System Qualification Project, FA32-3708-1000
"Nuclear Instrument & Control Systems Department Software Configuration Management Plan for FPGA-Based Safety-Related Systems," Rev. 1

4 Verification and Validation Overview

4.1 Organization

Figure 4-1 shows the Toshiba organizations for FPGA-based safety-related I&C systems design and development. Engineers from ICDD and NICSD organize Independent Verification and Validation (IV&V) Teams for the V&V of the FPGA logic. The engineers from ICDD and the engineers from NICSD in the IV&V Teams communicate with each other, and work together as one IV&V Team as needed for the quality of the products. In this plan, the word "ICDD IV&V Team" or "NICSD IV&V Team" is used when two IV&V Teams needs to be distinguished. Otherwise, the remark applies to the both IV&V Teams. The NICSD IV&V Team performs the NICSD V&V activities defined in this NICSD VVP. This structure provides the required independence between development activities and V&V activities.


Vice President, PS
Technology Executive for Light Water Reactors, NED
Quality Assurance Department.
Project QA Group
Senior Manager
(1)
(3)
IV&V Team
ICDD IV&V Team
(2)
(2)
Control System Engineering Group
Monitoring System Engineering Group
Communication
Instrumentation & Control Systems Design & Engineering Dept. (ICDD)
NED
Job Order (*)
Senior Manager
(1)
(3)
Quality Assurance Group
NICSD IV&V Team
Nuclear Instrumentation Systems Development & Designing Group
(2)
(2)
Nuclear Instrumentation & Control Systems Dept. (NICSD)
Power Platform Development Department (PPDD)
Fuchu-Complex

*) A Job Order is issued from each group in ICDD to the Nuclear Instrumentation Systems Development & Designing Group.

(1) Oversight of IV&V team
(2) Submittal of Design Documents
(3) Report of V&V Results

Figure 4-1 Toshiba Organizations for FPGA-based FPGA Systems Design and Development

For the FPGA-based safety-related I&C systems, the Nuclear Instrumentation Systems Development & Designing Group (NISD) in NICSD is responsible for the design and development. The NICSD Software Development Team (NICSD SD Team) comprised of NICSD Software Development Lead (NICSD SDL) and NISD design engineers are responsible for software development (i.e. FPGA logic development).

4.2 Master Schedule

The NICSD IV&V activities and milestones are developed and controlled as described in the NICSD SMP (Reference (47))

4.3 Software Integrity Level Scheme

The software integrity level (SIL) scheme shall be determined based on Table A-1 of NED AS-200A129 (Reference (11)), which is substantially equivalent to Appendix B of IEEE Std. 1012 (Reference (3)).

For safety-related FPGA logic, the SIL shall be 4 in accordance with RG 1.168 (Reference (1)). All documents pertaining to safety-related FPGA design are labeled as "US Safety-Related" on the cover sheet, and are considered SIL 4 software documents. All software embedded in the FPGA-based Safety-Related I&C systems shall be developed, verified, and validated as SIL 4, safety-related software.

4.4 Resource Summary

The Senior Manager (SM) of NICSD as the NICSD Project Manager (NICSD PM) shall provide appropriate resources for the V&V activities defined in this NICSD VVP. For human resources, the following conditions shall be met.

All NICSD IV&V Team members shall:

- Be independent of the design activities in management, budget, and resource.
- Be technically qualified for the work performed.

The NICSD IV&V Team members shall be qualified as described in the Section 15.4 of the NICSD SMP (Reference (47)). The Section 15.4 of the NICSD SMP requires that the NICSD IV&V Lead shall determine necessary training related to the following skills, as applicable to the job functions being performed, and require the responsible manager to schedule project specific training as "Project Specific Indoctrination/Training Course."

- Code inspection

- Software tool to be used for V&V

The NICSD IV&V Team members shall be aware of and comply with the requirement for independence from the development organization.

This NICSD VVP includes some special procedural requirements to PPDD. NICSD shall put these requirements in the procurement specification to the PPDD.

4.5 Responsibilities

The SM of NICSD as the NICSD PM shall assign the NICSD IV&V Lead, who leads the V&V activities encompassing the NICSD engineering/design work in accordance with the NICSD SMP (Reference (47)). The NICSD IV&V Lead assigns the other IV&V Team members of NICSD who were trained as described in Section 4.4 of this VVP.

The NICSD IV&V Lead is equivalent to the Software V&V Lead described in the SPP (Reference (44)). In addition to the responsibilities defined in the NICSD SMP, the NICSD IV&V Lead has responsibilities listed in Section 4.2.4 of the SPP (Reference (44)), including review of Secure Development and Operational Environment (SDOE) implementation. SDOE is defined in the SPP and in Regulatory Guide 1.152 (Reference (2)).

The following positions, created as necessary during the project, are administratively assigned to the Software V&V Lead, as necessary. If these positions are not assigned, the Software V&V Lead shall be responsible for the activities listed below:

> Software Test Lead –The Software Test Lead shall be responsible for defining the software and systems test plans, procedures, and cases. Each Software Test Lead shall be responsible for the overseeing the performance of testing and test engineers, working with the NICSD Software Development Lead (SDL) to resolve test anomalies, and setting boundaries and requirements for retest activities.
>
> Baseline Review – The NICSD IV&V Team ensures that activities are properly performed and documented at each phase in the software life cycle. The NICSD IV&V Team is responsible for verifying all work products are completed, placed under configuration control, and records updated to reflect completion of a life cycle phase, reporting to the NICSD Quality Assurance Group. Work products to be subject to baseline review shall be defined in the Software Configuration Management Plan. The NICSD IV&V Team shall prepare a Baseline Review report at the result of baseline review. Section 4.6.3 explains Baseline Review.

NED AS-200A130 (Reference (12)) defines the responsibilities in the V&V activities of both ICDD and NICSD. NQ-2030 (Reference (22)) defines the responsibilities in the NICSD V&V activities of the NICSD engineering and design work.

The Preparer(s) of the NICSD VVP and V&V reports (VVR) shall:

- Be part of the NICSD IV&V Team.
- Not have contributed to the design.
- Be technically qualified for the work performed, and knowledgeable in the technologies and methods used in the design.

The NICSD IV&V Team performs independent reviews of the NICSD and PPDD design documents.

The NICSD IV&V Team may also oversee the work of NICSD and PPDD, to verify that they are working in compliance with applicable internal standards, and to evaluate that their work is technically acceptable for safety-related use.

The NICSD Software Quality Assurance (SQA) Team (NICSD SQA Team) will conduct oversight of the NICSD IV&V Team activities.

4.6 Tools, Techniques, and Methodologies

The NICSD IV&V Team will use several commercial software tools for the V&V activities of the FPGA-based safety-related I&C systems. The NICSD SMP (Reference (47)) describes software tools used for engineering.

4.6.1 Verification and Validation

The NICSD IV&V Team shall review the Requirements Traceability Matrix (RTM) and the Software Safety Analysis Reports (SSAR), Equipment Design Specification (EDS), System Test Procedures, System User's Manuals, Elementary Control Wiring Diagrams (ECWD), Unit Detail Design Specifications, Unit User's Manuals, Module Design Specifications, Module Test Procedures, FPGA Design Specifications, and FPGA Test Procedures. This review may be performed on either the printed or the electronic documents. Toshiba NUPDM will be used for distribution and archives of the documents. And a set of standard business software tool will be used for the review.

Document review is a method of V&V, and shall be performed in accordance with NED AS-200A002 (Reference (7)), AS-200A130 (Reference (12)), and NQ-2036 (Reference (27)). IEEE Std. 1012 (Reference (3)), and IEEE Std. 1028 (Reference (4)) provide guidance for the reviews.

AS-200A002 requires to prepare a Design Verification Report (DVR) including a comment box. Section 4.2 of AS-200A002 describes that when the verifier (the verifier in AS-200A002 is called Independent Reviewer (IR) in this VVP) discovers problems, the verifier shall return the DVR with the comments. If the IR discovers so many problems, or a so complex problem that cannot be described in the limited space of the comment box, the IR may use separate comment sheets.

Document review performed as technical review to confirm that:

a) The document conforms to its upstream requirements

b) The document adheres to regulations, standards, guidelines, plans, and procedures applicable to the project

c) Changes to the document are properly implemented and affect only those system areas identified by the change specification

For planning documents, implementation process documents, and design outputs including SSAR and VVR, document review shall be performed for completeness, consistency, correctness, and verifiability as applicable. Appendix A of the SPP "Terms and Definition" provides definitions for these words.

4.6.2 Requirements Traceability Activities

Requirements Traceability Matrices (RTMs) shall be generated by the NICSD SD Team and PPDD design engineers and reviewed by the IV&V Team to ensure the software has completely, accurately, correctly, and consistently addressed the requirements. The RTM shall provide traceability, verification, and validation of requirements.

4.6.3 Baseline Reviews

The NICSD IV&V Team shall perform Baseline Reviews at the conclusion of each phase in the software life cycle to ensure that the required activities during that phase were completed. The Baseline Review shall confirm that planned products including design documents, test documents, VHDL source codes, netlists, fusemaps, test reports, RTMs, SSARs, and V&V Reports were prepared, that appropriate reviews were performed for these products, and that these products were documented and maintained under configuration management (CM).

The NICSD IV&V Team shall confirm the following:

- The NICSD design activities are performed, and the design outputs are prepared as planned in the NICSD SMP.
- NICSD V&V activities are performed as planned in this NICSD VVP.
- The NICSD design outputs are documented and controlled in accordance with NQ-2036 (Reference (27)).

All software life cycle activities for a given phase shall be completed prior to initiating a baseline review. Each anomaly or nonconformance found in baseline reviews shall be resolved through the software life cycle processes. Each of the baseline reviews shall confirm disposition of design, documentation, review, and any other nonconformance identified during the phase, or shall track any unresolved nonconformance through to resolution if the nonconformance cannot be resolved in that phase.

The NICSD IV&V Team shall document the result of a baseline review in a Baseline Review Report (BRR), and report it to the NICSD SQA Team for review and approve it as QA record. In accordance with Section 4.2.6.6 of the SPP (Reference (44)), the BRR shall:

- Describe the review scope,
- Identify the reviewers,
- Identify the persons contacted during the review,
- Document the outputs and versions reviewed,
- Contain a summary of the review results, and
- Describe recommendations and findings.

4.6.4 FPGA development Tool

The NICSD IV&V Team will use the following FPGA development tools for V&V activities..

1. Designer tool
2. Synplify® tool
3. Netlist Viewer tool
4. ModelSim® tool

These tools are commercial software tools, that PPDD uses for development of FPGA based modules. Section 8.1.2 of the NICSD SMP (Reference (47)) describes the tools as well as methods used to accept use of the tools for FPGA-based safety systems for nuclear power plants.

In addition to the above tools, NICSD uses office productivity tools, database software, or editor tools. These software tools are SIL 1 software, and do not need special control procedure.

4.6.5 Test Equipment

NICSD shall control the software tools as described in the NICSD SMP.

The NICSD IV&V Team will review and approve the PPDD work products associated with FPGA review and test.

The NICSD IV&V Team shall document the result of a software tool in a V&V Report.

NICSD expect that PPDD uses the following test equipment for the module testing at the factory:

- Signal-generating equipment – Signal-generating equipment is used to generate test signal to modules.
- Signal-recording equipment – Signal-recording equipment is used to record response signals from the module.
- Test Personal Computer (PC) – One or more PCs are used to control the signal-generating equipment and the signal-recording equipment. The Test PC records the generated and response signals.

NICSD will use test equipment for the verification and validation activities for the units and the system. The test equipment is similar to that of PPDD. The NICSD IV&V Team will evaluate adequacy of these tools.

Test equipment software is not embedded in any FPGA-based safety-related systems.

4.6.6 Metrics

The NICSD IV&V Team should monitor and track the following metrics through the lifecycle phases described in Section 5 to evaluate the product quality.

- Number of changes applied for the design documents
- Number of open items carried to the next phase
- Number of open items closed in the current phase
- Number of Site Corrective Action Requests (SCARs)
- Number of Site Nonconformance Notice Reports (SNNRs)
- Number of problems found during V&V testing

4.7 Security

NICSD takes appropriate measures to ensure Secure Development and Operational Environment (SDOE) as addressed in the SPP. The requirements for the NICSD SDOE are mapped and described in the NQ-2037 (Reference (28)). The NICSD IV&V Team shall verify that the cyber security requirements described in NQ-2037 are correctly reflected in the software life cycles.

5 Verification and Validation Activities

Table B of this NICSD VVP describes V&V activities assigned to each Software Life Cycle Phases.

The following sub-sections describe the V&V activities for the NICSD scope.

5.1 Management

5.1.1 Management of V&V

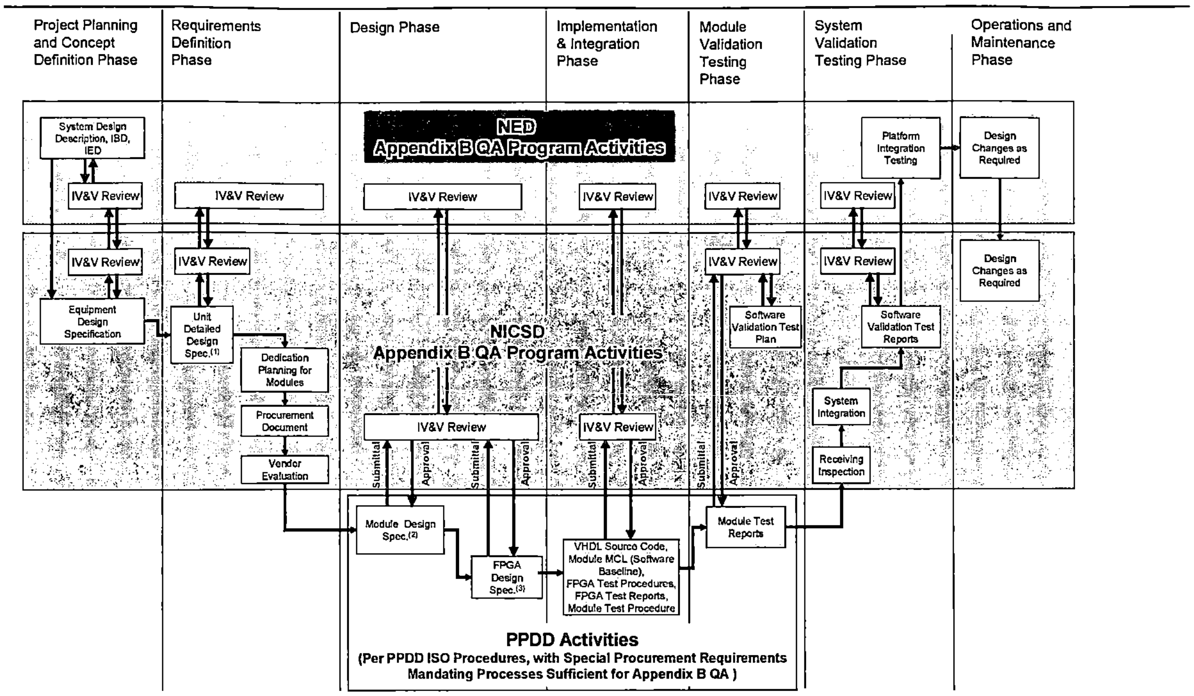
Section 4.3.1 of the SPP (Reference (44)) describes management of the V&V Activities. The management of the V&V process is performed throughout the life cycle phase. Table 10 of the SPP defines the V&V management tasks, which are equivalent to the management tasks defined in IEEE Std. 1012 (Reference (3)). Table 5-1 shows the corresponding activities to the management tasks in this VVP.

Table 5-1 V&V Management Activities

SPP Table 10 Tasks	Activity in this NICSD VVP
1) Software Verification and Validation Plan (SVVP) Update	Establishment of this NICSD VVP
2) Baseline Change Assessment	Activity Iteration Policy in Section 7.2 in this NICSD VVP covers the requirements of the Baseline Change Assessment
3) Management Review	The NICSD PM and NICSD SQA Team oversee the NICSD IV&V Team activities.
4) Management and Technical Review Support	A Process Review Meeting (PRM) is held in every phase to ensure that the required activities during that phase were completed. The NICSD IV&V Team shall attend the PRM for management and technical support.
5) Organizational and Supporting Processes Interface	The NICSD IV&V Team shall attend the PRM. The NICSD IV&V Team shall attend the project management meetings when the NICSD IV&V Lead considers it necessary. The NICSD SQA Team will oversee NICSD IV&V work when the NICSD SQA Lead determines that such oversights are needed.

5.1.2 V&V Phases

Section 13 of the NICSD SMP (Reference (47)) defines the software life cycle for the FPGA-based safety-related I&C systems. Figure 5-1 is the summary drawing illustrating the major activities in the life cycle process for FPGA-based systems.


Project Planning and Concept Definition Phase
Requirements Definition Phase
Design Phase
Implementation & Integration Phase
Module Validation Testing Phase
System Validation Testing Phase
Operations and Maintenance Phase
NED
Appendix B QA Program Activities
System Design Description, ISD, IED
IV&V Review
Platform Integration Testing
Design Changes as Required
Equipment Design Specification
Unit Detailed Design Spec.(1)
Dedication Planning for Modules
Procurement Document
Vendor Evaluation
NICSD
Appendix B QA Program Activities
Software Validation Test Plan
Software Validation Test Reports
System Integration
Receiving Inspection
Submittal
Approval
Module Design Spec.(2)
FPGA Design Spec.(3)
VHDL Source Code, Module MCL (Software Baseline), FPGA Test Procedures, FPGA Test Reports, Module Test Procedure
Module Test Reports
PPDD Activities
(Per PPDD ISO Procedures, with Special Procurement Requirements Mandating Processes Sufficient for Appendix B QA)

(1) Unit Detailed Design Spec. includes Software Requirements Specification.
(2), (3) Module Design Spec. and FPGA Design Spec. include Software Design Description.

Figure 5-1 Life Cycle Process for FPGA-based Systems

The NICSD IV&V Team activities shall be performed for the life cycle phases defined in the NICSD SMP (Reference (47)). This NICSD VVP includes the life cycle phases from the Project Planning and Concept Definition Phase through the System Validation Testing Phase. This NICSD VVP ends after the System Validation Testing, prior to shipment from Japan However, if any need for design change arises after finalizing the V&V activities, this NICSD VVP and the V&V activities shall be reactivated from the earliest phase affected by the change, and necessary activities shall be iterated. For design changes in the Operations and Maintenance phase, another VVP will be prepared.

5.1.3 Use of Previously Developed or Purchased Software

PPDD is a commercial supplier. The FPGA logic lifecycle is treated as the software lifecycle in the NICSD SMP (Reference (47)) and SPP (Reference (44)). The FPGA logic procured from PPDD is included in the FPGA and is commercial. The FPGA logic is treated as Previously Developed Software (PDS). The FPGA logic is comprised of combinations and connections of software elements called functional elements (FEs). The FEs are treated as Commercial-off-the Shelf (COTS) software. NICSD dedicates the FPGA logic implemented in FPGA under NICSD Commercial Grade Dedication (CGD) process defined in the NICSD SMP. NICSD shall evaluate the PPDD before ordering to PPDD through a CG Survey, Critical Digital Review (CDR), or both of them. The NICSD IV&V Team will review and oversee the PPDD in each step of works, and accept those works.

5.2 Project Planning and Concept Definition Phase

The activities in the Project Planning and Concept Definition Phase are performed by ICDD and NICSD. The activities of NICSD in the Project Planning and Concept Definition Phase are described in this section.

During this phase, NICSD generates the Equipment Design Specification (EDS) including the design basis and applicable regulations and industry practices in the design, and starts the master configuration list (MCL). The MCL started in this phase is updated throughout the software life cycle.

Table A of the NICSD SMP (Reference (47)) lists the outline of the output documents of the NICSD V&V activities.

5.2.1 Preparation of NICSD VVP

The NICSD IV&V Team shall prepare this NICSD VVP in accordance with NQ-2013 (Reference (17)), coordinating the plan with the ICDD VVP. The NICSD IV&V Lead shall review this NICSD VVP.

For the procedures to be used for the document review, see Section 4.6.1 in this NICSD VVP.

The NICSD IV&V Team delivers the NICSD VVP to the ICDD IV&V Team for review.

5.2.2 Preparation of Software Test Plan

The NICSD IV&V Team shall prepare a Software Test Plans as described in Section 9 of the SPP (Reference (44)). The NICSD IV&V Team uses the EDS as the base to prepare the Software Test Plan. The scope of tests covered by the Software Test Plan is as follows.

- FPGA Testing
- Module Validation Testing
- System Validation Testing

The Software Test Plan defines the scope, approach, resources, and schedule of the testing activities, and shall require generation of the following documents:

- Software Validation Test Plan (SVTP)
- Test Specification (including Test Design, Test Case)
- Test Procedure
- Test Report

5.2.3 Document Reviews

The NICSD IV&V Team shall perform independent reviews of the documents, which are listed in Table A of the NICSD SMP marked “DVR” in the “Other Outputs” column. For the procedures to be used for the document review, see Section 4.6.1 in this NICSD VVP.

The NICSD IV&V Team reviews the documents for the V&V activities in this phase referring to the methods and procedures described in Table 11 of the SPP. The Table B is provided for a better understanding of terminological difference between the SPP and NICSD VVP.

5.2.4 Project Planning and Concept Definition Phase RTM efforts

(1) Preparation of the RTM

The NICSD SD Team shall update the Project Planning and Concept Definition Phase RTM delivered by ICDD to maintain the traceability between the ICDD requirements and the EDS in accordance with NQ-2015 (Reference (19))

The NICSD SD Team traces the upper level requirements in the NED documents to the EDS, and traces the EDS requirements back to the upper level requirements.

The RTM efforts ensure the following:

- The requirements are traced "forwards" from the upstream documents to the downstream documents.
- The downstream requirements are traced back to the upstream documents.

See Section 8.1 for preparation of RTM.

(2) Compilation of the Project Planning and Concept Definition Phase RTM report

The NICSD SD Team summarizes open items revealed by the RTM efforts. The NICSD SD Team must resolve these items to the satisfaction of the RTM preparer(s).

The NICSD IV&V Team shall review the RTM for work performed by NICSD.

The NICSD IV&V Team shall describe the result of RTM review in the V&V Report for this phase.

5.2.5 Security Review

The NICSD IV&V Team shall review that the cyber security requirements described in NQ-2037 (Reference (28)) and the SPP are correctly reflected in the software life cycles.

The NICSD IV&V Team shall perform independent review (IR) of the EDS and SSARs, and ensure that appropriate cyber security requirements complying with NQ-2037 and the SPP are included in the EDSs and SSARs. In addition, the NICSD IV&V Team shall confirm that an appropriate secure development environment is established. The result of Security Review shall be described in the V&V Report.

5.2.6 Project Planning and Concept Definition Phase V&V Reporting

The NICSD IV&V Team shall prepare the Project Planning and Concept Definition Phase V&V Report summarizing the V&V activities performed for this Project Planning and Concept Definition Phase. This report will be extended at the end of each phase to add the results of each phase report. At the end of the lifecycle, the final report will thus contain the results from all lifecycle phases.

The NICSD V&V Report shall include:

(1) References to the reviewed documents
(2) References to the Design Verification Reports (DVR)
(3) Reference to the Project Planning and Concept Definition Phase RTM (NICSD portion)
(4) Open items revealed in the RTM efforts
(5) Result of the Security Review
(6) Result of the SSAR review
(7) Metrics described in Section 4.6.6
(8) Any findings, recommendations, or suggestions to reduce any risks identified in the V&V activities

The NICSD IV&V Team delivers the NICSD V&V Report to the ICDD IV&V Team for review.

5.2.7 Baseline Review

To complete the Project Planning and Concept Definition Phase, the NICSD IV&V Team shall perform baseline reviews at the phase end as described in Section 4.6.3. The NICSD IV&V Team shall issue a Baseline Review Report (BRR) documenting the results of the Baseline Review and report to the NICSD SQA Team for review and approval as QA record.

5.3 Requirements Definition Phase

The development activities in the Requirements Definition Phase are performed by NICSD. In the Requirements Definition Phase, the NICSD SD Team develops a Unit Detailed Design Specification. This specification addresses software and hardware requirements accomplished by unit design, and provides necessary functional requirements for module design.

Table A of the NICSD SMP (Reference (47)) lists the outline of the output documents of the NICSD V&V activities.

5.3.1 Document Reviews

The NICSD IV&V Team shall perform independent reviews of the documents, which are listed in Table A of the NICSD SMP (Reference (47)), and marked "DVR" in the "Other Outputs" column. For the procedures to be used for the document review, see Section 4.6.1 in this NICSD VVP.

The NICSD IV&V Team reviews the documents for the V&V activities in this phase referring to the methods and procedures described in Table 12 of the SPP (Reference (44). The Table B is provided for a better understanding of terminological difference between the SPP and NICSD VVP.

5.3.2 Requirements Definition Phase RTM efforts

(1) Preparation of Requirements Definition Phase RTM

The NICSD SD Team performs the Requirements Definition Phase RTM efforts.

The RTM efforts ensure the following:

- The requirements are traced "forwards" from the Project Planning and Concept Definition Phase to this phase design documents.
- The requirements are traced back from this phase to the Project Planning and Concept Definition Phase. That is, all requirements listed in this phase are covered by the Project Planning and Concept Definition Phase requirements, and no new requirements have been created in this phase.

In this Requirements Definition Phase, some requirements from the Project Planning and Concept Definition Phase are allocated to hardware. These hardware requirements are also traced. In addition, the RTM efforts must address interface requirements among units, and among modules.

(2) Compilation of the Requirements Definition Phase RTM report

The NICSD IV&V Team shall review the RTM.

The NICSD IV&V Team shall describe the result of RTM review in the V&V Report for this phase.

5.3.3 Security Review

The NICSD IV&V Team shall review that the cyber security requirements described in NQ-2037 (Reference (28)) and the SPP (Reference (44) are correctly reflected in the software life cycles.

The NICSD IV&V Team shall perform independent review (IR) of the Unit Detailed Design Specifications and SSARs, and confirm that appropriate cyber security requirements complying with NQ-2037 and the SPP are included in the Unit Detailed Design Specifications. The result of Security Review shall be described in the V&V report.

5.3.4 Requirements Definition Phase V&V Reporting

The NICSD IV&V Team shall prepare the Requirements Definition Phase V&V Report summarizing the V&V activities performed for this Requirements Definition Phase.

The NICSD V&V Report shall include:

(1) Reference to the reviewed documents

(2) Reference to the Design Verification Reports (DVR)

(3) Reference to the Requirements Definition Phase RTM

(4) Open items revealed in the RTM efforts

(5) Results of the Security Review

(6) Results of the SSAR review

(7) Metrics described in Section 4.6.6

(8) Any findings, recommendations, or suggestions to reduce any risks identified in the V&V activities

The NICSD IV&V Team delivers the NICSD V&V Report to the ICDD IV&V Team for review.

5.3.5 Baseline Review

To complete the Requirements Definition Phase, the NICSD IV&V Team shall perform baseline reviews at the phase end as described in Section 4.6.3. The NICSD IV&V Team shall issue a BRR documenting the results of the Baseline Review and report to the NICSD SQA Team for review and approval as QA record.

5.4 Design Phase

NICSD procures the FPGA-based modules from PPDD. In the design phase, PPDD produces the Module Design Specifications and the FPGA Design Specifications, which define the FPGA logic design, in accordance with PPDD procedure E-68017 (Reference (38)). A special characteristic of the Toshiba FPGA-based I&C systems is that FPGA logic consists of the verified and well proven functional elements (FEs) and interconnects between FEs. All FE are generated by PPDD. The V&V activities for FEs are described separately in Section 5.8

Table A of the NICSD SMP (Reference (47)) lists the outline of the output documents of these V&V activities.

5.4.1 Preparation of SVTP

The NICSD IV&V Team shall initiate preparation of a Software Validation Test Plan (SVTP) in accordance with this NICSD VVP and in Section 9 of the SPP (Reference (44)). The SVTP shall outline the methodology of how various tests will be used to validate that the integrated software meets the requirements stated in the EDS and the Unit Detailed Design Specification.

The SVTP can include a plan for Platform Factory Test (PFT), if necessary.

This activity shall be initiated in this phase to ensure completion prior to the System Validation Testing Phase.

5.4.2 Document Reviews

During this phase, the NICSD IV&V Team is involved in reviewing each PPDD work product. The NICSD IV&V Team ensures the quality and completeness of each work product and its readiness for CGD.

The NICSD IV&V Team shall perform independent reviews of the documents, which are listed in Table A of the NICSD SMP (Reference (47)), and marked "DVR" in the "Other Outputs" column. For the procedures to be used for the document review, see Section 4.6.1 in this NICSD VVP.

The NICSD IV&V Team reviews the documents for the V&V activities in this phase referring to the methods and procedures described in Table 13 of the SPP. The Table B is provided for a better understanding of terminological difference between the SPP and NICSD VVP.

The NICSD IV&V Team shall review design and test documents submitted by PPDD. PPDD use PPDD standard E-68017 (Reference (38)) that has equivalent requirements for FPGA design, coding and testing specified in NICSD Standard NQ-2031 (Reference (23)).

The NICSD IV&V Team shall confirm that the FPGA logic is designed adhering to the design rules given in the NICSD Standard NQ-2031, Appendix A, as well as confirming that guidance provided by the FPGA vendor, Microsemi Corporation, in Application Notes for the chosen FPGA integrated circuit is appropriately incorporated in the design. In particular, the FPGA logic consists of the verified and well proven FEs, and the interface to each FE is consistent with the FE specification. The NICSD IV&V Team shall review and approve the results of the PPDD review.

The NICSD IV&V Team shall check that the FE documents are appropriately maintained as described in Section 5.8.

The NICSD IV&V Team shall confirm that the requirements in PPDD Standard E-68017 are equivalent to the requirements in NICSD Standard NQ-2031 through the CG Survey report or CDR report, or other means.

5.4.3 Design Phase RTM efforts

(1) Preparation of Design Phase RTM

The PPDD design engineers prepare the RTM to maintain the traceability from the unit design to the module design and to the FPGA. The RTM efforts ensure the following:

- The requirements are traced "forwards" from the Requirements Definition Phase to this phase design documents. That is, all requirements in the unit design are allocated to modules mounted in the unit, and requirements in each module design are allocated to FPGAs included in the module.

- The requirements are traced back from this phase to the Requirements Definition Phase. That is, all requirements listed in this phase are covered by the Requirements Definition Phase, and no new requirements have been created in this phase.
  Note: An FPGA design may include maintenance or test purpose circuits. Inclusion of these kinds of circuits must be described in the Module Design Specification as exceptions. The NICSD IV&V Team shall confirm that these circuits do not cause any adverse effects to the module functions.

(2) Compilation of the Design Phase RTM report

The NICSD IV&V Team shall review the RTM prepared by PPDD.

The NICSD SD Team shall update the RTM of the Requirements Definition Phase based on the RTM prepared by PPDD.

The NICSD IV&V Team shall describe the result of RTM review in the V&V Report for this phase.

5.4.4 Security Review

The NICSD IV&V Team shall verify that the cyber security requirements described in NQ-2037 (Reference (28)) and the SPP (Reference (44)) are correctly reflected in the software life cycles.

The NICSD IV&V Team shall perform independent review (IR) of the Module Design Specifications, FPGA Design Specifications and SSARs, and confirm that appropriate cyber security requirements complying with NQ-2037 and the SPP are included in the Module Design Specifications and FPGA Design Specifications. In addition, the NICSD IV&V Team shall confirm that an appropriate secure development environment is established in PPDD. The result of the Security Review shall be described in the V&V Report.

5.4.5 Design Phase V&V Reporting

The NICSD IV&V Team shall prepare the Design Phase V&V Report summarizing the V&V activities performed for this Design Phase.

The NICSD V&V Report shall include:

(1) Reference to the reviewed documents

(2) Reference to the Design Verification Reports (DVR)

(3) Reference to the results of the FE document and the software tool control checks, see Section 5.8

(4) Reference to the Design Phase RTM

(5) Open items revealed in the RTM efforts

(6) Results of the Security Review

(7) Results of the SSAR review

(8) Metrics described in Section 4.6.6

(9) Any findings, recommendations, or suggestions to reduce any risks identified in the

V&V activities

The NICSD IV&V Team delivers the NICSD V&V Report to the ICDD IV&V Team for review.

5.4.6 Baseline Review

To complete the Design Phase, the NICSD IV&V Team shall perform baseline reviews at the phase end as described in Section 4.6.3. The NICSD IV&V Team shall issue a BRR documenting the results of the Baseline Review and report to the NICSD SQA Team for review and approval as QA record.

5.5 Implementation and Integration Phase

In the Implementation and Integration Phase, the FPGAs are developed by PPDD in the following three steps:

Step 1 VHDL Source Coding:

The PPDD design engineers generate VHDL source code that implements the functional requirements written in the FPGA Design Specification in accordance with PPDD procedure E-68017 (Reference (38)). In generating the VHDL source code, the PPDD design engineers use editor tools. Since subsequent activities adequately verify and validate the VHDL source code, no V&V activities are necessary for the editor tools.

Step 2: FPGA Implementation

The PPDD design engineers convert the VHDL source code into netlists using the Synplify® tool, a logic synthesizer. Netlists of FEs used in the design are taken from the PPDD FE library, and integrated into a single netlist by the Designer tool supplied by Microsemi.

To detect errors in the netlists, which may be undetected by the software tools, and errors in the source code, the NICSD IV&V Team confirms logic diagrams from the netlist, and inspects the logic diagrams comparing with the VHDL source code. The logic diagrams are drawn by the Netlist Viewer tool, which is supplied by Microsemi, but is independent of the Synplify® tool.

After the inspection, the PPDD design engineers convert the netlists into a placed, routed netlist, called fuse map, and embeds the fuse map into a test purpose FPGA.

To minimize risks associated with timing, the PPDD design engineers perform timing analysis and simulation during their design process. This two-part process includes static timing analysis and dynamic timing simulation. Static timing analysis evaluates the setup and hold times on each path within the FPGA design. The Designer software tool evaluates the propagation delay to each element in the code in order to determine each timing path in the code. The result from this static analysis can be interpreted by the ModelSim® tool. The PPDD design engineers then use ModelSim® tool to validate the design with dynamic simulation, using accurate propagation delays.

Step 3: FPGA Testing

PPDD performs testing on the FPGAs as defined below. The NICSD IV&V Team reviews the FPGA Test Procedure prepared by PPDD.

This testing includes:

a) Simulation of the fuse map generated in Step 2, and

b) FPGA Testing using the test purpose FPGA produced in Step 2.

The PPDD design engineers perform FPGA Testing using the ModelSim® tool, and the PinPort device. The ModelSim® tool is not only used in simulation, but also in FPGA Testing using an FPGA chip that embeds target FPGA logic for testing. The ModelSim® tool generates inputs to the FPGAs according to the test vectors that are prepared prior to the FPGA Testing.

The PPDD engineers use ModelSim® tool to simulate the internal operation of the logic. The ModelSim® tool provide the PPDD engineer with the capability to watch individual signals within the FPGA and validate that timed FPGA logic works as the engineer intends. These tests verify that the FPGA timing constraints are satisfied, and that additional PPDD timing rules are satisfied. The NICSD IV&V Team shall review FPGA Test Reports describing the result of the FPGA Testing.

After the test is satisfactorily performed using both the simulation software tool and an implementation in an FPGA, the FPGA logic is considered qualified, and registered. Thus the baseline for the registered FPGA logic is established.

The qualified FPGA logic must be implemented in an FPGA integrated circuit prior to being soldered to a module printed circuit board.

All testing results are brought into the NICSD Appendix B program and placed under configuration management at the successful conclusion of testing and acceptance of that testing by NICSD.

Table A of the NICSD SMP (Reference (47)) lists the outline of the outputs of these V&V activities.

The NICSD IV&V Team should observe PPDD activities to verify that PPDD work in accordance with their procedures and NICSD's expectations. These observations could be coordinated with NICSD SQA Team. Results of the observation shall be documented in the V&V Report. If the NICSD IV&V Team finds any nonconformance in PPDD's activities, the NICSD IV&V Team shall issue a SCAR documenting the rejection of the PPDD work product.

5.5.1 VHDL Source Code Reviews

The NICSD IV&V Team shall review the source code to verify correctness, consistency, completeness, accuracy, and traceability to the design specifications in accordance with NQ-2031 (Reference (23)) and Sections 13.4.3 and 14.5.1 of the NICSD SMP (Reference (47)). The results of these reviews must be documented using a Source Code Review Sheet. These verifications must include (at a minimum) review of the FPGA source code written in VHDL (or equivalent configuration information) to ensure that the source code matches what was specified in the FPGA Design Specification (Software Design Description). The reviewer may use software development tools such as a VHDL Simulator in addition to traditional techniques described in IEEE Std 1028 (Reference (4)).

5.5.2 Logic Synthesis and Layout

The PPDD design engineers convert the VHDL source code into a netlist using the Synplify® tool, and convert the netlist into a fuse map using a place and layout tool integrated in the

Designer tool. The PPDD design engineers check the message files from the software tools to confirm that logic synthesis and layout are performed without errors, or problematic warnings. The NICSD IV&V Team verifies the result of the message checks and documents it in the V&V Report.

5.5.3 Signal Timing

The NICSD IV&V Team confirms that the PPDD design engineers meet the FPGA design rules. The NICSD IV&V Team shall verify the timing analysis performed to show that the timing margin described in NQ-2031 (Reference (23)) exists within this FPGA. The NICSD IV&V Team shall evaluate the result of the FPGA internal timing analysis, and document it in the V&V Report.

5.5.4 Netlist Inspection

The NICSD IV&V Team inspects the netlists by comparing the original VHDL files with the logic diagrams generated from the netlists by the Netlist Viewer tool, to verify the correctness of the conversion. In the comparison, the FE interfaces shall be checked, because the VHDL source code implements logic using FEs.

The results of the netlist check shall be documented in the V&V Report.

5.5.5 Document Reviews

The NICSD IV&V Team shall perform independent reviews of the documents, which are listed in Table A of the NICSD SMP (Reference (47)), and marked "DVR" in the "Other Outputs" column. For the procedures to be used for the document review, see Section 4.6.1 in this NICSD VVP.

The NICSD IV&V Team reviews the documents for the V&V activities in this phase referring to the methods and procedures described in Table 14 of the SPP. The Table B is provided for a better understanding of terminological difference between the SPP and the NICSD VVP.

It should be noted that the NICSD IV&V team must confirm that the test cases for FPGA Testing achieve 100% toggle coverage (see NICSD Standard NQ-2011(Reference (16)) for a definition of toggle coverage) of the active FE connections, and the test cases are sufficient to ensure that the FPGA performs its intended functions.

5.5.6 FPGA Testing

PPDD prepares the FPGA Test Procedures in accordance with E-68016 (Reference (37)), including test cases, before the execution of the testing. The NICSD IV&V Team shall review the FPGA Test Procedures in accordance with NQ-2030 (Reference (22)).

FPGA Testing shall be performed in accordance with the FPGA Test Procedure approved by NICSD. The results of the FPGA Testing shall be documented in FPGA Test Reports. The NICSD IV&V Team shall evaluate the FPGA Test Reports.

Any test failures, any product or configuration nonconformances, or any errors in the test procedure itself shall be resolved as described in Section 7.1.

5.5.7 Software Tool Control Review

The NICSD IV&V Team shall review the PPDD control of the software tools used in their design and V&V activities as described in Section 8.1.2 of the NICSD SMP. The NICSD IV&V Team shall review PPDD's records for software tool control to ensure:

- PPDD uses correct versions of software tools for FPGA manufacturing.
- PPDD is controlling the software tools in accordance with procedures that NICSD has reviewed and approved.

5.5.8 Implementation and Integration Phase RTM efforts

(1) Preparation of Implementation and Integration Phase RTM

The PPDD design engineers perform the Implementation and Integration Phase RTM efforts. The RTM efforts ensure that the FPGA Test Procedures cover all logic requirements for FPGAs defined in the FPGA Design Specifications. Note that traceability between FPGA design to VHDL source code is verified in VHDL source code review, and is not included in the RTM efforts.

(2) Compilation of the Implementation and Integration Phase RTM Report

The NICSD IV&V Team shall review the RTM from PPDD.

The NICSD IV&V Team shall describe the result of RTM review in the V&V Report for this phase.

5.5.9 Security Review

The NICSD IV&V Team shall review that the cyber security requirements described in NQ-2037 (Reference (28)) and the SPP (Reference (44)) are correctly reflected in the software life cycles.

The NICSD IV&V Team shall perform an independent review (IR) of the FPGA Test Procedures, FPGA Test Reports. The NICSD IV&V Team shall also review that appropriate cyber security requirements complying with NQ-2037 and the SPP are included in the FPGA Test Procedures.

In addition, the NICSD IV&V Team shall confirm that appropriate security measures are taken in VHDL code generation, code conversion from source code to fuse map, and data storage.

The result of the Security Review shall be described in the V&V Report.

5.5.10 Implementation and Integration Phase V&V Reporting

The NICSD IV&V Team shall prepare the Implementation and Integration Phase V&V Report summarizing the V&V activities performed for this Implementation and Integration Phase. The combination of the Source Code Review Sheet and FPGA Test Report satisfies the requirements for Software Implementation Review Report described in Section 3.12.3.5 of the SPP (Reference (44)).

The NICSD V&V Report shall include:

(1) Reference to the reviewed documents

(2) Reference to the Design Verification Reports (DVR)

(3) Reference to the Source Code Review Sheet

(4) Reference to the software tools message file checks

(5) Reference to the netlist inspections

(6) Reference to the FPGA Test Reports

(7) Reference to the FPGA Control Sheets

(8) Reference to Purchase Specification to PPDD

(9) Reference to the Implementation and Integration Phase RTM

(10) Results of Software Tool Control Review

(11) Open items revealed in the RTM efforts

(12) Results of the Security Review

(13) Results of the SSAR review

(14) Metrics described in Section 4.6.6

(15) Any findings, recommendations, or suggestions to reduce any risks identified in the V&V activities

The NICSD V&V Report includes the Software Build Procedure and Report (SBPR) as defined in the SPP. The following documents are treated as SBPR.

- FPGA Control Sheet
  FPGA Control Sheet shall document the names of the VHDL source code files.

The NICSD IV&V Team delivers the NICSD V&V Report to the ICDD IV&V Team for review.

5.5.11 Baseline Review

To complete the Implementation and Integration Phase, the NICSD IV&V Team shall perform baseline review at the phase end as described in Section 4.6.3. The NICSD IV&V Team shall issue a BRR documenting the results of the Baseline Review and report to NICSD SQA Team for review and approval as QA record.

5.6 Module Validation Testing Phase

Once the module using verified FPGAs has been assembled, PPDD performs module functional testing in accordance with written test procedures. In the Module Validation Testing Phase, PPDD demonstrates that the modules perform all intended functions within the predetermined design, and that the modules do not perform unintended or undesirable functions. PPDD develops Module Test Procedures based on E-68016 (Reference (37)). These test procedures, including test plan, test cases, and acceptance criteria, are written by an engineer other than the engineer who designed the module to be tested.

The PPDD personnel perform module validation testing and generate a Module Test Report which includes a test log and a listing of any testing anomalies. PPDD will resolve test anomalies, by changing the test procedure or changing FPGA logic. If FPGA logic is changed, the V&V activities in Section 5.5 for the FPGA logic shall be iterated. These changes shall be recorded. The test is repeated in its entirety until the test passes successfully. After successful results are obtained, the test report shall be reviewed with change records (if any), approved, and placed under CM.

Table A of the NICSD SMP (Reference (47)) lists the outline of the outputs of these V&V activities.

In addition to the activities described in the following subsections, the NICSD IV&V Team should oversee PPDD activities to verify that PPDD work in accordance with their procedures and NICSD's expectations. Results of observation shall be documented in the V&V Report. If the NICSD IV&V Team finds any nonconformance in a PPDD's activity, the NICSD IV&V Team shall issue a SCAR in accordance with NQ-3019 (Reference (33)).

5.6.1 Document Reviews

The NICSD IV&V Team shall perform independent reviews of the documents, which are listed in Table A of the NICSD SMP (Reference (47)), and marked "DVR" in the "Other Outputs" column. For the procedures to be used for the document review, see Section 4.6.1 in this NICSD VVP.

The NICSD IV&V Team reviews the documents for the V&V activities in this phase referring to the methods and procedures described in Table 15 of the SPP (Reference (44)). The Table B is provided for a better understanding of terminological difference between the SPP and NICSD VVP.

5.6.2 Module Validation Testing

PPDD prepares Module Test Procedures in accordance with E-68016 (Reference (37)). PPDD personnel perform the module validation testing in accordance with the Module Test Procedures. PPDD prepares the Module Test Procedures before the execution of the testing. The NICSD IV&V Team shall review the Module Test Procedures in accordance with NQ-2030 (Reference (22)). If NICSD considers necessary, NICSD shall require additional testing to PPDD, in order to check that the module has satisfied the software requirements.

Any test failures, any product or configuration nonconformances, or any errors in the test procedure itself shall be resolved as described in Section 7.1.

5.6.3 Test Equipment Software Review

The NICSD IV&V Team shall review the PPDD control of the test equipment software, used in the Module Validation Testing. The NICSD IV&V Team shall review PPDD's records for test equipment software control to ensure:

- Test equipment software used for the project tests is prepared in accordance with procedures that the NICSD IV&V Team has reviewed and approved.
- PPDD is controlling the software tools in accordance with PPDD procedure E-68020 (Reference (41)).

5.6.4 Module Validation Testing Phase RTM efforts

(1) Preparation of Module Validation Testing Phase RTM

The PPDD design engineers perform the Module Validation Testing Phase RTM efforts. The RTM efforts ensure the module test procedures cover all logic requirements for the modules defined in the Module Design Specifications.

(2) Compilation of the Module Validation Testing Phase RTM Report

The NICSD IV&V Team shall review the RTM from PPDD.

The NICSD IV&V Team shall describe the result of RTM review in V&V Report for this phase.

5.6.5 Security Review

The NICSD IV&V Team shall review that the cyber security requirements described in NQ-2037 (Reference (28)) and the SPP (Reference (44)) are correctly reflected in the software life cycles.

The NICSD IV&V Team shall perform independent review (IR) of the Module Test Procedures and shall review that appropriate cyber security requirements complying with NQ-2037 and the SPP are included in the Module Test Procedures and the SSARs.

In addition, the NICSD IV&V Team shall confirm that appropriate security measures are taken in the following activities:

- Delivery of the fuse map
- Embedment of logic into FPGAs
- Storage of logic embedded FPGAs
- Module assembly
- Transportation and storage of modules

The result of Security Review shall be described in the V&V Report.

5.6.6 Module Validation Testing Phase V&V Reporting

The NICSD IV&V Team shall prepare the Module Validation Testing Phase V&V Report summarizing the V&V activities performed for this Module Validation Testing Phase.

The NICSD V&V Report shall include:

(1) Reference to the reviewed documents

(2) Reference to the Design Verification Reports (DVR)

(3) Reference to the Module Test Reports

(4) Reference to the Module Validation Testing Phase RTM

(5) Results of Test Equipment Software Review

(6) Open items revealed in the RTM efforts

(7) Results of the Security Review

(8) Results of the SSAR review

(9) Metrics described in Section 4.6.6

(10) Any findings, recommendations, or suggestions to reduce any risks identified in the V&V activities

The NICSD IV&V Team delivers the NICSD V&V Report to the ICDD IV&V Team for review.

5.6.7 Baseline Review

To complete the Module Validation Testing Phase, the NICSD IV&V Team shall perform baseline reviews at the phase end as described in Section 4.6.3. The NICSD IV&V Team shall issue a BRR documenting the results of the Baseline Review and report to NICSD SQA Team for review and approval as QA record.

5.7 System Validation Testing Phase

For the unit integration, a NICSD receiving inspector receives the modules to be installed in the units. After accepting the modules in the previous phase, NICSD assembles the module into the units. Then, NICSD assembles the system from the units. The NICSD test personnel shall perform the System Validation Testing in accordance with the SVTP. This test must demonstrate that the system performs all intended functions within the predetermined design, and that the system does not perform unintended or undesirable functions that were identified in the test scope.

The NICSD test personnel generate a test record, which includes a test log. Testing anomalies, if any, will be recorded in a NNR in accordance with NQ-3019 (Reference (33)). NICSD will resolve test anomalies, which may require changing the test procedure or changing FPGA logic. If FPGA logic is changed, the V&V activities in Section 5.5 and 5.6 for the FPGA logic shall be iterated. The test is repeated in its entirety until the test passes successfully. After successful results are obtained, the NICSD IV&V Team shall review the test record with change records (if any). Then the test record will be approved, and placed under the SCMP (Reference (49)).

Table A of the NICSD SMP (Reference (47)) lists the outline of the outputs of these V&V activities.

The NICSD IV&V Team evaluates the results of the System Validation Testing to confirm that requirements identified in the EDS and Unit Detailed Design Specifications are satisfactorily covered, and issue a Software Validation Test Report (SVTR).

The NICSD IV&V Team may also observe NICSD activities to verify that NICSD work in accordance with applicable NICSD procedures. Results of observation shall be documented in the V&V Report.

5.7.1 Document Reviews

The NICSD IV&V Team shall perform independent reviews of the documents, which are listed in Table A of the NICSD SMP (Reference (47)), and marked "DVR" in the "Other Outputs" column. For the procedures to be used for the document review, see Section 4.6.1 in this NICSD VVP.

The NICSD IV&V Team reviews the documents for the V&V activities in this phase referring to the methods and procedures described in Table 15 and Table 16 of the SPP (Reference (44)). The Table B is provided for a better understanding of terminological difference between the SPP and NICSD VVP.

5.7.2 Unit Validation Testing

The NICSD test personnel shall perform the unit validation testing as a part of System Validation Testing in accordance with SVTP.

Any test failures, any product or configuration nonconformance, or any errors in the test procedure itself shall be resolved as described in Section 7.1.

The NICSD IV&V Team shall describe the result of Unit Validation Testing in the V&V

Report for this phase.

5.7.3 System Validation Testing

The NICSD test personnel shall perform the System Validation Testing in accordance with SVTP.

Any test failures, any product or configuration nonconformance, or any errors in the test procedure itself shall be resolved as described in Section 7.1.

Successful completion of testing and document reviews will complete the requirements for commercial grade dedication. The NICSD IV&V Team shall review the completed commercial grade dedication package to confirm that all required activities are complete and that the evaluations are complete and correct. Completion of the NICSD IV&V Team review of the commercial grade dedication shall be the last technical activity to be completed.

The NICSD IV&V Team shall describe the result of System Validation Testing in V&V Report for this phase.

The NICSD IV&V Team shall prepare a Software Validation Test Report (SVTR). The Software Validation Test Report (SVTR) includes the result of Unit Validation Testing and System Validation Testing.

5.7.4 Test Equipment Software Review

The NICSD IV&V Team shall review the NICSD control of the test equipment software, used in the Unit and System Validation Testing. The NICSD IV&V Team shall review NICSD's records for test equipment software control to ensure that the test equipment software used for the tests is controlled in accordance with NQ-2003 (Reference (26)).

5.7.5 System Validation Testing Phase RTM efforts

(1) Preparation of System Validation Testing Phase RTM

NICSD design engineers perform the System Validation Testing Phase RTM efforts. The RTM efforts ensure the units and system validation test procedures cover all functional requirements defined in the Unit Detailed Design Specifications and the EDS.

(2) Compilation of the System Validation Testing Phase RTM Report

The NICSD IV&V Team shall review the RTM.

The NICSD IV&V Team shall describe the result of RTM review in the V&V Report.

5.7.6 Security Review

The NICSD IV&V Team shall review that the cyber security requirements described in NQ-2037 (Reference (28)) and the SPP (Reference (44)) are correctly reflected in the software life cycles.

The NICSD IV&V Team shall perform independent review (IR) of the test procedures, and SSARs. The NICSD IV&V Team shall also review that appropriate cyber security requirements complying with NQ-2037 and the SPP are included in the test procedures
In addition, the NICSD IV&V Team shall confirm that appropriate security measures are taken in storage of the units and the systems.
The result of Security Review shall be described in the V&V Report.

5.7.7 System Validation Testing Phase V&V Reporting

The NICSD IV&V Team shall prepare the System Validation Testing Phase V&V Report summarizing the V&V activities performed for this System Validation Testing Phase.

The NICSD V&V Report shall include:

(1) Reference to the reviewed documents, including hardware verification, see Section 5.9

(2) Reference to the Design Verification Reports (DVR)

(3) Reference to the units and system validation test report

(4) Reference to the System Validation Testing Phase RTM

(5) Results of the Test Equipment Software Review

(6) Results of the Security Review

(7) Completion of SSAR, which shall confirm that:

- All system safety requirements have been satisfied by the life cycle phases.
- No additional hazards have been introduced by the work done during the life cycle activity.

(8) Metrics described in Section 4.6.6

(9) Evaluation of the test results

(10) Conclusion of the V&V activities

The NICSD IV&V Team delivers the NICSD V&V Report to the ICDD IV&V Team for review.

5.7.8 Baseline Review

To complete the software development, the NICSD IV&V Team shall perform baseline reviews at the phase end as described in Section 4.6.3. ICDD and NICSD shall confirm the completion the V&V activities from the Project Planning and Concept Definition Phase through the System Validation Testing Phase to complete the software development. All open items shall be closed. The NICSD IV&V Team shall issue a BRR documenting the results of the Baseline Review and report to NICSD SQA Team for review and approval as QA record.

5.8 Functional Element V&V

FPGA logic is designed using FEs from the PPDD FE library. The control of these FEs is reviewed in the Design Phase by the NICSD IV&V Team. The IV&V Team shall review the following at a minimum:

- Documentation for the FEs including FE test reports — each FE shall be developed, verified, and validated in accordance with PPDD procedure E-68018 as described below.
- Control of FE library and software tools — FE library and software tools shall be controlled under an appropriate configuration management.

The following subsection provides details of the review.

These FE V&V activities can be omitted for the FE for which PPDD has already performed the same V&V activities, and NICSD or ICDD has performed the same review for another safety-related work.

To prepare an FE used in the FPGA-based system, PPDD shall follow the PPDD procedure E-68018 (Reference (39)) for design and testing, and shall get review and approval from NICSD, including the IV&V Team.

The outline of the procedure prescribed in E-68018 is as follows:

(1) FE Requirements Specification

The FE Requirements Specification is established to address at a minimum:

- FE functional requirements,
- Input/Output Signals, and
- Interface/Interaction with other FE.

The FE Requirements Specification must be verified by other engineers who do not contribute the FE Requirements Specification.

(2) FE Design

The PPDD design engineers establish the FE Specification and the other PPDD design engineers establish the FE Test Procedure. The FE Specification states how all of the requirements specified in the FE Requirements Specification for this FE will be implemented, and should contain sufficient criteria to support functional testing of the FE.

The FE Test Procedure describes the process from producing the VHDL source code through the execution of FE testing using test FPGA chips.

The FE Specification and FE Test Procedure must be verified by other engineers who do not contribute to the FE Specification or FE Test Procedure.

An RTM is prepared to trace the design features in the FE Specification to the requirements shown in the FE Requirements Specification. The RTM must also be verified.

(3) FE Coding

The PPDD design engineers generate VHDL source code of FEs in accordance with the design rules shown in E-68017 (Reference (38)) Appendix A. The VHDL source code is converted into an FE EDIF File by the Synplify® tool. At this point, the PPDD design engineers perform functional testing of the FE to verify that the FE meets the requirements defined in the FE Specification using the ModelSim® tool.

The FE source code must be reviewed by independent engineers in PPDD who do not contribute to the FE coding.

(4) FE Testing

The PPDD design engineers map FE to FPGA, program FPGA, and perform an FE validation using hardware stimulation of the programmed FPGA.

The PPDD design engineers perform FE testing in accordance with an FE Test Procedure prepared prior to the testing and record the results in an FE Test Report. Another PPDD design engineer evaluates the FE Test Report and record the results of the evaluation.

(5) Final FE Acceptance/Release

The PPDD design engineers propose the registration of the FE in the FE library to the PPDD configuration manager. The PPDD configuration manager confirms that the FE Requirement Specification, FE Specification, FE Test Procedure, and FE Test Reports with a satisfactory result are established, and determines whether the FE is acceptable. When the FE is acceptable, the PPDD configuration manager releases the FE for use, by approving the registration of the FE in the FE library.

The duplicated complete package of electronic files for FEs library that is incorporated into FPGA design is also stored in NICSD controlled storage locker.

(6) Maintenance Phase

FE logic modifications are approved, documented, verified and validated, and controlled. Section 7.1.2 explains PPDD activities for problem reporting

The verification process for the FE permits a more traceable process than for complete FPGA logic verification. Because of the simplicity of the FE, a shorter simulation is possible, with more thorough verification at this level.

.

5.8.1 Document Check

The NICSD IV&V Team shall check the following documents to ensure that PPDD procedure E-68018 is appropriately applied for FEs placed in the FE library:

- FE Requirements Specification
- FE Specification
- RTM between the FE Specification and the FE Requirements Specification
- FE Test Procedure
- RTM between the FE Specification and the FE Test Procedure
- FE Test Report

The NICSD IV&V Team shall check the documents for the following items:

- FE Specifications, FE Test Procedure and FE Test Reports should be established and checked against FE Requirements Specifications. FE Requirements Specifications should be established and checked against NQ-2032 (Reference (24)).

- The RTMs between documents have been appropriately prepared and reviewed.
- Full pattern tests have been performed for each FE
- The test results are acceptable

The results of the check shall be documented and included in the V&V Report at the Design Phase. See Section 5.4.5.

5.8.2 Check of FE Library Control and Software Tool Control

The NICSD IV&V Team shall check the following items at a minimum, to confirm that PPDD adequately controls the FE library:

- PPDD controls the FE library in accordance with PPDD procedure E-68019 (Reference (40)).
- PPDD controls the software tools in accordance with PPDD procedure E-68020 (Reference (41)). See Section 5.5.7 of this NICSD VVP.

The NICSD IV&V Team shall document the results of the check in the V&V Report at the Design Phase. See Section 5.4.5 of this NICSD VVP.

5.9 Hardware V&V

The NICSD IV&V Team or verifier in NICSD shall perform an independent review of the unit and module hardware design in accordance with NQ-2030 (Reference (22)). The NICSD IV&V Team or verifier in NICSD shall perform an independent review (IR) of ECWD. The results of the review shall be documented and reported as a part of the V&V Report.

6 V&V Reporting

6.1 V&V Report

The NICSD IV&V Team prepares the NICSD VVR, which documents the NICSD activities from the Project Planning and Concept Definition Phase through the System Validation Testing Phase. The NICSD VVR is first prepared at the Project Planning and Concept Definition Phase, and is updated at the end of each life cycle phase. Subsections in Section 5 describes the contents to be included in this NICSD VVR.

The NICSD IV&V Lead shall approve above NICSD VVR.

6.2 Anomaly Reporting

Site Corrective Action Request (SCAR) and Site Nonconformance Notice Report (SNNR) are used for anomaly reporting. Section 6.2.1 and 6.2.2 explains SNNR and SCAR.

6.2.1 Site Nonconformance Notice Report

If an anomaly is found in the FPGA-based equipment to be shipped, the Quality Assurance Group for Nuclear Instrumentation & Control Systems (NICS-QA) determines whether the anomaly is disposed as nonconformance or not, and issues a SNNR in accordance with NQ-3019 (Reference (33)) only if the anomaly is a nonconformance. NQ-3019 also describes subsequent corrective actions against the nonconformance.

Anomalies may be found during validation testing, or in a design used at equipment fabrication.

6.2.2 Site Corrective Action Request

For an anomaly found during the design verification, reviews of SSARs, RTM , EDS, System Test Procedures, System User's Manuals, Elementary Control Wiring Diagrams (ECWD), Unit Detail Design Specifications and Unit User's Manuals, the NICSD IV&V team has a responsibility for issuance of SCAR in accordance with AS-300A009 (Reference (15)). For an anomaly found during reviews of Module Design Specifications, Module Test Procedures, FPGA Design Specifications, and FPGA Test Procedures, the NICSD IV&V Team has a responsibility for issuance of SCAR in accordance with AS-300A009 (Reference (15)). Note that if the anomaly has already been implemented in the product, the NICSD IV&V Team shall report the anomaly to NICS-QA to determine whether a SNNR is to be issued or not.

7 V&V Administrative Requirements

7.1 Anomaly Reporting and Resolution

7.1.1 Problems Found in NICSD Activities

If a problem found in NICSD activities including V&V, the problem shall be reported using SNNR and SCAR as described in Section 6.3.

NICSD test personnel perform the unit and system validation testing. The test personnel shall document any test failures, any product or configuration nonconformance, or any errors in the test procedure as a nonconformance. The nonconformance may be resolved by modifying design documentation, logic, test plans and procedures as necessary. The NICSD IV&V team shall review the revised materials that incorporate the changes. NICSD documents the amount of retest required for these changes, and performs retests as needed to resolve all SNNRs and SCARs The NICSD IV&V team shall confirm that all SNNRs and SCARs are adequately resolved by the end of the System Validation Testing Phase.

7.1.2 Problems Found in PPDD Activities

The PPDD engineers who perform FPGA or module testing shall document any test failures, any product or configuration nonconformance, or any errors in the test procedure using Problem Reporting Sheets (PRSs) as described in E-68016 (Reference (37)). The PRS may be resolved by modifying design documentation, logic, or test plans and procedures as necessary. The NICSD IV&V Team shall review the revised materials that incorporate the changes. PPDD documents the amount of retest required for these changes, and performs retests as needed to resolve all PRSs. Retests will go back to PPDD design team.

If PPDD finds any problem in the configuration items during FPGA Testing and Module Validation Testing, problems shall be reported using a Vendor Nonconformance Report (VNNR) in accordance with NQ-3006 (Reference (30)). A format of VNNR as problem reporting is transmitted to PPDD as an attachment of procurement document to PPDD. Also, if PPDD detects nonconformance after shipment of the modules by PPDD to NICSD (e.g., when the nonconformance discovered in other PPDD projects is affected to this FPGA products.), PPDD issues a VNNR. NICSD controls the VNNR in accordance with NQ-3006.

The NICSD IV&V Team shall confirm that all PRSs are adequately resolved.

7.1.3 Problems Found in Other Vendors' Activities

If any problem is found in NICSD vendor's activities, the problem is considered a vendor nonconformance, and a VNNR is issued in accordance with NQ-3006.

7.1.4 Design Change Activities

Change control shall be implemented in accordance with the NICSD SCMP (Reference (49))

When changes are needed in documents, Document Change Request (DCR) sheet can be used for notification in accordance with NQ-2024 (Reference (21)).

7.2 Activity Iteration Policy

If a design is changed, or a result of test or analysis is changed, the V&V activities that are affected by the change shall be iterated as follows:

- The NICSD IV&V Team shall perform an independent review, or evaluation of the affected documents.
- The NICSD SD Team shall update the RTM and the SSAR to reflect the design change.
- The PPDD engineers shall update the RTM to reflect the design change.
- The NICSD IV&V Team shall perform an independent review of the updated part of the RTM and SSAR.
- The NICSD IV&V Team shall update the VVR for the updated document.
- The NICSD IV&V Team shall prepare a V&V Report for the updated document.

For RTM, a change of the RTM in one phase may affect another phase, and the effect can be propagated through the RTM. The NICSD SD Team shall follow the propagation. The NICSD IV&V Team shall review the changes in the RTM.

7.3 Deviation Policy

If any deviations from this NICSD VVP are required, this NICSD VVP shall be updated using the same review and approval process by which this NICSD VVP was originally created.

The information required for deviations shall identify activities to be deviated, and shall include rationales and effects on software quality.

7.4 Control Procedures

The documents that resulted from the V&V activities shall be controlled in accordance with the NICSD SCMP (Reference (49))

7.5 Standards, Practices and Conventions

Toshiba Internal Standards in Section 3.4, and project documents in Section 3.6 shall be applied to the V&V activities. The SPP (Reference (44)) has been used for guidance. IEEE standards in Section 3.3 are used as guidance.

Toshiba Internal Standards in Section 3.5 shall be applied to the PPDD's activities.

8 V&V Documentation Requirements

8.1 RTM

The RTM traces the base requirements through the life cycle phases, ensuring forward and backward traceability. The NICSD SD Team shall use NQ-2015 (Reference (19)) to prepare the RTM. Also, the PPDD design engineer shall use NQ-2015 required with the procurement specification by the NICSD SD Team to prepare the RTM.

8.2 Test Documents

(1) NICSD Test Documents

The NICSD IV&V Team prepares the test documents for unit validation testing and System Validation Testing, which contain test cases and acceptance criteria, in accordance with the Software Test Plan.

The following procedures are used when creating test documents.

- NQ-2019 (Reference (20))
- NQ-3016 (Reference (32))
- NQ-3015 (Reference (31))

(2) PPDD Test Documents

The PPDD design engineers prepare the FPGA Test Procedures and the Module Test Procedures in accordance with E-68027 (Reference (42)). The PPDD design engineers generate the FPGA Test Reports in accordance with E-68017 (Reference (38)). The PPDD test personnel generate the Module Test Reports in accordance with E-68016 (Reference (37)).

9 VVP Maintenance

The NICSD IV&V Team shall be responsible for the maintaining of this NICSD VVP. The NICSD VVP shall be maintained in accordance with Section 16 of the NICSD SMP (Reference (47)). The updated NICSD VVP shall be prepared, verified and approved in the same manner that the NICSD VVP was first established as a document in accordance with NICSD NQ-2024, "Procedure for Document Control" (Reference (21)). Also the issued NICSD VVP shall be retained as a QA record in accordance with NICSD NQ-3020, "Control Procedure of QA Records" (Reference (34)).

Table A, Compliance to SPP

Table A, Compliance to the SPP

No	SPP Section	Title	VVP Section(s)	Remark
1	4	Software Verification and Validation Program Plan (SVVPP)	N/A	Section Title
2	4.1	Introduction	N/A	No requirement
3	4.1.1	Purpose	1	
4	4.1.2	Scope	1	
5	4.1.3	[Deleted]	N/A	No requirement
6	4.1.4	Relationship of the SVVPP to Other SPP Sections	N/A	No requirement
7	4.2	Verification and Validation Overview	1	
8	4.2.1	Organization	4.1	
9	4.2.2	Schedule	4.2	
10	4.2.3	Resource Summary	4.4	
11	4.2.4	Roles and Responsibilities	4.5	
12	4.2.5	Qualifications	4.4, 4.5	
13	4.2.6	Tools, Techniques, and Methodologies	4.6	
14	4.3	Life Cycle Verification and Validation	5	
15	4.3.1	Management of V&V Activities	5.1	
16	4.3.2	Planning Phase V&V Activities	5.2	
17	4.3.3	Requirements Phase V & V Activities	5.3	
18	4.3.4	Design Phase V & V Activities	5.4	
19	4.3.5	Implementation Phase V & V Activities	5.5	
20	4.3.6	Testing and Integration Phase V & V Activities	5.5, 5.6, 5.7	
21	4.3.7	Installation Phase V & V Activities	5.7	SVT include PFT
22	4.3.8	Operation Phase V & V Activities	N/A	Out of scope
23	4.3.9	Maintenance Phase V & V Activities	N/A	Out of scope
24	4.3.10	Summary of V&V Activities	Table B	
25	4.3.11	Previously Developed or Purchased Software	5.1.3	
26	4.4	V & V Reporting and Administrative Requirements	N/A	Section Title
27	4.4.1	Reporting For Each System or Logical Group of Systems	5.11	
28	4.4.2	Anomaly Reporting and Resolution	6.3, 7.1	

Notice:

The definition of phase for the FPGA-based safety-related systems differs from that in the SPP (Reference (44)), see SMP (Reference (47)).

Table B, V&V Activities Assigned to Each Software Life Cycle Phase

Table B, V&V Activities Assigned to Each Software Life Cycle Phase

Life Cycle Process		Development					
SPP	This NICSD VVP	Project Planning and Concept Definition V&V	Requirements Definition V&V	Design V&V	Implementation and Integration V&V	Module Validation Testing V&V	System Validation Testing V&V
Software Classification		SR	SR	SR	SR	SR	SR
V&V Activities							
Management Review of V&V	Management Review of V&V	PM	PM	PM	PM	PM	PM
SVVP Generation	SVVP Generation	V&V					
Concept Documentation Evaluation	Project Planning and Concept Definition Phase DVR	V&V					
Program Plan Evaluation		V&V					
PFT Plan Generation	Software Test Plan Generation (PFT Plan is included in SVTP)	V&V					
PIT Plan Generation	N/A						
Planning Traceability Analysis	RTM Review	V&V					
Hazard Analysis	N/A (Safety Analysis)	SST	SST	SST	SST	SST	SST
Risk Analysis	N/A	PM	PM	PM	PM	PM	PM
Phase Report	Project Planning and Concept Definition Phase V&V Report	V&V	V&V	V&V	V&V	V&V	V&V
Baseline Reviews	Baseline Reviews	V&V	V&V	V&V	V&V	V&V	V&V
Requirements Traceability Matrix	RTM Review		V&V				
Software Requirements Evaluation	Requirements Definition Phase DVR		V&V				
Software Requirements Interface Analysis			V&V				
Configuration Management Assessment	N/A		DT				
Design Traceability Analysis	RTM Review			V&V			

Table B, V&V Activities Assigned to Each Software Life Cycle Phase

Life Cycle Process		Development					
SPP	This NICSD VVP	Project Planning and Concept Definition V&V	Requirements Definition V&V	Design V&V	Implementation and Integration V&V	Module Validation Testing V&V	System Validation Testing V&V
Software Design Evaluation	Design Phase DVR			V&V			
Software Design Interface Analysis				V&V			
Unit Test Plan Generation	System Validation Test Plan Generation			V&V(Test personnel)			
Integration Test Plan Generation				V&V(Test personnel)			
System Validation Test Plan Generation				V&V(Test personnel)			
SVT Test Case Generation				V&V(Test personnel)			
PFT Test Case Generation				V&V(Test personnel)			
PIT Test Case Generation	N/A						
Source Code Traceability Analysis	VHDL Source Code Review				V&V		
Source Code Evaluation					V&V		
Source Code Interface Analysis					V&V		
Unit and Integration Test Case Generation	Implementation and Integration Phase DVR				PPDD(prepare V&V(review)		
Unit, Integration, and SVT Test Procedure Generation					PPDD(prepare V&V(review)		
Operation and Maintenance Manual Review					V&V		
Unit and Integration Test Execution					STT		
Software Release Report	Implementation and Integration Phase and System Validation Phase DVR				V&V		V&V
Test Traceability Analysis	RTM Review					V&V	V&V

Table B, V&V Activities Assigned to Each Software Life Cycle Phase

Life Cycle Process		Development					
SPP	This NICSD VVP	Project Planning and Concept Definition V&V	Requirements Definition V&V	Design V&V	Implementation and Integration V&V	Module Validation Testing V&V	System Validation Testing V&V
PFT Procedure Generation	System Validation Test Procedure Generation					V&V(Test personnel)	V&V(Test personnel)
SVT Execution	SVT Execution (including PFT)					V&V(Test personnel)	V&V(Test personnel)
PFT Execution						V&V(Test personnel)	V&V(Test personnel)
PIT Execution	N/A						
Installation Configuration Audit	N/A						
Installation Checkout	N/A						
V&V Final Report Generation	Final V&V Report Generation						V&V
Evaluation Of New Constraints	N/A						
Operation Procedures Evaluation	N/A						
Proposed Change Assessment	N/A						
SVVP Revision	N/A						
Anomaly Evaluation	N/A						
Migration Assessment	N/A						
Retirement Assessment	N/A						
Task Iteration	N/A						
Regression Analysis	N/A						

SR = Safety related

empty cell = process is not applied

CCB=Change Control Board
CM=Configuration Management Lead
DT=Software Development Team

PM=Project Manager, may be two separate PM, one responsible for design/development and responsible for V&V
SSL=Software Safety Lead
SST=Software Safety Team

V&V=V&V Lead
SIT=System Installation Test Team
STT=Software Test Team