ENCLOSURE 3

FA32-3702-1000 Rev. 2
Nuclear Instrumentation & Control System Department
Software Management Plan for FPGA-based Safety-Related Systems

Non-Proprietary Version

Safety-Related

Toshiba Project Document No.	Rev. No.
FA32-3702-1000	2

Document Filing No.	Rev. No.
RS-5159335	2

NRW-FPGA-Based I&C System Qualification Project

Software Management Plan

Title: Nuclear Instrumentation & Control Systems Department Software Management 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

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: Monitoring System Engineering Group		
Approved by		Reviewed by
Y. Goto Mar 11, 2013		T. Miyazaki Mar 11, 2013

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

Rev.	Issue Date	Description	Approved by	Reviewed by	Prepared by
2	Feb. 25. 2013	See DECN- FA32-3702-1000-02	A. Naka Feb. 25, '13	K. Wakita Feb 25. 2013	T. Furusawa Feb. 22, 2013

Initial Issue Date	Issued by	Approved by	Reviewed by	Prepared by	Document filing No.
Oct.31, 2011	Nuclear Instrumentation Systems Development & Designing Group	S. Tosuka Oct.31, 2011	K. Wakita Oct.31, 2011 T. Sato Oct.28, 2011	T. Furusawa Oct.27, 2011 M. Tomitaka Oct.27, 2011	5B8K0035

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	See cover page	See DECN- FA32-3702-1000-01	S. Tosuka Apr. 20, 2012	K. Wakita Apr. 20, 2012	T. Furusawa Apr.18, 2012
2	See cover page	See DECN- FA32-3702-1000-02	See cover page	See cover page	See cover page

Table of contents

1 Purpose

The purpose of this Nuclear Instrumentation & Control Systems Department (NICSD) Software Management Plan (NICSD SMP) is to describe the software management planning and the process to be followed by the NICSD in the development and procurement of the Field Programmable Gate Array (FPGA)-Based safety-related Instrumentation and Control (I&C) systems for US nuclear power plants..

Project Document FA10-0501-0024, "Software Program Plan," (SPP) (Reference (2)) establishes requirements and provides guidance and expectations for the design, development, implementation, safety analysis, review, testing, installation, and configuration management of supporting software program plans, e.g., this NICSD SMP.

This NICSD SMP defines:

- Management process, including organization and responsibilities for development of the software design;
- The procedures to be used, the interrelationships between software design activities
- The methods for conducting software safety analyses;
- Development process, including activities performed in each phase of the development process;
- Methods, tools, and techniques used in the development and software safety analyses.
- Software training activities to be carried out for staff responsible for design, development, review, and test of systems.

2 Scope

This NICSD SMP applies to FPGA-based safety-related I&C systems for US nuclear power plants. This NICSD SMP applies to the software management planning and the process to be followed by the NICSD. This NICSD SMP covers the software development activities performed by NICSD that are defined in Section 13. This NICSD SMP complies with the following sections of the SPP (Reference (2)):

- Section 1, Introduction
- Section 2, Software Project Management Program Plan
- Section 3, Software Development Program Plan
- Section 6, Software Safety Program Plan
- Section 10, Software Training Program Plan

This NICSD SMP is prepared in accordance with the processes summarized in Nuclear Energy Systems & Services Division (NED) Document "FPGA-based Safety-Related Systems Software Management Plan" (NED SMP) (Reference (3)) and the appropriate Job Order Sheets that apply to the given system development.

Table C shows the compliance traceability matrix of this NICSD SMP to the SPP.

This NICSD SMP uses existing NED AS standards and NICSD Nuclear Quality (NQ) standards to implement all safety-related activities. Any software specific quality assurance requirements that augment the standard quality assurance procedures are identified in the NICSD Software Quality Assurance Plan (SQAP).

3 Definitions and Abbreviations

3.1 Definitions

Commercial-Off-The-Shelf (COTS): This term (COTS) is defined to be software purchased from a vendor, which is not modified to support plant requirements, but may be configured to support plant requirements. This definition does not vary for safety or nonsafety life cycles. [This definition is extracted from the SPP (Reference (2))]

In this NICSD SMP, the Functional Elements (FEs) are treated as previously developed COTS software. For more details, see Section 11.1.

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. 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 fusemap.

Previously Developed Software (PDS): This term (PDS) is defined to be software that a vendor wrote, or purchased from another vendor, at an earlier date, which might be used as-is, or more likely will be modified to support plant requirements. This definition does not vary for safety or nonsafety life cycles. [This definition is extracted from the SPP (Reference (2))]

In this NICSD SMP, FPGA logic is treated as PDS. For more details, see Section 11.1.

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.

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

Table 3-1 Comparative Table for Terms Used in SPP and NICSD SMP

SPP	NICSD SMP	Notes
Baseline Review Report	Baseline Review Report	Refer to Section 10
Configuration Management Assessment	NICSD SD Team activity (Defined in NICSD SCMP)	Refer to Section 13.1.10
COTS Evaluation Report and Documentation Package	CGD Package (including CGD Report, CG Survey Report, PTER, FTER CDR Report.)	Refer to Section 11.2.2
Data Communication Protocol and Architecture	EDS	Refer to Section 13.1.6
Hardware Requirements Specification	Unit DDS	Refer to Section 13.2.3
Intra-System Communication Protocol Specification	MDS, FPGA Design Specification	Refer to Sections 13.3.4 and 13.3.5
PDS Evaluation Report and Documentation Package	CGD Package (including CGD Report, CG Survey Report, PTER, FTER CDR Report.)	Refer to Section 11.2.1
Platform Factory Test (PFT) Plan and Procedure	Included in Software Validation Test Plan (Platform Factory Test (PFT) can be combined with System Validation Testing)	Refer to Section 13.3.7
Platforms Integration Test (PIT) Plan and Procedure	N/A	Outside the scope of this plan
Requirements Traceability Matrix	Requirements Traceability Matrix	Refer to Section 12
Secure Development and Operational Environment Analysis Report	Included in NICSD V&V Reports (VVR)	Refer to Section 8.3
Software Build Description Software Build Procedure and Report	Included in NICSD VVRs	Refer to Section 13.4.10
Software Coding Convention and Guideline Documents	Software Coding Convention and Guideline Documents	Refer to Section 11.3
Software Configuration Management Plan (SCMP)	NICSD SCMP	Refer to Section 13.1.4
Software Design Description	MDS, FPGA Design Specification	Refer to Sections 13.3.4 and 13.3.5
Software Development Plan (SDP)	Section 13 of NICSD SMP	Refer to Section 13
Software Functional Testing	FPGA testing	Refer to Section 13.4.4
Software Functional Test Report	FPGA Test Report	Refer to Section 13.4.4
Software Interfaces Document (SID)	EDS	Refer to Section 13.1.6
Software module	FPGA logic	"FPGA logic" is combination of FEs and connection between FEs
Software module test	FPGA testing	Refer to Section 13.4.4
Software Project Management Plan	NICSD SMP	This document
Software Quality Assurance Plan	NICSD SQAP	Refer to Section 13.1.4
Software Release Notes, Software Release Report	NICSD MCL, PPDD Module MCL	Refer to Sections 13.5.4 and 13.6.13
Software Requirements Specification (SRS)	Unit DDS	Refer to Section 13.2.3
Software Safety Analysis Report	NICSD SSAR	Refer to Section 14
Software Safety Plan	Section 14 of NICSD SMP	Refer to Section 14
Software Test Plan	Software Test Plan	Refer to Section 13.1.4
Software Tool Documentation Package	CGD Package (including CGD Report, CG Survey Report, CDR Report.)	Refer to Section 8.1.2
Software Training Manual	Included in System O&M Manual	Refer to Section 13.5.8
Software Training Plan	Section 15 of NICSD SMP	Refer to Section 15
Software unit	FPGA logic	Refer to Section 11.1
Software unit test	FPGA testing	Refer to Section 13.4.4

Table 3-1 Comparative Table for Terms Used in SPP and NICSD SMP

SPP	NICSD SMP	Notes
Software Verification and Validation Plan	NICSD VVP	Refer to Section 13.1.4
Software Validation Testing	Module Validation Testing, System Validation Testing	Refer to Sections 13.5.3 and 13.6.3
Software Validation Test Plan and Test Cases Specification	Module Test Procedure, Software Validation Test Plan	Refer to Sections 13.3.4 and 13.3.7
Software Validation Test Report	Module Test Report, Software Validation Test Report	Refer to Sections 13.5.3 and 13.6.3
Software Validation Procedure	Module Test Procedure, Software Validation Test Plan	Refer to Sections 13.3.4 and 13.3.7
Source Code	VHDL source code	Refer to Section 13.4.3
System Architecture Description (SAD)	EDS	Refer to Section 13.1.6
System O&M Manual	System O&M Manual	Refer to Section 13.5.8
N/A	FPGA	"FPGA" means the FPGA chip (hardware).

3.2 Abbreviations

AS	Toshiba Nuclear Energy Systems and Services Division Work Standard
BRR	Baseline Review Report
BTP	Branch Technical Position
CAD	Computer Aided Design System
CC	Critical Characteristic
CCA	Critical Characteristics for Acceptance
CCD	Critical Characteristics for Design
CDI	Commercial Dedication Instruction
CDR	Critical Digital Review
CG	Commercial Grade
CGD	Commercial Grade Dedication
CI	Configuration Item
COTS	Commercial-Off-The-Shelf
DCN	Design Change Notice
DCTR	Design Change Technical Report
DDS	Detailed Design Specification
DIS	Design Input Sheet
DRM	Design Review Meeting
DVR	Design Verification Report
ECWD	Elementary Control Wiring Diagram
EDS	Equipment Design Specification
EPC	Engineering, Procurement, and Construction
EPRI	Electrical Power Research Institute
ES	Engineering Schedule
FE	Functional Element
FMEA	Failure Mode Effect Analysis
FPGA	Field Programmable Gate Array
FTA	Fault Tree Analysis
FTER	Final Technical Evaluation Report
Fuchu-PS	Fuchu Complex Power Systems Segment
GPM	Group Manager
I&C	Instrumentation and Control
IBD	Interlock Block Diagram

ICDD	Instrumentation & Control Systems Design & Engineering Department
IED	Instrumentation Electrical Diagram
IEEE	Institute of Electrical and Electronics Engineers
ISCPS	Intra System Communications and Protocol Specification
ISO	International Standardization Organization
ISRG	Information Security Rules and Guidelines
IV&V	Independent Verification and Validation
IV&V Lead	Independent Verification and Validation Lead
MCL	Master Configuration List
MDS	Module Design Specification
MTP	Master Test Plan
NED	Nuclear Energy Systems & Services Division
NICSD	Nuclear Instrumentation & Control Systems Department
NICS-QA	Quality Assurance Group for Nuclear Instrumentation & Control Systems
NICS-QC	Quality Control Group for Nuclear Instrumentation & Control Systems
NISD	Nuclear Instrumentation Systems Development & Designing Group
NQ	Nuclear Quality
NQAD	Nuclear Quality Assurance Department
O&M	Operations and Maintenance
PCDL	Project Control Document List
PDS	Previously Developed Software
PFT	Platform Factory Test
PIT	Platforms Integration Test
PM	Project Manager
PPDD	Power Platform Development Department
PPS	Procurement Planning Sheet
PRM	Process Review Meeting
PSNE	Power Systems Company Nuclear Energy
PTER	Preliminary Technical Evaluation Report
QA	Quality Assurance
QAPD	Quality Assurance Program Description
QC	Quality Control
RTM	Requirements Traceability Matrix
SAD	System Architecture Description
SAR	Safety Analysis Report
SBPR	Software Build Procedure and Report
SCAR	Site Corrective Action Request
SCL	Software Configuration Lead
SCMP	Software Configuration Management Plan
SCSI	Small Computer System Interface
SD	Software Development
SD Team	Software Development Team
SDD	System Design Description
SDL	Software Development Lead
SDOE	Secure Development and Operational Environment
SDPP	Software Development Program Plan
SES	Sub-master Engineering Schedule
SID	Software Interfaces Document
SIL	Software Integrity Level
SM	Senior Manager
SMP	Software Management Plan
SNNR	Site Nonconformance Notice Report

SPMPP	Software Project Management Program Plan
SPP	Software Program Plan
SQ	Software Quality
SQA	Software Quality Assurance
SQA Team	Software Quality Assurance Team
SQAL	Software Quality Assurance Lead
SQAP	Software Quality Assurance Plan
SRS	Software Requirements Specification
SS	Software Safety
SS Team	Software Safety Team
SSAR	Software Safety Analysis Report
SSL	Software Safety Lead
SSPP	Software Safety Program Plan
SVTP	Software Validation Test Plan
SVTR	Software Validation Test Report
SwDD	Software Design Description
TBD	To Be Determined
TDMS	Toshiba Design and Manufacturing Service Corporation
TR	Technical Report
USNRC	United States Nuclear Regulatory Commission
V&V	Verification and Validation
VHDL	Very High Speed Integrated Circuit Hardware Description Language
VVP	Verification and Validation Plan
VVR	Verification and Validation Report
WBS	Work Breakdown Structure

4 References

(1) Not used

(2) Toshiba Project Document Number FA10-0501-0024
"Software Program Plan" Rev.1

(3) Toshiba Project Document Number FA32-3702-0005
"Nuclear Energy Systems and Services Division FPGA-based Safety-Related Systems Software Management Plan" Rev.1

(4) Not used

(5) USNRC, NUREG-0800 Branch Technical Position (BTP) 7-14
"Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems" Rev.5

(6) Not used

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

(8) EPRI NP-5652 "Utilization of Commercial Grade Items in Nuclear Safety Related Applications," March 1988

(9) EPRI TR-102260 "Supplement Guidance for the Application of EPRI Report NP-5652 on the Utilization of Commercial Grade Items," March 1994

(10) EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," October 1996

(11) EPRI TR-107339, "Evaluating Commercial Digital Equipment for High Integrity Applications," December 1997

(12) Electric Power Research Institute (EPRI) Technical Report 1011710, "Handbook for Evaluating Critical Digital Equipment and Systems," November 2005

(13) Toshiba Corporation, Power Systems Company 4401-4
"Nuclear Energy QA Program Description"

(14) Toshiba Nuclear Energy Systems and Service Division AS-100A008
"Procedure for Indoctrination and Training"

(15) Toshiba Nuclear Energy Systems and Service Division AS-100A009
"Procedure for Preparation of the Position Guides/Description"

(16) Toshiba Nuclear Energy Systems and Service Division AS-200A008
"Procurement Planning Procedure"

(17) Toshiba Nuclear Energy Systems and Service Division AS-200A014
"Procedure for Documentation of Design Inputs"

(18) Toshiba Nuclear Energy Systems and Service Division AS-200A110
"Procedure for commercial grade items and services"

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

(20) Toshiba Nuclear Energy Systems and Service Division AS-200A132
"Digital System Safety and Hazards Analysis Procedure"

(21) Toshiba Nuclear Instrumentation & Control Systems Department NQ-1002
"Standard of Organization for Fuchu-PS Nuclear Quality Assurance"

(22) Toshiba Nuclear Instrumentation & Control Systems Department NQ-1003
"Application of AS Standards"

(23) Toshiba Nuclear Instrumentation & Control Systems Department NQ-2001
"Process Review Meeting Convening Standard"

(24) Not used

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

(26) Toshiba Nuclear Instrumentation & Control Systems Department NQ-2004
"Preparation Procedure for Equipment Design Specification"

(27) Toshiba Nuclear Instrumentation & Control Systems Department NQ-2005
"Preparation Procedure for Detailed Design Specification"

(28) Toshiba Nuclear Instrumentation & Control Systems Department NQ-2010
"Preparation Procedure for FPGA Design Specification"

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

(30) Toshiba Nuclear Instrumentation & Control Systems Department NQ-2017
"Preparation Procedure for ECWD"

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

(32) Toshiba Nuclear Instrumentation & Control Systems Department NQ-2025
"Preparation Procedure for Procurement Document for CG Items & Services"

(33) Toshiba Nuclear Instrumentation & Control Systems Department NQ-2026
"Control Procedure of supplier generated documents"

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

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

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

(37) Toshiba Nuclear Instrumentation & Control Systems Department NQ-2034
"Procedural Standard for Control of Software Tools Used with FPGA Based Systems"

(38) Toshiba Nuclear Instrumentation & Control Systems Department NQ-2035
"Procedure for Design Change Control"

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

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

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

(42) Toshiba Nuclear Instrumentation & Control Systems Department NQ-3010
"Inspection control procedure"

(43) Toshiba Nuclear Instrumentation & Control Systems Department NQ-3022
"Internal Audit Procedure"

(44) Toshiba Nuclear Instrumentation & Control Systems Department NQ-3024
"Receiving Inspection Procedure"

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

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

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

(48) Toshiba Power Platform Development Department E-68018

"PPDD Procedural Standard for Functional Element Development"

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

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

(51) Not used

(52) Toshiba Project Document Number FA10-0301-0001
"Project Specific Document Control Procedure" Rev.0,

(53) Not used

(54) Toshiba Project Document Number FA32-3709-0001
"Nuclear Energy Systems and Services Division FPGA-based Safety-Related Systems Verification and Validation Plan" Rev.2

(55) Toshiba Project Document Number FA32-3701-1001
"Nuclear Instrumentation & Control Systems Department Software Quality Assurance Plan for FPGA-based Safety-Related Systems" Rev.1

(56) Toshiba Project Document Number FA32-3708-1000
"Nuclear Instrumentation & Control Systems Department Software Configuration Management Plan for FPGA-based Safety-Related Systems" Rev.1

(57) Toshiba Project Document Number FA32-3709-1000
"Nuclear Instrumentation & Control Systems Department Verification and Validation Plan for FPGA-based Safety-Related Systems" Rev.5

(58) Not used

(59) Not used

(60) Not used

Notice: When using above NED, NICSD and other Toshiba internal standards, the latest version shall be used.

5 Organizations and Responsibilities

5.1 Organizations

Figure 5-1 shows the organizations responsible for development of the FPGA-based systems software design. Based on the SPP (Reference (2)), FPGA logic is considered to be developed using a software-like lifecycle. For the Toshiba plans, FPGA logic is referred to as software,

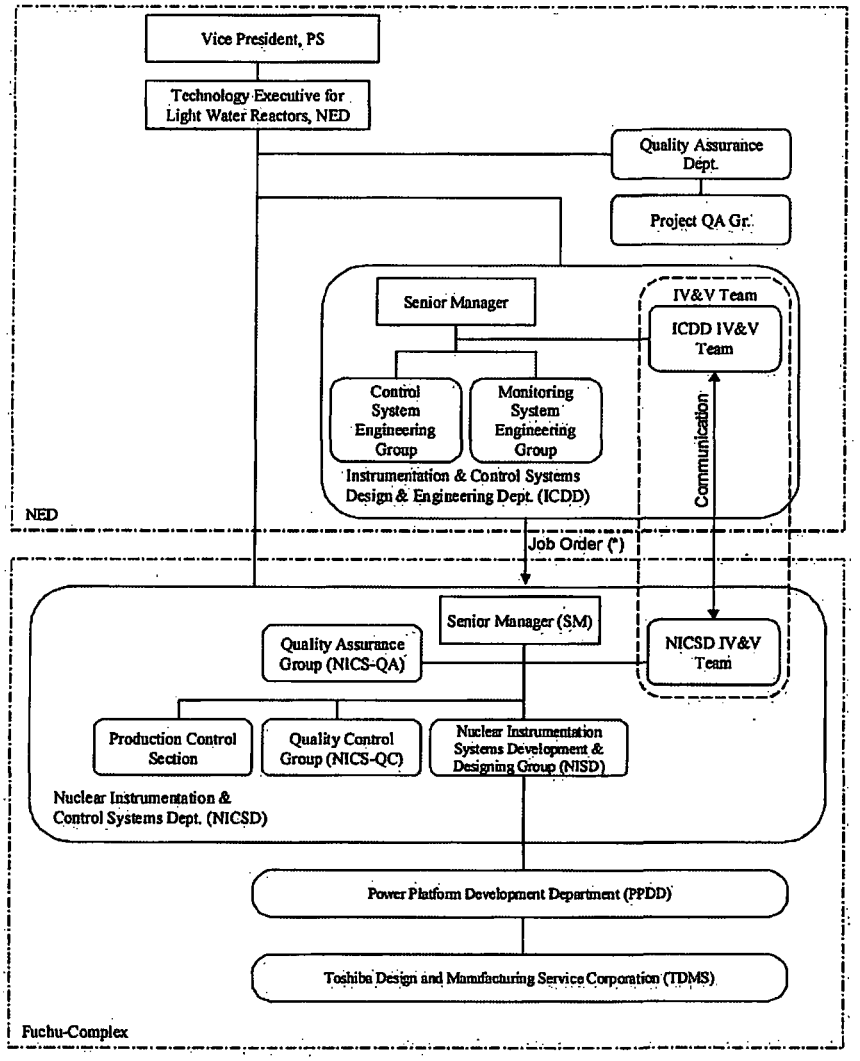
for simplicity. The Instrumentation & Control Systems Design & Engineering Department (ICDD) of NED is responsible for the I&C system design documents. NED procures the assembled FPGA-based equipment from NICSD and delivers it to customers.

NICSD is responsible for detailed design of the FPGA-based equipment, procures the modules for the FPGA-based equipment from the Power Platform Development Department (PPDD), and assembles the FPGA-based equipment from the modules.

The Quality Assurance Group in NICSD (NICS-QA) is responsible for quality assurance in NICSD. Responsibilities for the QA Group are described in NQ-1002 "Standard of Organization for Fuchu-PS Nuclear Quality Assurance" (Reference (21)). Additional software QA responsibilities are provided in the NICSD Software Quality Assurance Plan (NICSD SQAP) (Reference (55)).

PPDD designs the modules for the FPGA-based equipment and tests the FPGAs and the modules. PPDD procures manufacturing of the designed modules from Toshiba Design and Manufacturing Service Corporation (TDMS). NICSD oversees PPDD activities.

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 team communicate with each other, and work together as one IV&V team as needed for the quality of the products.



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

Figure 5-1 Organizations for FPGA-based Safety-Related I&C Systems

5.2 Responsibilities

This section describes the organizations for FPGA-based safety-related I&C system development and defines the responsibilities and authorities of the organizations performing safety-related activities in NICSD. Responsibilities and authorities of NED organizations are defined in the NED SMP (Reference (3)).

The person holding the responsible position shall be able to designate other person for defined aspects of their roles. The person holding the responsible position shall always be responsible for the actions and decisions of the designated person as specified in NQ-1002 (Reference (21)).

5.2.1 NICSD Project Manager (NICSD PM)

The NICSD PM shall be responsible for the managerial process and technical direction of the

software development activities within the NICSD scope. The Senior Manager (SM) of NICSD is expected to be the NICSD PM, or the SM may assign a NICSD PM, to whom the SM delegates the SM's responsibilities and authority for the project.

Through the life cycle, the NICSD PM shall be responsible for management of the schedule, budget, and resources. The PM shall assign the NICSD IV&V Lead and ensure independence of resources and budget between the NICSD IV&V Team and design groups. The NICSD PM shall also assign an NICSD Software Safety Lead (NICSD SSL) independent of the design and Verification and Validation groups.

The NICSD PM shall be responsible for ensuring independence of the design, V&V, software quality assurance, and software safety analysis functions.

The NICSD PM shall ensure that all process requirements are complete, the systems have been evaluated and accepted by NED, deliveries and signoffs are complete, and final disposition of nonconformance has been performed.

5.2.2 NICSD Software Development Lead (NICSD SDL)

The NICSD SDL shall be responsible for the software development and personnel training. The NICSD PM is responsible for assigning the NICSD SDL, delegating the authority for the project.

The NICSD SDL and the NICSD PM shall not be the same person, in order to ensure the independence of the V&V personnel whom the NICSD PM assigns. The NICSD SDL cannot be the NICSD SSL.

The NICSD SDL shall assign a NICSD Software Configuration Lead (NICSD SCL) who shall be responsible for configuration management of software and hardware. The NICSD SCL takes a role of "Configuration Manager" specified in NQ-2033 (Reference (36)). The NICSD SCL shall be responsible for preparing a NICSD Software Configuration Management Plan (NICSD SCMP) (Reference (56)). The NICSD SDL shall have overall responsibility for identifying and preparing software configuration items. The responsibility of the NICSD SCL shall be described in the NICSD SCMP. The NICSD SDL also performs the NICSD Architecture Lead and NICSD Integration Lead role.

The NICSD SDL shall build a NICSD Software Development Team (NICSD SD Team).

5.2.3 NICSD IV&V Lead

The NICSD PM assigns a NICSD IV&V Lead who leads the NICSD IV&V Team. The NICSD IV&V Team shall perform the V&V activities technically, managerially, and financially independent of the software development. The NICSD IV&V Lead shall assign other V&V personnel, and shall be responsible for the V&V activities and baseline reviews. Also, the NICSD IV&V Team shall review the software safety analysis reports, and perform baseline reviews. The NICSD IV&V Team shall oversee the following activities.

- Software tests in PPDD and NICSD
- Software implementation and integration in PPDD
- Baseline review

The NICSD IV&V Lead shall have overall responsibility for software testing. The NICSD IV&V Lead shall build a NICSD IV&V Team containing a Software Test Lead and test engineers.

5.2.4 NICSD Software Safety Lead (NICSD SSL)

The NICSD PM assigns a NICSD SSL in NICSD. The NICSD SSL is responsible for carrying out the software safety activities described in Section 14. The NICSD SSL shall build a NICSD Software Safety Team (NICSD SS Team).

5.2.5 NICSD Software QA Lead (NICSD SQAL)

The manager of the NICS-QA performs the NICSD SQAL role. The NICSD SQAL shall provide oversight of the design team, the NICSD IV&V Team and SS Team from QA perspective.

The NICSD SQAL shall build a NICSD Software QA Team (NICSD SQA Team).

The manager of the NICS-QA is provided with a direct line of communication to senior management on all quality-related matters through the NED Nuclear Quality Assurance Department (NQAD) as described in the Power Systems Company Nuclear Energy (PSNE) QA Program Description (QAPD) (Reference (13)).

The manager of the NICS-QA is responsible for the entire internal audit activities with NICSD in accordance with NQ-3022.

6 QA Programs and Procedures

6.1 Overview

The Power Systems Company Nuclear Energy (PSNE) QA Program Description (QAPD) (Reference (13)) is compliant to 10 CFR Appendix B, and establishes the quality system document structure which includes the NED "AS" standards. The PSNE QAPD also shall be applied to NICSD. Certain AS Standards apply to NICSD. Applicable AS standards are identified in NQ-1003 "Application of AS Standards." (Reference (22))

NICSD establishes its QA program based on applicable AS standards, and NQ standards which are developed by NICSD for the areas that AS standards do not cover. NICSD works under this QA program for the FPGA-based safety-related systems.

PPDD works under its ISO 9001 QA program. To use the modules designed and manufactured under the ISO 9001 QA program in nuclear safety systems, NICSD applies their Commercial Grade Dedication (CGD) process to dedicate the FPGA logic, modules, produced by PPDD. The NICSD SQAP (Reference (55)) shall describe requirements for CGD and subcontractor management.

6.2 Commercial Grade Dedication Overview

As described in the previous section, NICSD procures the modules from a commercial supplier, PPDD, under NICSD CGD process in accordance with AS200A110 (Reference (18)), NQ-4001 (Reference (45)) and NQ-2030 (Reference (34)). PPDD designs and manufactures the modules under a commercial QA program. For typical CGD processes, the commercial product is produced, and then the CGD is performed to qualify the commercial product for use in a safety-related application. However, since FPGA development follows a typical software

lifecycle, waiting for a completed product to perform the CGD is inappropriate for verification of software dependability. NICSD performs activities in each life cycle phase that support a final CGD of the completed modules. NICSD oversees PPDD activities during each lifecycle phase with PPDD involvement. This ensures that the FPGA development is acceptable as it proceeds through the lifecycle. A module's CGD can only be completed when the completed module is delivered to and accepted by NICSD.

The NICSD CGD process complies with EPRI NP-5652 (Reference (8)), which has been endorsed by the USNRC. NICSD developed its commercial grade acceptance process based on the process described in EPRI TR-102260 (Reference (9)), EPRI TR-106439 (Reference (10)), EPRI TR-107339 (Reference (11)), and EPRI 1011710 (Reference (12)) in development of the evaluation and CGD process for FPGA I&C systems.

NICSD also procures the unit chassis, cables, and other equipment that do not include FPGA or software from commercial suppliers, under NICSD CGD process in accordance with NQ-4001 (Reference (45)).

7 Management Process

7.1 Management Objectives and Priority

The NICSD PM shall be responsible for project management. The NICSD PM shall require the NICSD SDL, other leads, and managers in NICSD involved in the project to guide and supervise their subordinates involved in the project to address each of the following critical elements of project deliverables. The NICSD SDL, other leads, and managers in NICSD shall be responsible for reporting to the NICSD PM.

- Integrity

  The NICSD PM shall require the NICSD SDL, other leads, and managers in NICSD involved in the project to guide and supervise their subordinates involved in the project to keep the Toshiba internal commitment and standard to work with integrity.

- Quality

  The NICSD PM shall require all NICSD personnel to keep the requirements in NICSD SQAP (Reference (55)), and applicable industry codes and standards.

- Occupational safety

  The NICSD PM shall require the NICSD SDL, other leads, and managers in NICSD involved in the project to guide and supervise their subordinates involved in the project to keep the Toshiba internal policies for their occupational safety.

- Project Standards

  The NICSD PM shall ensure that related documents are prepared on schedule, in accordance with the NICSD QA program, and that they meet the project requirements.

7.2 Risk Management

The NICSD PM shall be responsible for project risk management, concerning schedule, budget, and resources, and must take appropriate actions to minimize the risks.

The NICSD PM shall require the NICSD SQAL to establish the requirements for anomaly reporting, corrective action and change control in NICSD SQAP (Reference (55)).

Section 14 contains the necessary requirements for software risk management for FPGA-based safety-related systems.

The NICSD SDL, other leads, and managers in NICSD shall report to the NICSD PM any concerns related to project risk as a part of periodic NICSD Management Meetings. At the periodic ICDD-NICSD Project Meeting, the NICSD SDL shall report the concerns related to project risk identified at the periodic NICSD Management Meetings to ensure that the NED PM is informed.

7.3 Monitoring and Controlling Mechanisms and Metrics

The NICSD PM shall monitor the performance of the work. The NICSD SDL prepares the NICSD Engineering Schedules (ESs) for the FPGA-based system as described in Section 9. The NICSD PM shall monitor the work performance against the ESs based on reporting from the NICSD SDL, and other leads. The NICSD communicates to the NED PM who integrates the NICSD schedule into the overall Integrated Project Schedule.

Project management occurs throughout the software life cycle. This NICSD SMP describes project control mechanisms applied in each phase as follows:

7.3.1 Initiation

The NICSD PM shall produce the NICSD Engineering Schedules (NICSD ESs), which shall consider resource availability and allocate these resources according to the approved schedule and budget with the support from the NICSD SDL, other leads.

7.3.2 Planning and Scheduling

The NICSD PM shall be responsible for developing the process model, schedule, design inputs and outputs, deliverables, QA requirements and resource allocation in NICSD.

Work packages including submittal documents are defined in the NICSD Project Control Document List (NICSD PCDL) as specified in NQ-2024 (Reference (31)). The procedures for developing and maintaining the documents are described in Table-A. Table-A defines all the documents required by NICSD's process to design, develop, implement, verify, validate, and perform system safety analyses for the FPGA-based safety-related systems. Any additional documents defined in the SPP (Reference (2)) do not apply to the FPGA-based safety-related systems.

The NICSD PM shall ensure that the issued documents are developed and maintained in accordance with these procedures. The NICSD SDL shall provide support to NICSD PM activities.

NICSD procures the modules from PPDD under the NICSD CGD process in accordance with AS200A110 (Reference (18)), NQ-4001 (Reference (45)) and NQ-2030 (Reference (34)). NICSD has the responsibility to ensure that the CGD activities in NICSD are conducted correctly. NICS-QA will conduct an audit of NICSD in accordance with NQ-3022 (Reference (43)), and a CGD survey of PPDD in accordance with NQ-3005 (Reference (41)).

PPDD shall develop and maintain required documents and records in accordance with PPDD standard QA program as described in PPDD E-68016 (Reference (46)).

The project management tools used to accomplish these activities and control processes are described in Section 8.1.1. The software development tools and evaluation processes are

described in Section 8.1.2.

7.3.3 Execution

The following section describes the requirements, content, approval process, use, maintenance, change process, and measurement techniques of following project execution elements.

(1) Work Breakdown Structure (WBS)

The NICSD PM is responsible for making appropriate work breakdown structure, and keeping the NICSD ES consistent with the Sub-master Engineering Schedule (SES) prepared by NED. The NICSD ES shall be planned considering the work breakdown structure, document the work dependencies, and reflect the documentation requirements specified in the NICSD SMP.

(2) Requests for Services and Materials

There is no specific requirement for services and materials obtained from any third party related to software management, thus this requirement is not applicable for the project.

(3) Recurring Project Status Meetings

- Periodic NICSD Management Meeting.

  The NICSD PM convenes a periodic NICSD Management Meeting. The NICSD SDL reports the status of the project to NICSD PM at the meetings. As described in Section 7.2, the NICSD SDL, other leads and manager reports any concerns related to project risk as a part of risk assessment activity. The NICSD SDL, other leads and manager in NICSD shall report their activity progress.

- Periodic ICDD-NICSD Project Meeting.

  The NICSD SDL, responsible leads and engineers attend and report the project status including the progress in PPDD at the periodic meetings between ICDD and NICSD which are convened by NED PM to check and monitor the project progress.

  The NICSD SSL shall report the hazards identified during software safety activities to the NED System Safety Lead and NED PM.

  As described in Section 7.2, the NICSD SDL reports the concerns related to project risk to be shared with NED identified at the periodic NICSD Management Meetings.

  The NICSD IV&V Lead shall report the status of V&V activities and baseline review.

  An issue tracking spread sheet is used to track the issues found during the meetings.

- Process Review Meeting (PRM)

  The NICSD SDL is responsible for planning the Process Review Meetings (PRM) in accordance with NQ-2001 (Reference (23)). In the PRMs, the NICSD SDL and SQAL review the status of the project including V&V activities and baseline review. For each PRM, a PRM record is prepared to track the issues identified during the meeting. The PRM records are registered in the[ ]d

- Attending PPDD Design Review Meeting

  NICSD confirms the status of PPDD activities through the oversight of Design Review Meetings (DRMs). For each DRM, a DRM record is prepared to track the issues identified during the meeting. The DRM records are registered in the[ ]d [ ]d

(4) Hardware and Software development

The requirements, content, approval process, use, maintenance, and change process for hardware and software development are specified in NQ-2036 and NQ-2030 (Reference (34)).

(5) Interfaces between Software and Hardware, and Interfaces between Systems

The detailed development process including interface control, document review and approval, verification and validation, and PPDD control process are described in Section 13.

(6) Software V&V and Testing

The software V&V and testing activities are defined in the NICSD VVP (Reference (57)). The NICSD IV&V Lead shall oversee the V&V and testing activities, and report the status of the metrics defined in the NICSD VVP to the NICSD PM at the periodic NICSD Management Meeting.

With support from the IV&V Lead, the NICSD PM shall

- Monitor the execution of the NICSD VVP and analyze problems associated with the execution,
- Ensure software being produced fulfills requirements,
- Evaluate testing results and check for completeness,
- Monitor V&V outputs and determine when a task is complete, and
- Assess proposed changes to the software to identify affected requirements and any new hazards or risks as well as changing and re-performing V&V tasks as necessary to address the changes in accordance with the change control process defined in the NICSD SCMP (Reference (56)).

(7) Software Safety Analysis

The software safety analysis activities are defined in Section 14 of this NICSD SMP.

The NICSD SSL shall oversee the software safety analysis activity, and report the software safety concerns to the NICSD PM at the periodic NICSD Project Management Meeting.

(8) Implementation of the NICSD SQAP

The software quality assurance activities shall be implemented in accordance with the NICSD SQAP (Reference (55)). The NICSD SQAP shall describe the metrics used to measure the product quality. The NICSD SQAL shall oversee the software quality assurance activities, and report the status of the metrics to the NICSD PM at the periodic NICSD Project Management Meeting.

(9) Assuring Project Progress and Correct Deliverables

The NICSD PM and SDL ensure that the document shall be developed as defined in the NICSD PCDL.

The schedule for the developments of the documents is developed and controlled by the NICSD SDL, and documented in the NICSD ESs. The major milestone of the document development and delivery are provided to and are reviewed and approved by NED PM. The NED PM populates the milestones in the Sub-master Engineering Schedule (SES) prepared by NED to be shared among NED and NICISD. The NICSD PM also populates the activities and milestones as needed in the overall integrated project schedule, and prepares the NICSD ESs with support from NICSD SDL. The NICSD ESs describe the milestone dates for critical activities such as software safety analysis, independent V&V, and configuration control. The NICSD SDL shall prepare the NICSD ESs considering the necessary time for each critical activity based on the information and request from each lead.

In addition, the NICSD SDL shall prepare the NICSD ESs considering the training plans provided by the NICSD PM, and managers in NICSD. The NICSD ESs shall provide sufficient time for review and approval of the software plans described in Section 13.1.4 prior to use.

Design activities, V&V activities, and baseline reviews shall be listed in the NICSD ESs linking those activities as appropriate to thoroughly control the schedule progress, and that the progress status shall be followed up in the periodic ICDD-NICSD Project Meetings and the PRMs.

The NICSD ESs, issue tracking spread sheet, and PRM reports are registered in the Toshiba [ ]d The NICSD PM has approval authority in the[ ]d [ ]d The NICSD PM shall confirm and review the software development progress by checking the PRM reports and NICSD ESs updated in the[ ]d [ ]d The NICSD design documents are reviewed by the NICSD IV&V Team and NICSD SQA Team in accordance with the NICSD VVP and SQAP respectively.

The NICSD SDL, other leads, and managers in NICSD shall be responsible for controlling the team activities in accordance with the NICSD ESs developed by NICSD SDL. The detail progress for each team activities is monitored at a daily or periodic team meeting.

The production control section in NICSD shall be responsible for controlling the production schedule including PPDD schedule, and reporting to the NICSD PM at the periodic NICSD Management Meeting. The PPDD design documents are reviewed by NICSD IV&V Team in accordance with the NICSD VVP (Reference (57)), and approved by NICSD SD Team in accordance with NQ-2026 (Reference (33)).

(10) Resource and Manpower Levels

The responsibility of the NICSD PM, NICSD SDL, other leads, and managers in NICSD regarding training and personnel qualification is described in Section 15.1.

7.3.4 Closeout

The NICSD PM shall ensure that all process requirements are complete, the system has been evaluated and accepted by the customer, deliveries and signoffs are complete, and final disposition of nonconformance is performed according to this SMP by reviewing the NICSD ES, issue track spreadsheet, PRM reports and project deliverables using[ ]d [ ]d

7.4 Staffing Plan

The NICSD PM shall require the NICSD SDL to prepare the NICSD ES commensurate with the workload and specialties required for the work.

8 Technical Process

8.1 Methods, Tools, and Techniques

8.1.1 Project Management and Engineering Tool Control

NICSD uses the tools listed in Table 8-1 for electronic document control and project activities.

Table 8-1 does not include standard office software such as Microsoft® Office Word, Excel, Project, Access, and Power Point that will be used for ES development, editing documents, configuration control and training by NICSD personnel.

Table 8-1 Systems and Tools for Project Management and Engineering

System/Tool Name	Application
NUPDM2 (Controlled by NED)	For engineering communication and electronic document delivery between NED, NICSD and PPDD.
Toshiba Document Portal (Controlled by NED)	For browsing the NED documents
Customer Portal (If required by the customer)	For submitting documents to the customer, and for checking the document review and approval status
GENESIS	CAD used for drawing ECWD and other schematic

The NICSD SD Team shall control software tools used for project management in accordance with NQ-2003 (Reference (25)). The tools used during testing shall be specified in each test plan and specification, and evaluated prior to use in accordance with Software Test Plan prepared by the IV&V Team.

8.1.2 Software Development Tool Control

The software tools shown in Table 8-2 are used for the software design, development, and implementation of FPGAs. These software tools are categorized as SIL2 software.

Table 8-2 Software Development Tools

System/Tool Name	Application
Synplify® Tool	The Synplify® tool synthesizes logic from VHDL source codes and produces netlists. As by-products of logic synthesizing, Synplify® performs syntactic check of the VHDL source codes and adequacy check of the synthesized logic.
Netlist Viewer tool	The Netlist Viewer tool depicts the logic block diagrams according to the netlists. The Netlist Viewer tool is used to inspect the netlist to ensure the correct conversion of the logic, i.e. ensure that functional elements (FEs) are correctly connected in the netlists. The Netlist Viewer tool is integrated as a function in the Actel Libero® tool, which is an FPGA development package.

System/Tool Name	Application
Designer tool	The Designer tool is a layout tool. It converts gate-level netlists into a fusemap file. To generate the fusemap file, the Designer tool determines which cells in an FPGA chip are to be used, and makes connections to obtain the desired circuit defined by the netlist. The Designer tool also generates gate-level delay information that the ModelSim® tool uses for simulation.
ModelSim® tool	ModelSim® tool is used for simulation of an FPGA using the gate-level netlists and gate-level delay information generated by Designer tool, for generation of test signals for the PinPort device to test FPGAs, and for measurement of the toggle coverage rate for given test vectors.
Silicon Sculptor tool	Silicon Sculptor tool embeds fusemaps generated by the Designer tool on the FPGA chips.
PinPort device	The PinPort device has a small computer system interface (SCSI), which is connected by a SCSI cable to a personal computer containing the ModelSim® tool. For each test, the ModelSim® tool generates inputs to, and monitors outputs from, the FPGA chip. For this testing, the FPGA chip is mounted in a socket in the PinPort device.

* In the job order to PPDD, the NICSD SD Team identifies the version of the software tool that shall be used.

The NICSD SD Team shall control the software tools used for the software design, development, and implementation of FPGAs in accordance with NQ-2034 (Reference (37)). As described in NQ-2034, in the case that a supplier of FPGA-based components is required to control these software tools, NICSD shall evaluate that the supplier has a procedure equivalent to NQ-2034 and the supplier controls the software tools appropriately.

PPDD uses the controlled software tools for software development. PPDD controls the software tools in accordance with E-68020 (Reference (50)). The NICSD SDL shall be responsible for evaluating the PPDD software tool control before issuing a job order to PPDD. The NICSD SD Team shall evaluate how PPDD controls the software tools through a Critical Digital Review (CDR) or Commercial Grade Survey (CG Survey), and will approve PPDD to use these tools for FPGA products in procurement document to PPDD. The NICSD IV&V Lead shall be responsible for review of software tool evaluation documentation provided by PPDD. When conducting the CDR, the NICSD SD Team shall issue the CDR report including the result of evaluation. The CDR report shall be approved by NICSD PM. NICS-QA shall conduct a CG Survey when required by the NICSD SD Team, and prepare a CG Survey Report. The NICSD SD Team shall prepare or update the Preliminary Technical Evaluation Report (PTER) as software tool report to reflect the result of evaluation.

When PPDD requests to change the version of software tools after job ordering, the NICSD SDL requires the NICSD IV&V Team to review the software tool evaluation documentation provided by PPDD. The NICSD IV&V Team shall document the review result in a NICSD V&V Report (NICSD VVR). After the successful review by the NICSD IV&V Team, the NICSD SDL approves the use of new version software tools. The NICSD SD Team shall update the PTER, or finalize the PTER as the Final Technical Evaluation Report (FTER) as software tool report to reflect the result of additional evaluation.

The following tool evaluation documents by PPDD shall be reviewed by the NICSD IV&V Team, and approved by NICSD SD Team.

- Software Tool Information Sheet
- Installation Verification Sheet
- Installation Verification Test Specification

- Installation Verification Test Report
- Error Notice Evaluation Sheet (if any)

All tool evaluation documents shall be treated as quality records. All software development tools and all tool evaluation documents shall be placed under configuration management in accordance with the NICSD SCMP (Reference (56)).

The IV&V Lead shall review the PTER and FTER, and issue a Design Verification Report (DVR). The NICSD SQAL shall accept the PTER and FTER through reviewing the DVR prepared by the IV&V Lead. Finally, the PTER and FTER shall be approved by the NICSD PM. The PTER and FTER as a software tool report shall contain:

- Unique tool identification (e.g., software name and version)
- Purpose of the support tool
- Acceptance criteria
- Verification methods
- An evaluation of the acceptability of the software tool for its intended use

The PTER, FTER and other documentation on the support tool shall be included in the CGD Package.

After the approval by NICSD, PPDD can use these software tools for their software development. Some of these software tools controlled by PPDD such as Netlist Viewer are also used by NICSD IV&V activity. The software tools used by NICSD IV&V activity shall be specified in the NICSD VVP (Reference (57)). TDMS, under PPDD and NICSD oversight, uses the Silicon Sculptor tools to embed the FPGA logic into the FPGA integrated circuit, which will later be mounted on the printed circuit board.

The Microsemi Corporation (formerly Actel Corporation) supplies FPGAs and software tools. Microsemi publishes several types of notifications, including product change, product discontinuation, as well as general customer notifications. In the job order to PPDD, the NICSD SD Team requires PPDD to receive these notifications by email or by registering in the Customer Portal at the Actel web site. In addition, the NICSD SD Team requires PPDD to evaluate customer notifications before applying software tools to actual design work. When error notifications are distributed by Microsemi, PPDD evaluates the error notices to identify possible problems in using the software in the FPGA design as well as the possible problems in materials already shipped to customers. If potential problems are identified, the PPDD engineer documents the results from this evaluation in an Error Notice Evaluation Sheet and submits to NICSD for review. If potential problems are identified for developed or manufactured FPGA products, NICSD engineers file a Design Change Technical Report in accordance with NICSD procedure NQ-2035 "Procedure for Design Change Control" (Reference (38)), and contact NED for review and support.

In addition, if NICSD considers necessary from a technical point of view, the NICSD SD Team will perform a CDR of the Actel (Microsemi) toolset and Actel development practices before applying software tools to actual design work, with support from NED.

8.2 Software Documentation

Documentation is part of the life cycle phase outputs described in Table-A.

8.3 Secure Development and Operational Environment

The NICSD PM shall require the NICSD SDL, and other leads to ensure the existence of and

compliance with the requirements for a Secure Development and Operational Environment (SDOE). NICSD shall take appropriate measures for SDOE in accordance with NQ-2037 "Cyber Security Procedure of Safety Related Digital System" (Reference (40)). The NICSD IV&V Team shall perform security assessment in each life cycle phase, and document the assessment result in NICSD VVRs in accordance with the NICSD VVP (Reference (57)).

The design documents, code, records and all other work products associated with the FPGA systems shall be protected in accordance with Toshiba Information Security Rules and Guidelines (ISRGs) in a manner that shall not compromise the security of the digital systems, other systems, or the plant. The NICSD PM shall require the NICSD SDL, other leads and managers to implement SDOE in accordance with the project cyber security plan and the ISRGs listed in Table 8-1 of NED SMP (Reference (3)). The Toshiba ISRGs mandate application of security measures including access control using password, anti-theft device, hard disk encryption, and anti-virus software. The security information critical to SDOE shall not be combined with software life cycle output documents and records information.

For electronic document control system used by NICSD [ ]d the NICSD PM shall be responsible for registration of users to the system, and supervision of access control to the systems.

The NICSD PM, NICSD SDL, and other leads shall be responsible for ensuring that team members are cleared for access, as necessary, or coordinate with the appropriately cleared Cyber Security Team who already has access to cyber security information.

9 Work Packages, Schedule, and Budget

As described in Section 5.2.1, the NICSD PM is responsible for management of the schedule and budget through the life cycle.

- Deliverable lists (Project Control Document List (PCDL))

  The NICSD SDL registers the updated PCDL on [ ]d so that the NICSD PM can confirm the project deliverables are issued timely.

- NICSD Engineering Schedule (NICSD ES)

  The NICSD SDL registers updated NICSD ES on [ ]d so that the NICSD PM can confirm the project progress.

- Budget plan necessary for human and other resources

  The NICSD SDL, NICSD IV&V Lead, NICSD SSL, and NICSD SQAL shall control the cost using [ ]d

The NICSD ESs shall be planned considering dependencies on each work, and be consistent with the SES prepared by NED. If the SES is changed, the NICSD ESs shall be changed appropriately. The NICSD PM shall require the NICSD SDL other leads to plan the assignment of engineers for the project, and preparation of development tools and facilities.

For V&V activities, the NICSD PM ensures independence of the NICSD IV&V Team in assignment and its budget.

The development process with a detailed breakdown of interfaces and activities is defined in Section 13 "Software Development Plan".

10 Baseline Review and Disposition of Nonconformance

The NICSD IV&V Team shall perform baseline reviews at the end of each phase, and complete the phase activities in accordance with the NICSD VVP (Reference (57)).

Each baseline review confirms disposition of design, documentation, and test nonconformances identified during the phase. The software safety, and verification and validation work product is reviewed in the baseline reviews. The NICSD IV&V Team shall document the result of a baseline review in a Baseline Review Report (BRR). The NICSD SQA Team group shall review the BRR.

In the case of delay in design documentation or specific project task, a responsible lead shall hold an adjustment meeting calling other leads and managers as needed to discuss measures against the project delay before holding a baseline review meeting. In the adjustment meeting, the leads and managers shall determine whether to reschedule the baseline review meeting or not. Multiple meetings for baseline review in a lifecycle phase to separately review project outputs can be scheduled if an agreement by the leads and managers in the adjustment meeting. The NICSD SDL shall update the NICSD ES to reflect the schedule change, and get approval from the NICSD PM.

The NICSD PM shall attend the baseline review meetings to monitor the performance of the work against the NICSD ES from a managerial point of view. In the baseline review meetings, discussions shall cover the details on baselines as well as more systematic activities such as resource allocation, schedule progress status, impact on schedule, and countermeasures to be taken.

The baseline review conducted in the Design Phase is served as a hold point to start the procurement of equipment.

The NICSD SQAP (Reference (55)) shall describe the method to dispose of nonconformances. The NICSD IV&V Team shall report nonconformances occurred and disposition of the nonconformances in a NICSD VVR.

11 Use of Previously Developed or Purchased Software

11.1 Identification of Previously Developed Software (PDS) and Commercial-off-the-Shelf (COTS)

NICSD purchases the modules comprising the FPGA-based equipment from PPDD. The FPGA logics embedded in FPGA on the module printed circuit board are designed and tested by PPDD under their ISO 9001 QA program. NICSD treats the FPGA logics as PDS and dedicates the FPGA logic for FPGA based safety-related application under the NICSD CGD process (see Section 13). NICSD does not modify or customize the FPGA logics procured from PPDD. The evaluation process for the FPGA logic under NICSD CGD process is described in Section 11.2.1.

The FPGA logic is comprised of combinations and connections of software elements called functional elements (FEs). PPDD, under their ISO 9001 Program, has designed, verified, and registered all standard, reusable FEs required for an FPGA logic development. The FEs are treated as COTS, registered in the FE library, and controlled by PPDD. PPDD procedure E-68018 (Reference (48)) describes the process followed by PPDD to develop FEs. The evaluation process for the FEs under the NICSD CGD process is described in Section 11.2.2. Modifications to the FEs are not planned for a specific project purpose. In the case that the design changes are required to FPGA-based safety-related system, NICSD shall evaluate the contents of each design change in accordance with NQ-2035 (Reference (38)) to determine

whether new development of FEs are necessary. If new FE development is necessary as the result of design change evaluation, NICSD shall instruct PPDD to develop new FEs, and evaluate the new FEs. The supplemental evaluation shall be performed for the new FEs in a manner described in Section 11.2.2. The evaluations required in Section 11.2.2 shall be applied to the existing FEs.

11.2 Evaluation of FPGA logic and FEs

11.2.1 Evaluation of FPGA logic

As described in Section 6.2, NICSD dedicates the FPGA logic implemented in FPGA under the NICSD CGD process. NICSD shall evaluate PPDD before ordering to PPDD as described in Section 13.2.8 during the Requirements Definition Phase. The NICSD shall perform independent review and safety analysis for the PPDD documents, and approve prior to incorporation into the design as described in Sections 13.3 through 13.5. NICSD shall summarize the result of dedication as described in Section 13.6.

The followings task shall be performed through the NICSD software safety analysis in Sections 13.3.9, 13.4.7 and 13.5.10.

- Evaluate the software quality assurance and software safety requirements applied in the FPGA logic development comparing with the NICSD SQAP requirements and software safety plan in the NICSD SMP. The evaluation shall determine whether the requirements are met or additional V&V activities are needed.
- Review the requirements and V&V activities performed in development of the FPGA logic. Any additional requirements or verification activities needed for the intended application shall be identified.

The result of evaluation shall be documented in the NICSD SSAR for each phase.

The following tasks shall be performed through the evaluation.

- Review the operating history of the product.
- Identify and review any relevant problem reports and their disposition. Ensure there are no unresolved problems that may affect the safety function of the intended application.
- Review the development process documentation and identify differences between available documentation and that required for the application.

After conducting the CDR, the NICSD SD Team shall issue a CDR report including the result of evaluation. The CDR report shall be approved by NICSD PM. NICS-QA shall conduct a CG Survey when required by the NICSD SD Team, and prepare a CG Survey Report.

The NICSD SD Team shall prepare or update the Preliminary Technical Evaluation Report (PTER) to reflect the result of evaluation. If the evaluation acceptance criteria are not met, the FPGA logic should be re-engineered and re-evaluated. The supplemental activities and documentation shall be verified in a manner described above. The NICSD SD Team shall update the PTER, or finalize the PTER as the Final Technical Evaluation Report (FTER) to reflect the result of additional evaluation.

The PTER and FTER, at a minimum shall:

- Identify the FPGA logics.
- Describe the function of the FPGA logics and previous applications.

- Describe the evaluation processes and acceptance criteria applied.
- Any deviations or deficiencies found in the review process.

The NICSD SSAR, CDR Report, and CG Survey Report shall also provide above information.

The IV&V Team and the NICSD SSL shall review the PTER and FTER prior to the FPGA logic being incorporated into the design.

The PTER, FTER and any other applicable documentation, including plans, reviews, and other documentation associated with re-engineering, shall be included in the CGD Package prior to being incorporated into the design, and shall be stored as a permanent quality record. The CGD Package shall be provided to the customer.

11.2.2 Evaluation of FEs

The FEs shall be evaluated to ensure it meets the quality level required prior to incorporation into the design.

The NICSD SD Team and the NICSD IV&V Team with support from the NICSD SQA Team shall perform an evaluation of FEs. The NICSD SS Team shall participate in the evaluations. The NICSD SD Team, NICSD IV&V Team, and NICSD SS Team shall ensure completion, documentation, and maintenance of these evaluations.

As required in Section 4.3.11 of the SPP (Reference (2)), the NICSD VVP (Reference (57)) shall identify the methods used to verify and document that FEs are of appropriate quality for use, based on the evaluations performed in this section.

The NICSD SD Team shall perform the evaluation of FEs as a part of preliminary technical evaluation activity described in Section 13.1.7 (2). If supplemental requirements for FEs are necessary, the NICSD SD Team shall add the supplemental requirements to procurement document to PPDD.

The evaluation process shall include the following activities:

- Review of development process and its documentation
- Review of the FEs (e.g., adherence to accepted coding practices, internal consistency, and readability)
- Review of the qualification and experience of personnel involved in design and verification
- Review of the supplier software quality assurance program
- Review of the supplier configuration control program
- Review of the product operating history
- Review of the reported problems and their dispositions to ensure they do not impact the safety function of the application

The result of the evaluation process shall be captured in a Preliminary Technical Evaluation Report (PTER). The report shall:

- Identify the FEs, using configurations and version numbers as applicable
- Describe the FEs function
- Describe the evaluation processes and acceptance criteria applied
- Any deviations or deficiencies found in the review process
- Intended application of the FEs within the design

The NICSD SD Team shall generate the PTER. The NICSD IV&V Lead and NICSD SSL shall review the PTER. The PTER and the documentation associated with CGD activity shall be included in the CGD Package and shall be filed in the permanent quality records. The CGD

Package shall be provided to the customer.

In the case that the evaluation acceptance criteria are not met, the FEs shall be re-engineered and re-evaluated. The supplemental activities and documentation shall be verified in a manner described above.

The FPGA Design Specification identifies the logic to be implemented in the FPGA. PPDD uses this information to match the logic with the FEs available in the library. If the FEs required for the FPGA logic are not in the library, PPDD may develop new FEs. In the case that the use of new FEs is suggested by PPDD, the supplemental evaluation shall be performed in a manner described above.

11.3 Software Coding Conventions and Guidelines Document Review

The NICSD SD Team shall perform a review of software coding conventions and guidelines document provided by PPDD as a part of preliminary technical evaluation activity described in Section 13.1.7(2). If supplemental requirements for software coding conventions and guidelines document provided by PPDD are necessary, the NICSD SD Team shall add the supplemental requirements to procurement document to PPDD.

The software coding conventions and guidelines document shall establish the software coding practices to be followed in the implementation of software design. The guideline document shall provide coding practices that will result in readable, consistent, correct, maintainable, reliable, and efficient VHDL source code. The guidelines shall be programming language or development platform specific.

The guidelines provided shall include:

- Code formatting guidelines
- Commenting guidelines
- Techniques for declaration and naming of variables
- Technology specific coding practices to be applied as well as practices to be avoided
- Coding practices to include maintainability, readability, robustness, calculations, timing dependability, and traceability
- In-code comment documentation formatting and required content
- Code version tracking practices, including change identification within the code
- Architectural practices to be avoided
- Other coding guidance specific to the FPGA technology

11.4 Software Coding Readiness Review

The NICSD SD Team shall perform a software coding readiness review during the oversight of DRM for FPGA design review as described in Section 13.3.8.

This review ensures:

- The software development team is familiar with the Module Design Specification (MDS), FPGA Design Specification, and software coding conventions and guidelines document.
- Software tools needed for development are evaluated, approved, under configuration control, and available for use.
- FEs are evaluated and approved under configuration control, and available for use.

The review result shall be documented in a PTER. The NICSD SD Team shall update the PTER.

12 Requirements Traceability Matrix

Requirements Traceability Matrices (RTMs) shall be prepared for FPGA based safety-related software design outputs. The RTMs shall be updated at the end of each life cycle activity group. The RTM shall provide traceability, verification, and validation of requirements. The NICSD SD Team shall prepared the RTM. The NICSD IV&V Team shall review the RTM in accordance with the NICSD VVP (Reference (57)).

13 Software Development Plan

AS-200A128 "Digital System Life Cycle Procedure" (Reference (19)), defines a life cycle process that NED follows in digital systems development. For FPGA-Based safety-related systems, the life cycle phases of AS-200A128 are used with a modification that divides the Validation Testing Phase into the Module Validation Testing Phase and the System Validation Testing Phase. Table 13-1 maps the life cycle phases of the BTP 7-14 (Reference (5)), IEEE 1012 (Reference (7)), SPP (Reference (2)), AS-200A128, and the FPGA-Based systems.

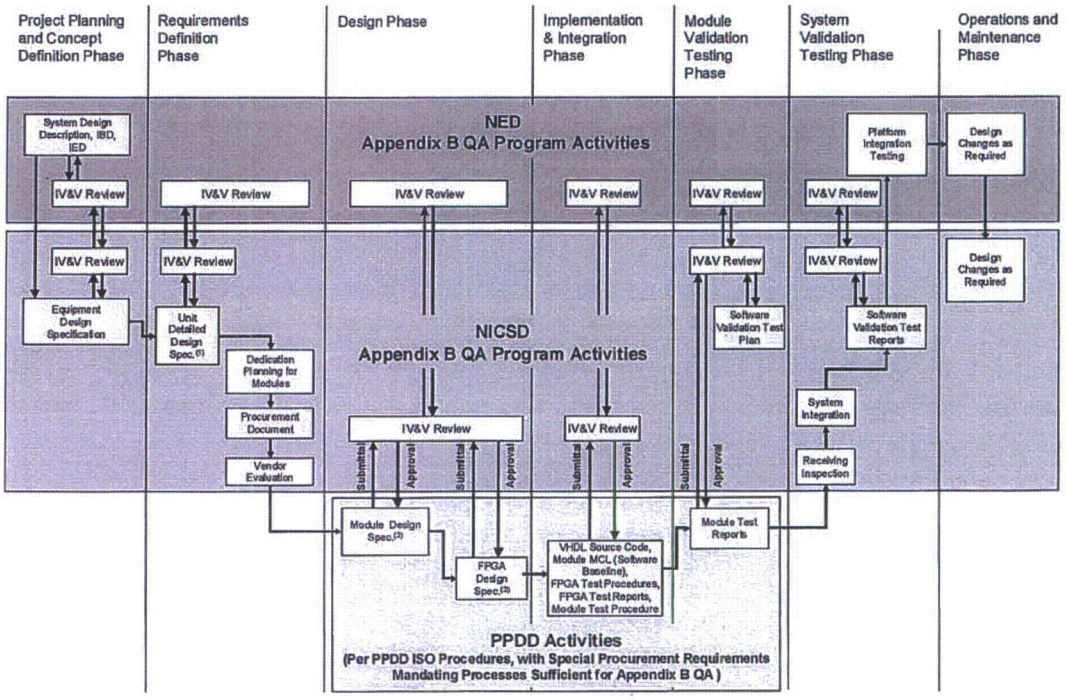
Table 13-1 Mapping of Life Cycle Phases

BTP 7-14	IEEE 1012	SPP	AS-200A128	FPGA-Based Systems
Software Life Cycle Process Planning	Planning	Planning	Project Planning and	Project Planning and
Requirements	Concept		Concept Definition	Concept Definition
	Requirements	Requirements	Requirements Definition	Requirements Definition
Design	Design	Design	Design	Design
Implementation	Implementation	Implementation	Implementation and Integration	Implementation and Integration
Integration				
Validation	Test	Testing and Integration	Validation Testing	Module Validation Testing
				System Validation Testing
Installation	Installation and Checkout	Installation	N/A	N/A
Operations and Maintenance	Operation	Operation	Operations and Maintenance.	Operations and Maintenance.
	Maintenance	Maintenance		
Not included	Retirement	Retirement	Retirement	Retirement

Note 1: FPGA based system uses Non-Rewritable FPGA, one-time programmable devices. Because FPGA logic is implemented and fixed as physical contacts in the chips, there is no need for software installation.

Figure 13-1 shows a simplified diagram of the process flow through the lifecycle phases for the FPGA-Based systems. After NICSD receives the design input from NED, NICSD performs the Project Planning and Concept Definition Phase and Requirements Definition Phase activities

under NICSD Appendix-B QA program (Sections 13.1 and 13.2). During the Requirements Definition Phase, NICSD conducts a vendor evaluation before ordering from PPDD (Section 13.2.8). NICSD oversees the PPDD activities from Design Phase through Module Validation Testing Phase. Detail NICSD involvement with PPDD activity is described in the subsections in Sections 13.3 through 13.5. After NICSD receives the modules from PPDD, NICSD integrates FPGA-Based systems and conducts System Validation Testing (Section 13.6). System Validation Testing can be combined with factory acceptance testing and Platform Factory Test (PFT). Detailed test plan is defined in the Software Test Plan. After the System Validation Testing, NICSD ships the FPGA-Based systems for plant installation or a Platforms Integration Test (PIT) if the PIT is planned for overall project.



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

Figure 13-1 Lifecycle Process for FPGA-based Systems

The following sections describe activities of NICSD and PPDD in the life cycle phases used in development of the FPGA-based safety-related systems. The phases identified are consistent with the FPGA-Based system lifecycle defined in Table 13-1. The detailed design process flow is delineated in the following subjections.

The outputs from each phase of software life cycle shall be controlled as Configuration Items (CI). All CI shall be controlled in accordance with the NICSD SCMP (Reference (56)). Any discrepancies or deficient conditions found in a CI shall be resolved in accordance with the corrective action process in NICSD SQAP (Reference (55)), and the change control process in the NICSD SCMP.

When a design document or portion of a design cannot be completed prior to release for

verification and validation, such as a To Be Determined (TBD) requirement or an assumption, conditional release of the document is permissible. The portions of the document that cannot be verified shall be controlled in accordance with the method described in the NICSD VVP (Reference (57)). Documents that have incomplete requirements shall be tracked, and, at the earliest opportunity, the document shall be completed, reviewed, and approved in accordance with the method described in the NICSD VVP. All Conditional Releases shall be resolved prior to FPGA logic design can complete.

13.1 Project Planning and Concept Definition Phase

In the Project Planning and Concept Definition Phase, system design requirements and software development plans are addressed.

13.1.1 Project Planning and Concept Definition Phase Inputs

Regulations and regulatory guidance specified in the NED documents attached to the NED Job Order Sheet are input to the planning phase throughout the plant life cycle.

The System Design Description (SDD), Instrumentation Electrical Diagram (IED), Interlock Block Diagram (IBD), NED SMP (Reference (3)), NED V&V Plan (NED VVP) (Reference (54)), procurement specification, and other technical and quality assurance requirement documents attached to the NED Job Order Sheet are the design inputs to NICSD for the Project Planning and Concept Definition Phase.

The NICSD SD Team shall prepare the Design Input Sheet (DIS) to identify the design inputs for the project in accordance with AS-200A014 "Procedure for Documentation of Design Inputs" (Reference (17)).

13.1.2 Process Review Meeting (PRM-B0)

After the identification of the design inputs is finished, a PRM is convened, as described in Section 7.3.3(3).

13.1.3 Project Planning and Concept Definition Phase Outputs

Table-A lists the NICSD outputs of the Project Planning and Concept Definition Phase.

13.1.4 Plans for Software Design Process

- The NICSD SD Team shall prepare a NICSD SMP (this document) to satisfy the requirements specified in Sections 1, 2, 3, 6, and 10 of the SPP (Reference (2)).
- The NICSD SD Team shall prepare a NICSD SCMP to satisfy the requirements specified in Section 7 of the SPP.
- The NICSD SQA Team shall prepare a NICSD SQAP which defines the software quality assurance requirements and the configuration management requirements to satisfy the requirements specified in Section 5 of the SPP.
- The NICSD IV&V Team shall prepare a NICSD V&V Plan (NICSD VVP) to satisfy the requirements specified in Section 4 of the SPP.
- After the Equipment Design Specification (EDS) is established, including approval of the

customer if necessary, the NICSD IV&V Team shall prepare a Software Test Plan to satisfy the requirements specified in Section 9 of the SPP.

- After the Equipment Design Specification (EDS) established, the NICSD SD Team shall prepare a Master Test Plan (MTP) which describes the whole test plan for the FPGA testing, Module Validation Testing, System Validation Testing, Equipment Qualification test, EMC test and other functional tests.

The NICSD SMP, SCMP, SQAP, VVP and Software Test Plan shall be reviewed and approved by customer if necessary.

13.1.5 Process Review Meeting (PRM-B1)

After the planning documents are prepared, a PRM is convened, as described in Section 7.3.3(3).

13.1.6 Equipment Design Specification (EDS)

Based on the SDD, IBD, and IED, the NICSD SD Team shall prepare an EDS that breaks down the system level requirements into the equipment design requirements, and defines the specification of the FPGA-based equipment in accordance with NQ-2004 "Preparation Procedure for Equipment Design Specification" (Reference (26)).

The EDS includes the elements of System Architecture Description (SAD) and Software Interfaces Document (SID) which is required as output of Requirements Definition Phase in Sections 3.10.3.3 and 3.10.3.4 of the SPP (Reference (2)), respectively.

13.1.7 CGD Preparation

(1) CGD Plan.

The NICSD SD Team shall prepare a CGD Plan for FPGA-based system to describe the plan for dedicating the commercial grade items comprising the equipment in accordance with AS-200A110 (Reference (18)). The CGD Plan is called a dedication plan in AS-200A110. The CGD Plan also documents methods for safety classification of system, and describes the activities required for the dedication of the commercial grade items and services.

(2) Preliminary Technical Evaluation Report (PTER)

The NICSD SD Team shall prepare a PTER for each FPGA-based system to document safety classification of system, and identify Critical Characteristics for Design (CCD) typically applicable to components comprising system (i.e. whole component) in accordance with AS-200A110. The PTER also identifies Critical Characteristics for Acceptance (CCA) and acceptance methods as an acceptance plan that provides acceptance process typically applicable to components comprising system.

The NICSD SD Team shall perform the evaluation of FEs as a part of technical evaluation activity described in Section 11.2.2.

The NICSD SD Team shall perform a review of software coding conventions and guidelines document provided by PPDD as a part of technical evaluation activity described in Section 11.3.

(3) Procurement Planning Sheet (PPS)

The NICSD SD Team shall prepare PPS to schedule the procurement and vendor evaluation activities in accordance with AS-200A008 "Procurement Planning Procedure" (Reference (16)).

13.1.8 Software Safety Analysis

The NICSD SS Team shall prepare a NICSD SSAR as described in Section 14.

13.1.9 Requirements Traceability Matrix

As described in Section 12, the NICSD SD Team updates the RTM delivered by ICDD to maintain the traceability between the ICDD requirements and the EDS. The NICSD IV&V Team shall review the RTM in accordance with the NICSD VVP (Reference (57)).

13.1.10 Configuration Management Assessment

The NICSD SD Team generates the NICSD Master Configuration List (NICSD MCL) and conducts the configuration management assessment to ensure the followings in accordance with the NICSD SCMP (Reference (56)).

- All phase activities are completed on the required outputs
- Adequacy of activities in accordance with applicable procedures and the NICSD SCMP.
- Appropriate configuration controls (according to the NICSD SCMP) are in place to monitor design activities including document revision and track changes control.

13.1.11 Verification and Validation

The NICSD IV&V Team shall prepare a NICSD VVR in accordance with the NICSD VVP (Reference (57)).

13.1.12 Process Review Meeting (PRM-B2)

After the planning activities described above sections are finished, a PRM is convened, as described in Section 7.3.3(3).

13.1.13 Baseline Review and Disposition of Nonconformance

As described in Section 10, the NICSD IV&V Team performs a baseline review, and issues a BBR in accordance with the NICSD VVP (Reference (57)).

13.2 Requirements Definition Phase

In the Requirements Definition Phase, implementation of equipment design requirements and configuration requirements are addressed.

13.2.1 Requirements Definition Phase Inputs

The documents developed by NICSD in the Project Planning and Concept Definition Phase are inputs for the Requirements Definition Phase.

13.2.2 Requirements Definition Phase Outputs

Table-A lists the NICSD outputs of the Requirements Definition Phase.

13.2.3 Unit Detailed Design Specification (Unit DDS)

A Unit DDS is provided as Software Requirements Specification (SRS) for each specific unit which comprises the FPGA-based equipment. The Unit DDSs also include the hardware requirements specification. This specification includes communication links and interfaces with other units and external systems, providing the external communication link and interfaces documentation.

The NICSD SD Team shall prepare the Unit DDS in accordance with NQ-2005 "Preparation Procedure for Detailed Design Specification" (Reference (27)).

13.2.4 Equipment Schematic

The NICSD SD Team designs hardware connections in system based on the IBDs, IEDs, EDS, and Unit DDSs. The NICSD SD Team prepares an Elementary Control Wiring Diagram (ECWD) in accordance with NQ-2017 (Reference (30)) to define detailed hardware connections of the FPGA-based equipment.

13.2.5 Equipment User's Manual

The NICSD shall prepare a unit user's manual for each of unit comprising the FPGA-based equipment with reference to PPDD design.

13.2.6 Data Communication Protocol

The EDS prepared in the previous phase and the Unit DDS define the data communication protocol. The data communication protocol shall define the external system communication interfaces to the FPGA-based equipment, identify and define each external communication interface, message structure, format, and sequence. The data communication protocol shall:

- Identify and define communications between safety channels, between safety divisions, and between safety-related software and nonsafety related software, to ensure communications independence, such that communication malfunctions will not interfere with the execution of the safety function.
- Incorporate the SDOE security requirements, based on Section 8.3.

13.2.7 CGD Preparation

As described in Section 6.2, NICSD procures and dedicates the modules for the FPGA-based system under the NICSD CGD process. During this phase, the NICSD SD Team develops a technical specification and a QA specification for PPDD, which are included in the Job Order to PPDD.

(1) Commercial Dedication Instruction (CDI)

The NICSD SD Team shall prepare a CDI for each module type comprising part of unit in accordance with NQ-4001 (Reference (45)). This document identifies the specific Critical Characteristics for each module type, technical evaluation, acceptance plan that includes acceptance criteria, and methods for acceptance for the items. The acceptance methods identified in the CDI are reflected in the procurement document or the receiving inspection procedure for the item and service.

(2) Procurement Document

The NICSD SD Team shall prepare a procurement document for each module type comprising part of unit in accordance with NQ-2025, "Preparation Procedure for Procurement Document for CG Items & Services" (Reference (32)).

The procurement document includes the technical requirements and QA requirements. The technical requirements are the applicable design requirements for the modules derived from the Unit DDS. The QA requirement identifies applicable quality assurance requirements for the commercial grade items provided by PPDD.

The procurement document to PPDD shall identify the procedures to be followed by PPDD for building software. PPDD has the following development procedures for commercial grade item development. The applicable revision of the following procedures identified through the vendor evaluation described in Section 13.2.8 shall be specified in the procurement document to PPDD.

- "PPDD Procedural Standard for FPGA Products Development," E-68016 (Reference (46));
- "PPDD Procedural Standard for FPGA Device Development," E-68017 (Reference (47));
- "PPDD Procedural Standard for Functional Element Development," E-68018 (Reference (48));
- "PPDD Procedural Standard for FPGA Configuration Management," E-68019 (Reference (49)); and
- "PPDD Procedural Standard for Control of Software Tools for FPGA-based Systems," E-68020 (Reference (50)).

13.2.8 Vendor Evaluation

The NICSD SD Team shall conduct a vendor evaluation with support from the NICSD IV&V Team, SQA Team, SS Team, and NICS-QA. The evaluation shall be conducted before issuing the Job Order to PPDD.

The followings shall be evaluated at a minimum.

- PPDD's control over the critical characteristics identified in the PTER, or CDIs.
- Evaluation of software development tools as described in Section 8.1.2
- Evaluation of FPGA logic as described in Section 11.2.1
- Evaluation of PPDD procedures for using a Libero tool ensuring that only approved codes are included in fusemap, and FPGA logic does not contain any undocumented code or

configuration as described in Section 13.4.10.

- PPDD's control over the personnel qualification for FPGA development and testing as described in Section 15.

13.2.9 Software Safety Analysis

The NICSD SS Team prepares a NICSD SSAR as described in Section 14.

13.2.10 Requirements Traceability Matrix

As described in Section 12, the NICSD SD Team updates the RTM to maintain the traceability between the EDS and the unit design. As described in Section 12, the NICSD IV&V performs independent review of the RTM in accordance with the NICSD VVP (Reference (57)).

13.2.11 Configuration Management Assessment

The NICSD SD Team shall update the NICSD MCL, and conduct the configuration management assessment to ensure the following in accordance with the NICSD SCMP (Reference (56)).

- All phase activities are completed on the required outputs
- Adequacy of activities in accordance with applicable procedures and the NICSD SCMP.
- Appropriate configuration controls (according to the NICSD SCMP) are in place to monitor design activities including document revision and track changes control.

13.2.12 Verification and Validation

The NICSD IV&V Team shall prepare a NICSD VVR in accordance with the NICSD VVP (Reference (57)).

13.2.13 Process Review Meeting (PRM-C1)

After the above activities are finished, a PRM is convened, as described in Section 7.3.3(3).

13.2.14 Baseline Review and Disposition of Nonconformance

As described in Section 10, the NICSD IV&V Team performs a baseline review and issues a baseline review report in accordance with the NICSD VVP (Reference (57)).

13.3 Design Phase

In the Design Phase, design of software architecture, program structure elements, and software module (i.e. FPGA logic) functions are addressed.

13.3.1 Design Phase Inputs

The documents developed in the Requirements Definition Phase are inputs for the Design Phase.

13.3.2 Design Phase Outputs

Table-A lists the NICSD outputs of the Design Phase.

13.3.3 Job Order to PPDD

The NICSD SD Team issues a job order to procure the modules from PPDD in accordance with NQ-2025 (Reference (32)). In the job order to PPDD, the NICSD SD Team shall specify the version of the software tool that can be used for FPGA products.

13.3.4 Module Design Specification (MDS)

The combination of Module Design Specification (MDS) and FPGA Design Specifications fulfill the requirements of the Software Design Description (SwDD) described in Section 3.11.3.1 of the SPP (Reference (2)).

The MDS consists of a combination of the hardware and software detailed design description necessary to define the modules. This specification includes identification of communication links and interfaces with other modules, providing the internal and external communication link specification.

The MDS shall satisfy the requirements identified in the Unit DDS attached to Job Order to PPDD, and provide sufficient detail to allow someone other than the author of the MDS to create, review, and test the module function. The MDS shall translate the software requirements into a description of the software and its structure, software components, interfaces, and data necessary for implementation.

PPDD prepares and submits a MDS to NICSD for review and approval as required in the procurement document attached to Job Order. The NICSD IV&V Team performs independent review for the MDS in accordance with the NICSD VVP (Reference (57)). The NICSD SD Team shall approve the MDS in accordance with NQ-2026 (Reference (33)).

After the Module Design Specification is approved by NICSD, PPDD shall submit a Module Test Procedure which includes test cases and test procedures to NICSD for review and approval as required in the procurement document attached to Job Order to PPDD. The NICSD IV&V Team performs independent review for the Module Test Procedure in accordance with the NICSD VVP (Reference (57)). The NICSD SD Team shall approve the Module Test Procedure in accordance with NQ-2026 (Reference (33)). Module Test Procedure shall be traceable to the MDS using the RTM.

13.3.5 FPGA Design Specification

The FPGA Design Specification consists of a combination of the hardware and software detailed design description necessary to define the FPGAs that will be soldered onto the module printed circuit boards. This specification includes communication links and interfaces with other FPGAs on a given module, providing the internal communication link and interfaces documentation.

The FPGA Design Specification shall satisfy the requirements identified in the MDS approved by NICSD, and provide sufficient detail to allow someone other than the author of the FPGA Design Specification to create, review, and test the FPGA function. The FPGA Design

Specification shall translate the software requirements into a description of the software and its structure, software components, interfaces, and data necessary for implementation.

PPDD can submit an FPGA Design Specification to NICSD for review and approval after the NICSD approval of MDS. The NICSD IV&V Team performs independent review for the FPGA Design Specification in accordance with the NICSD VVP (Reference (57)). The NICSD SD Team shall approve the FPGA Design Specification in accordance with NQ-2026 (Reference (33)).

13.3.6 Intra System Communications and Protocol Specification

The MDS and FPGA Design Specification shall include the Intra System Communications and Protocol Specification (ISCPS) described in Section 3.11.3.2 of the SPP (Reference (2)).

The MDS shall define each communication interface established between the modules.

The NICSD IV&V Team shall review the MDS to ensure that the MDS shall:

- Identify and define each communication interface, message structure, format, and sequence that was not included in the EDS and Unit DDS
- Identify communication interfaces between FPGAs at different safety classification levels and ensure the safety related systems can perform the required safety function or functions when communication errors occur.
- Define response to data loss or communication failures.
- Incorporate the SDOE security requirements, based on Section 8.3.

The NICSD IV&V Team shall review the FPGA Design Specification to ensure that the FPGA Design Specification shall:

- Identify communication interfaces to other FPGAs and external devices.
- Define connection between the FEs
- Incorporate the SDOE security requirements, based on Section 8.3.

13.3.7 Initiation of Software Validation Test Plan (SVTP) Development

The NICSD IV&V Team shall initiate the development of the SVTP for System Validation Testing including test case specification, and development of the testing procedure to satisfy the requirements specified in Section 9 of the SPP (Reference (2)).

The SVTP shall outline the methodology of how various tests will be used to verify that the integrated software meets the requirements stated in the EDS and Unit DDS. The SVTP shall identify environments, cases (including inputs, procedures, outputs, and expected results), resources (including tools, personnel, and equipment), methodologies, and acceptance criteria. The RTM ensures that test documents cover functional requirements in the EDS and Unit DDSs

13.3.8 Design Review Meeting (DRM) Oversight

PPDD convenes Design Review Meetings (DRMs). NICSD confirms that PPDD follows their software development process correctly, and confirms the status of PPDD activities through the oversight of DRMs. For each DRM, a DRM record is prepared to track the issues identified during the meeting.

During this phase, NICSD performs an oversight of the following DRMs.

- DRM for module design review

- DRM for FPGA design review

The NICSD SD Team performs a software coding readiness review during the oversight of DRM for FPGA design review as described in Section 11.4.

13.3.9 Software Safety Analysis

The NICSD SS Team prepares a NICSD SSAR for the FPGA-based safety-related system as described in Section 14.

13.3.10 Requirements Traceability Matrix

PPDD prepares the RTM to maintain the traceability between the module design, FPGA design and the unit design. As described in Section 12, the NICSD IV&V performs independent review of the RTM in accordance with the NICSD VVP (Reference (57)).

13.3.11 Configuration Management Assessment

The NICSD SD Team shall update the NICSD MCL, and conduct the configuration management assessment to ensure the followings in accordance with the NICSD SCMP (Reference (56)).

- All phase activities are completed on the required outputs
- Adequacy of activities in accordance with applicable procedures and the NICSD SCMP.
- Appropriate configuration controls (according to the NICSD SCMP) are in place to monitor design activities including document revision and track changes control.

13.3.12 Verification and Validation

The NICSD IV&V Team shall prepare a NICSD VVR in accordance with the NICSD VVP (Reference (57)).

13.3.13 Process Review Meeting (PRM-C2)

After the above activities are finished, a PRM is convened, as described in Section 7.3.3(3).

13.3.14 Baseline Review and Disposition of Nonconformance

As described in Section 10, the NICSD IV&V Team performs a baseline review and issues a baseline review report in accordance with the NICSD VVP (Reference (57)).

13.4 Implementation and Integration Phase

In the Implementation and Integration Phase, software coding activities and testing activities of individual software module (i.e. FPGA logic) are addressed. Unlike a microprocessor-based system, the FPGA that Toshiba selected for the FPGA-based systems requires software installation to be performed before hardware assembly. There are no provisions for conditional software releases since they are not applicable to FPGA-based technology.

13.4.1 Implementation and Integration Phase Inputs

The documents developed in the Design Phase are inputs for the Implementation and Integration Phase.

13.4.2 Implementation and Integration Phase Outputs

Table-A lists the NICSD outputs of the Implementation and Integration Phase. The outputs are required to include the software baseline.

13.4.3 Software Coding and Coding Review (VHDL Source Code)

PPDD shall write VHDL source code to implement the FPGA design, which includes safety critical functions, consistent with the coding guidelines evaluated by the NICSD SD Team prior to use.

Appendix A of PPDD procedure E-68017 (Reference (47)) requires the FPGA design engineers to use synchronous design techniques, and limits the logic depth between synchronous elements within the FPGA. If the FPGA designers find that an FPGA design cannot meet this requirement, the FPGA designers are required to perform a detailed timing analysis within the FPGA to show that the FPGA design has enough timing margin.

The NICSD IV&V Team shall perform a VHDL source code review and issue a source code review sheet, as required in Sections 3.12.3.2 and 3.12.3.3 of the SPP (Reference (2)) in accordance with the NICSD VVP (Reference (57)).

13.4.4 FPGA Testing

The FPGA testing is performed taking two separate approaches. The first approach uses a VHDL simulator, and the second approach uses a programmed FPGA. Because the system consists of several FPGAs, FPGA logic is considered a "software module" from a software engineering point of view. And the programmed FPGA is considered a hardware part integrated with software. Therefore, the FPGA testing corresponds to the software module testing and the software integration testing.

The FPGA testing, as Software Functional Testing required in Section 3.12.3.4 of the SPP (Reference (2)), shall be performed during this phase to ensure that each FPGA logic satisfies the requirements provided in the design documents, to identify and correct code design errors prior to the System Integration Testing, and to verify that the FPGA logic interfaces properly.

The NICSD IV&V Team performs independent review for the FPGA Test Procedure in accordance with the NICSD VVP (Reference (57)). The NICSD SD Team shall approve the FPGA Test Procedure in accordance with NQ-2026 (Reference (33)).

The FPGA Test Procedure shall outline the methodology of how various tests will be used to verify that the integrated software meets the requirements stated in the FPGA Design Specification. The FPGA Test Procedure shall be traceable to the FPGA Design Specification using the RTM.

PPDD shall perform the FPGA testing in accordance with the test procedures approved by NICSD.

A summary of test activities, including a basis for determining the rigor of testing and the test results, shall be prepared and documented in the FPGA Test Report as a software functional test

report. The NICSD IV&V Team performs independent review of the FPGA Test Report in accordance with NICSD VVP (Reference (57)), and the NICSD SDL approves FPGA Test Report in accordance with NQ-2026 (Reference (33)).

13.4.5 FPGA Implementation

After the FPGA Test Report is reviewed and approved by NICSD, PPDD shall submit electronic media and PPDD Module MCL including the FPGA control sheet, VHDL source code, FPGA logic (fusemap) and related configuration items for review by NICSD deign group. The FPGA control sheet identifies the FPGA configuration items including the FPGA documents, VHDL source code, fusemap, and software development tool version.

The NICSD SD Team shall receive the electronic media and PPDD Module MCL in accordance with NQ-2033 "Procedure for Configuration Management of FPGA" (Reference (36)). The NICSD SD Team shall prepare a master media and copy media, and store the master and copy media in accordance with NQ-2033. The master media and copy media are controlled by NICSD.

The NICSD SD Team shall send an FPGA Logic Implementation Request/Record Sheet and approved FPGA logic (fusemap) to TDMS via PPDD to implement the FPGA logic into the FPGA chip. The fusemap file in the copy media controlled by NICSD is used by TDMS to implement the FPGA logic into the FPGA chip.

The NICSD QC inspector shall witness the FPGA logic implementation into the FPGA by TDMS, and NICSD QC inspector shall check whether the FPGA logic implementation has been carried out correctly by checking a specific checksum indicated on the programming tool.

The FPGAs which passed the inspection are mounted on the printed circuit board and assembled as a module by TDMS. TDMS delivers the module to PPDD.

13.4.6 Design Review Meeting (DRM) Oversight

During this phase, NICSD performs an oversight of the following DRMs.

- DRM for FPGA test planning and specification review
- DRM for FPGA test activity result review
- DRM for module test planning and specification review

The Module Test Procedure shall be approved by the NICSD SD Team before Module Validation Testing no later than the Implementation and Integration Phase.

13.4.7 Software Safety Analysis

The NICSD SS Team prepares a NICSD SSAR for the FPGA-based safety-related system as described in Section 14.

13.4.8 Requirements Traceability Matrix

PPDD prepares the RTM to maintain the traceability between the FPGA Design Specification and the FPGA Test Procedure. As described in Section 12, the NICSD IV&V shall perform independent review of the RTM in accordance with the NICSD VVP (Reference (57)).

13.4.9 Configuration Management Assessment

The NICSD SD Team shall update the NICSD MCL, and conduct the configuration management assessment to ensure the following in accordance with the NICSD SCMP (Reference (56)).

- All phase activities are completed on the required outputs
- Adequacy of activities in accordance with applicable procedures and the NICSD SCMP.
- Appropriate configuration controls (according to the NICSD SCMP) are in place to monitor design activities including document revision and track changes control.

13.4.10 Verification and Validation

The NICSD IV&V Team shall prepare a NICSD VVR in accordance with the NICSD VVP (Reference (57)).

The NICSD VVR for this phase shall include the list of the following documents as the result of the V&V activity of this phase. The following documents satisfy the requirements for Software Build Procedure and Report (SBPR) described in Section 3.12.3.6 of the SPP (Reference (2)). 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. The documents listed below are treated as a quality record and retained for the life of the system.

- Source Code Review Sheet
- FPGA Test Report
- FPGA Control Sheet

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

- Procurement document (Output of Requirements Definition Phase)

  As described in Section 13.2.7 (2), procurement document to PPDD identifies the procedures to be followed by PPDD for software building. The PPDD procedure for using Libero tool shall ensure that only approved codes are used in fusemap, and FPGA logic does not contain any undocumented code or configuration. The evaluation of PPDD procedure is performed as described in Section 13.2.8.

13.4.11 Baseline Review and Disposition of Nonconformance

As described in Section 10, the NICSD IV&V Team performs a baseline review, and issues a baseline review report in accordance with the NICSD VVP (Reference (57)).

13.5 Module Validation Testing Phase

In the Module Validation Testing Phase, PPDD performs Module Validation Testing using the Module Test Procedures.

13.5.1 Module Validation Testing Phase Inputs

The documents developed in the Implementation and Integration Phase and Module Design Specification are inputs for the Module Validation Testing Phase.

13.5.2 Module Validation Testing Phase Outputs

Table-A lists the NICSD outputs of the Module Validation Testing Phase.

13.5.3 Module Validation Testing

PPDD shall perform a module testing in accordance with the Module Test Procedure approved by NICSD.

PPDD shall document the result of the Module Validation Testing in the Module Test Report. The NICSD IV&V Team performs independent review for the Module Test Report in accordance with the NICSD VVP (Reference (57)). The NICSD SD Team shall approve the Module Test Report in accordance with NQ-2026 (Reference (33)).

PPDD shall report any failures in Module Validation Testing to NICSD.

The NICSD IV&V Team shall identify any failures in Module Validation Testing that require changing FPGA logic that has already been tested. These test failures require at least an evaluation of the FPGA testing and repetition of affected tests. Failures that result in logic modification also require repetition of the complete FPGA testing on modified FPGA logic and all interfaces between unmodified and the modified FPGA logic.

13.5.4 Description of As-Tested Software

PPDD shall update and submit the PPDD Module MCL as their software release report to include the identification of the Module Test Report to NICSD. The NICSD SD Team shall review and approve the PPDD Module MCL in accordance with NQ-2033 (Reference (36)). Accordingly, NICSD shall update the NICSD MCL to reflect the PPDD Module MCL updates.

13.5.5 Design Review Meeting (DRM) Oversight

During this phase, NICSD performs an oversight of the following DRM.

- DRM for module testing activity result review

13.5.6 Receiving of FPGA Modules

After Module Test Report is approved by NICSD, PPDD can deliver the modules to NICSD. An NICSD receiving inspector performs receiving inspections in accordance with NQ-3024, "Receiving Inspection Procedure" (Reference (44)).

13.5.7 Process Review Meeting (PRM-E2)

After the above activities are finished, a PRM is convened, as described in Section 7.3.3(3).

13.5.8 System Operations and Maintenance Manual (System O&M Manual)

The NICSD SD Team shall prepare a System Operations and Maintenance (O&M) Manual.

The contents of the System O&M Manual will be based on the requirements documents provided by the costumer.

The System O&M Manual shall satisfy the requirements for the user documentation specified in requirements documents supplied by the customer.

The System O&M Manual shall satisfy the requirements described in Sections 12.4 and 13.4 of the SPP (Reference (2)).

The System O&M Manuals shall provide hardware and system installation instructions. The instructions shall provide sufficient information to install all configuration data into the system or equipment.

The software for the Toshiba FPGA-based safety-related systems can only be replaced by replacing modules in those systems. Therefore, the System O&M Manual shall document procedures for module replacement.

Setpoint data are stored in nonvolatile re-writable memory mounted on modules allowing adjustment in the field. Therefore, the System O&M Manual shall document procedures for setpoint adjustment.

In addition, the System O&M Manual can be used as a System Training Manual described in Section 3.14.3.2 of the SPP. The requirements for the system training manual contents and format will be described in requirements documents provided by customer The System O&M Manual should include training information for supporting FPGA based system maintenance, module replacement, and tools needed for calibration, surveillance, troubleshooting, maintenance as applicable.

13.5.9 Process Review Meeting (PRM-F1)

After the SVTP is prepared, a PRM is convened, as described in Section 7.3.3(3). The SVTP shall be reviewed and approved by the NICSD IV&V Team before System Validation Testing no later than the Module Validation Testing Phase.

13.5.10 Software Safety Analysis

The NICSD SS Team prepares a NICSD SSAR for the FPGA-based safety-related system as described in Section 14.

13.5.11 Configuration Management Assessment

The NICSD SD Team shall update the NICSD MCL, and conduct the configuration management assessment to ensure the followings in accordance with the NICSD SCMP (Reference (56)).

- All phase activities are completed on the required outputs
- Adequacy of activities in accordance with applicable procedures and the NICSD SCMP.
- Appropriate configuration controls (according to the NICSD SCMP) are in place to monitor design activities including document revision and track changes control.

13.5.12 Verification and Validation

The NICSD IV&V Team shall prepare a NICSD VVR in accordance with the NICSD VVP (Reference (57)).

13.5.13 Baseline Review and Disposition of Nonconformance

As described in Section 10, the NICSD IV&V Team performs a baseline review, and issues a baseline review report in accordance with the NICSD VVP (Reference (57)).

13.6 System Validation Testing Phase

13.6.1 System Validation Testing Phase Inputs

The documents developed in the Module Validation Testing Phase, Unit Design Specification, and EDS are inputs for the System Validation Testing Phase.

13.6.2 System Validation Testing Phase Outputs

Table-A lists the NICSD outputs of the System Validation Testing Phase.

13.6.3 System Validation Testing

The System Validation Testing verifies proper functionality of the fully integrated software once installed on the production hardware. The results of System Validation Testing shall be documented in a Software Validation Test Report (SVTR). The NICSD IV&V Team shall prepare the SVTR to satisfy the requirements specified in Section 9 of the SPP (Reference (2)). The testing shall be planned to demonstrate that all safety-related functions identified in the base requirements are operational.

The NICSD IV&V Team shall identify any failures in System Validation Testing that require modification of FPGA logic that has already been tested. Test failures require at least an evaluation of the FPGA testing and repetition of affected tests. Test failures that result in modified FPGA logic require repetition of the complete FPGA testing on the modified FPGA logic and all interfaces between unmodified and modified FPGA logic.

13.6.4 Process Review Meeting (PRM-F2)

After the SVTR is prepared, a PRM is convened, as described in Section 7.3.3(3).

13.6.5 Description of As-Tested Software

After successful completion of the System Validation Testing, NICSD shall update NICSD MCL to include the identification of SVTR.

13.6.6 CGD Package

NICSD CGD activities are summarized in the following documents in this phase.

(1) CGD Report
The NICSD SD Team shall prepare a CGD Report for each module type, unit chassis, cables, and other equipment in accordance with NQ-4001 (Reference (45)). This report contains the list of documents used for dedication activity and acceptance records.

(2) Final Technical Evaluation Report (FTER)
The NICSD SD Team shall prepare a Final Technical Evaluation Report (FTER) for the system in accordance with AS-200A110. This report will summarize the results of CGD activities.

(3) CGD Package
The NICSD SD Team shall prepare a CGD Package in accordance with AS-200A110. This package contains the list of documents used for dedication planning, FTER, CDIs, and CGD Reports.

13.6.7 Software Safety Analysis

The NICSD SS Team prepares a NICSD SSAR as described in Section 14.

13.6.8 Requirements Traceability Matrix

The traceability from the system requirements in the EDS and Unit DDS is ensured by the RTM.

The NICSD SD Team finalizes the RTM to maintain the traceability from the Project Planning and Concept Definition Phase through the System Validation Testing Phase. As described in Section 12, the NICSD IV&V performs independent review of the RTM in accordance with the NICSD VVP (Reference (57)).

13.6.9 Configuration Management Assessment

The NICSD SD Team shall update the NICSD MCL, and conduct the configuration management assessment to ensure the followings in accordance with the NICSD SCMP (Reference (56)).

- All phase activities are completed on the required outputs
- Adequacy of activities in accordance with applicable procedures and the NICSD SCMP.
- Appropriate configuration controls (according to the NICSD SCMP) are in place to monitor design activities including document revision and track changes control.

13.6.10 Verification and Validation

The NICSD IV&V Team shall prepare a NICSD VVR and V&V Report (NICSD VVR) in accordance with the NICSD VVP (Reference (57)).

13.6.11 Final Inspection before Shipping

After System Validation Testing, NICSD QC inspectors perform a final inspection in accordance with NQ-3010, "Inspection Control Procedure" (Reference (42)).

13.6.12 Baseline Review and Disposition of Nonconformance

As described in Section 10, the NICSD IV&V Team performs a baseline review, and issues a baseline review report in accordance with the NICSD VVP (Reference (57)).

13.6.13 Production Release (Shipment)

Once a software build meets the requirements of the System Validation Testing, it shall be released as production software through the baseline review process. A software quality assurance audit shall be performed on the software build as part of the Baseline Review for this phase. The NICSD SD Team shall finalize NICSD MCL as software release report in accordance with NICSD SCMP to satisfy the requirements specified in Section 7.2.3.2 of the SPP (Reference (2)).

13.7 Operations and Maintenance Phase

The Operations and Maintenance Phase begins with the completion of the System Validation Testing Phase.

NICSD shall address any problem occurred after the System Validation Testing, and perform the necessary activities in accordance with AS-200A128 (Reference (19)), which include update of the design documents, NICSD MCL, VHDL source codes, RTM, NICSD SSAR, NICSD VVR, and NICSD VVR. To perform these activities, NICSD shall implement the established software change control procedure in the NICSD SCMP (Reference (56)).

13.8 Retirement Phase

NICSD plans no activity for the Retirement Phase beyond those written in the SPP (Reference (2)).

13.9 Life Cycle Task Iteration Process

The modifications made to any FPGA logic after the completion of System Validation Testing shall be analyzed for appropriate regression testing under the configuration management process described in the NICSD SCMP (Reference (56)).

It should be noted that the use of the lifecycle model includes the nested pass, because development processes frequently need to be iterated. Figure 13-2 shows the concept of nested pass. In the figure, the left arrows indicate the primary pass corresponding to the progress of development process. If a nonconformance is found, e.g. at the Module Validation Testing Phase, the process shall pause at the phase in which nonconformance found. The cause of nonconformance shall be identified, and then corrective actions shall be taken as a nested pass. In the figure the nested pass flows from the Design Phase through the Implementation and Integration Phase, where the activities affected by the corrective actions shall be updated. After the nested pass reach the paused phase, the development process restarts.

When an input document to NICSD is changed, each lead reviews the software plans, procedures, and instructions as described in Section 16. The responsible lead shall evaluate the backfit to existing work products to determine the extent to which tasks shall be repeated as described in Section 16.

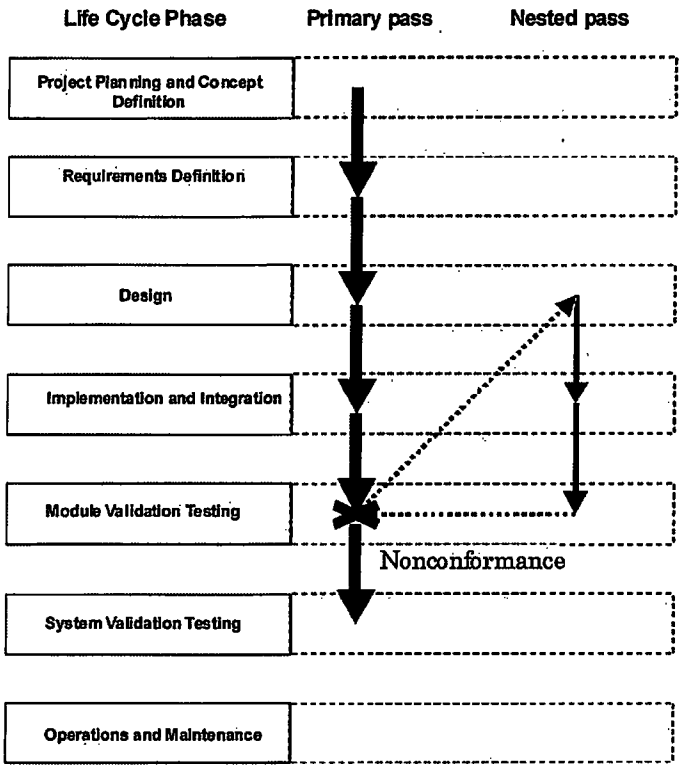


Figure 13-2 Life Cycle Iteration Process

14 Software Safety Plan

As described in the NED SMP (Reference (3)), if plant specific documents or plant safety analysis information exist, the NED System Safety Lead is responsible for identification and documentation of software safety requirements including the requirements derived from plant specific documents and plant safety analysis information. The NED System Safety Lead performs a safety assessment on the plant planning phase output (SDD, IED, and IBD), and issues a NED Software Safety Analysis Report (NED SSAR) that is an input for NICSD software safety analysis activities.

As described Section 5.2.4, the NICSD SSL appointed by the NICSD PM is responsible for software safety analysis activities with coordination through the NED System Safety Lead. The NICSD SSL shall prepare a Software Safety Plan (i.e. this section). The contents of this section shall be reviewed by the NICSD SDL, IV&V Lead and NED System Safety Lead. The NICSD SMP including this section shall be approved by the NICSD PM.

The NICSD SS Team shall perform safety analysis for the safety requirements identified in the NED SSAR using the method in this section. The NICSD SS Team shall document the result of safety activities in a NICSD SSAR issued for each phase. The NICSD IV&V shall perform independent review of the NICSD SSARs in accordance with the NICSD VVP (Reference (57)). Each NICSD SSAR shall include the following information:

- Name, Description, and Version of the Software Evaluated
- System

- Software Classification
- Purpose and Scope
- Reference Inputs
- Software Safety Analysis Body of Report
- Anomalies Noted
- Conclusion
- Responsible Engineer
- Approving Authority

The NICSD SSARs and records associated with the software safety activities described in the following sections shall be prepared, maintained current, and retained, and shall be maintained in accordance with the NICSD SCMP (Reference (56)), and stored as quality records.

The scope of the FPGA logic lifecycle phase applied to the safety analysis performed by NICSD is as follows.

- Project Planning and Concept Definition Phase
- Requirements Definition Phase
- Design Phase
- Implementation and Integration Phase
- Module Validation Testing Phase
- System Validation Testing Phase

As described in Section 7.3.3(3), the NICSD SSL reports the hazards identified during software safety activities to the NED System Safety Lead and NED PM at periodic ICDD-NICSD Project Meeting. The issue tracking spread sheet is used to track the hazards.

14.1 Analysis Techniques

Three sets of information are essential to a software and systems safety analysis. They are the functional requirements, the hazards (or failure effects), and the causes. The quality of the software safety analysis is largely determined by the completeness of these sets of information. The quality is also dependent on the quality and completeness of the hardware analyses performed to support the software safety analyses.

The functional requirements shall be an input to the analysis; the hazards and causes shall be outputs.

- The functional requirements establish what the system or equipment shall do. Each key function shall be carefully examined. As necessary, functions should be subdivided to examine the specific components that support the function.
- The hazards are the undesirable effects or consequences of a system's failure to meet its functional requirements. Built-in safety features, alarms, or procedural controls, shall be considered in assessing the hazard.
- The causes shall be the different ways that the hazards might occur.

The following methods are used in the risk analysis as described in AS-200A132 "Digital System Safety and Hazard Analysis Procedure" (Reference (20)).

(1) Fault Tree Analysis (FTA)

If plant specific documents or plant safety analysis information are not available, this method is used for safety analysis at the Project Planning and Concept Definition Phase based on the information in the EDS.

(2) Failure Modes and Effects Analysis (FMEA)

This method is used for safety analysis at the Design Phase based on the information in the MDS and FPGA Design Specification.

14.2 Project Planning and Concept Definition Phase

14.2.1 EDS Review

The NICSD SS Team shall review the EDS to ensure that each system safety requirement defined in the SDD, which is also identified in NED SSAR, is adequately addressed in the EDS.

The NICSD SS Team shall review the EDS, and provide any additional text or diagrams necessary for the software safety analysis. The NICSD SSAR for this phase shall define the scope, roles, and responsibilities for each party, and shall clearly indicate the methods used to perform software safety analysis for the EDS across the scope of other safety and non safety system.

14.2.2 Hazard Analysis

The NED SSAR includes the preliminary hazard analysis. The NICSD SS Team shall perform a hazard analysis to update the preliminary hazard analysis throughout each software life cycle. If plant specific documents or plant safety analysis information are not available, the FTA is used for safety analysis at this phase based on the information in the EDS. The results of the analysis shall be documented in the NICSD SSAR for this phase.

14.3 Requirements Definition Phase

14.3.1 Unit DDS Review

The NICSD SS Team shall review the Unit DDSs (i.e. SRSs) to ensure that each system safety requirement defined in the EDS is adequately addressed in the Unit DDSs. This analysis shall also verify that the safety requirements are written as clear, concise, unambiguous, testable, understandable statements. The results of the safety analysis shall be documented in the NICSD SSAR for this phase.

14.3.2 Hazard Analysis

The NICSD SS Team shall perform a hazard analysis to identify risks requiring additional mitigation and to evaluate the effectiveness of such mitigations. Design controls that mitigate the risk and reduce it to negligible levels shall be identified for all non-negligible risks.

14.4 Design Phase

14.4.1 Design Document Review

(1) MDS

The NICSD SS Team shall review the MDSs to ensure that each system safety requirement defined in the Unit DDS is adequately addressed in the MDSs.

(2) FPGA Design Specification

The NICSD SS Team shall review the FPGA Design Specification to ensure that each system safety requirement defined in the MDS is adequately addressed in the FPGA Design Specification.

14.4.2 FPGA Design Analysis

Analyses on the FPGA design shall be performed using the following analysis methods through IV&V activities and software safety activities:

- Functional Analysis

  The FPGA Design Specification defines the hardware and software detailed design of an FPGA on each module. This FPGA Design Specification includes functional requirements of the FPGA on the module.

  The NICSD IV&V Team shall review that the functional requirement of each module defined in the MDS is adequately addressed in the FPGA Design Specification. The NICSD IV&V Team shall also review that the FPGA Design Specification is consistent to NQ-2010 "Preparation Procedure for FPGA Design Specification" (Reference (28)) and NQ-2031 "Procedural Standard for FPGA Device Development" (Reference (35)).

- Logic Analysis

  The FPGA Design Specification describes the detailed logic requirements including the safety-critical equations, algorithms, and control logic which are necessary to perform the functional requirements of the FPGA.

  The NICSD IV&V Team shall review that the logic requirements such as safety-critical equations, algorithms, and control logic defined in the MDS is adequately addressed in the FPGA Design Specification. The NICSD IV&V Team shall also review that the FPGA Design Specification is consistent to NQ-2010 and NQ-2031.

- Data Analysis and Structure

  The FPGA Design Specification describes the data used in the FPGA. Some data are provided as a part of logic and others are provided from the memories or switches outside of the FPGA.

  The NICSD IV&V Team shall review that the data defined in the MDS is adequately addressed in the FPGA Design Specification. The NICSD IV&V Team shall also review that the FPGA Design Specification is consistent to NQ-2010 and NQ-2031.

- Internal Interface Analysis

  The FPGA Design Specification includes interface requirements such as input and output signal assignments and communication links with hardware devices and other FPGAs on the module.

  The NICSD IV&V Team shall review that the interface requirement of each module defined in the MDS is adequately addressed in the FPGA Design Specification. The NICSD IV&V Team shall also review that the FPGA Design Specification is consistent to NQ-2010 and NQ-2031.

- Constraint Analysis

  The FPGA has some restrictions for the application such as logic gate size, input and output pins' number, input and output pins' voltage, an operation clock rate, propagation delays, power supply voltages, and environmental requirements. The restrictions are defined in the FPGA device specifications, NQ-2010 and NQ-2031.

The NICSD IV&V Team shall review that the restrictions are adequately addressed in the FPGA Design Specification.

- Software Element Analysis

  An FPGA logic is comprised of combinations and connections of software elements called functional elements (FEs). The NICSD IV&V Team shall review that this hieratical design practice using FEs is adequately addressed in the FPGA Design Specification.

  The NICSD SS Team examines FEs that are not designated safety-critical and ensures that these FEs not cause a hazard.

- Timing and Sizing Analysis

  The NICSD IV&V Team shall review that the timing requirement of each module defined in the MDS is adequately addressed in the FPGA Design Specification. The NICSD IV&V Team shall also review that the timing and sizing design in the FPGA Design Specification is consistent to the FPGA device specifications, NQ-2010, and NQ-2031.

- Reliability and Availability Assessments

  The NICSD SS Team shall review the FPGA product operating history, product stability, reliability, and freedom from critical software errors. The NICSD SS Team shall also review that the FPGA Design includes failure analysis and reliability analysis to maximize design integrity and minimize the likelihood of common cause failure.

14.4.3 Hazard Analysis

During the Design Phase, the NICSD SS Team shall perform a safety assessment to confirm that potential hazards associated with design are adequately resolved to provide adequate safety levels. The NICSD SS Team shall perform a hazard analysis to identify risks requiring additional mitigation and to evaluate the effectiveness of such mitigations. Design controls that mitigate the risk and reduce it to negligible levels shall be identified for all non-negligible risks. The mitigation features shall be incorporated into the appropriate design documents, and shall be documented in the NICSD SSAR for this phase. The NICSD SSAR shall document the result of this analysis and identify design controls that shall be implemented in the design phase of the project. The risk analysis shall be performed to ensure that all necessary steps have been taken to ensure that the software meets acceptable levels of safety.

The NICSD SSAR for Design Phase shall:

- Document the intended use of the system and any reasonably foreseeable misuse.
- Identify and document those qualitative and quantitative characteristics of the system or logical group of systems that could affect safety, with defined limits as appropriate.
- Identify and document known and foreseeable hazards associated with the system in both normal and fault conditions.
- Estimate and document the risk(s) for each hazardous situation.
- Identify risk controls that mitigate risks.
- Evaluate acceptability of residual risks.

During design verification and/or validation, the NICSD SSAR shall be reviewed and updated as necessary to evaluate the effectiveness of risk mitigations that were incorporated in the design and to establish the level of residual risk. The NICSD SSAR shall provide summary information regarding postulated failure modes and the resulting hazards for the system.

The NICSD SS Team shall address on the requirements for the FPGA logic evaluation as required in Section 11.2.1, and document the result in the SAR for this phase.

14.5 Implementation and Integration Phase

14.5.1 Code Analysis

The NICSD IV&V Team performs a VHDL source code review. The following code analyses shall be performed from a safety viewpoint to verify that the VHDL source code implementation is traceable back to the FPGA Design Specification through the source code review, IV&V activities and software safety activities:

- Equations, algorithms, and control logic

  The FPGA Design Specification describes the detailed logic requirements including the safety-critical equations, algorithms, and control logic which are necessary to perform the functional requirements of the FPGA.

  The NICSD IV&V Team shall review that the equations, algorithms, and control logic are adequately addressed in the logic design code as a combination of VHDL and FEs. The NICSD IV&V Team shall also review that the design is consistent to NQ-2031.

- Constraints

  The NICSD IV&V Team shall review that the restrictions imposed by the FPGA Design Specification is adequately addressed in the design output code for the FPGA. The NICSD IV&V Team shall also review that the design of the code for the FPGA is consistent with NQ-2031.

- FPGA testing for correct execution of elements

  The NICSD IV&V Team shall review that the function requirements of an FPGA are adequately addressed in the FPGA Test Procedures. The NICSD IV&V Team shall also review that the FPGA Test Procedures are consistent with NQ-2011 "Procedure for FPGA Test" (Reference (29))

- Interface review for compatibility between FPGA

  The NICSD IV&V Team shall review that the interface requirement of each FPGA defined in the MDS are consistent. The NICSD IV&V Team shall also review that the interface requirements described in the FPGA Design Specification is adequately addressed in the design output code in the FPGA.

- Software operation within requirement constraints

  The NICSD IV&V Team shall review that the constraints described in the FPGA Design Specification is adequately addressed in the design output code in the FPGA. The NICSD IV&V Team shall also review that the design output code is consistent to NQ-2031.

- Test Procedure Evaluation

  The NICSD IV&V Team shall review that the function requirement of each module defined in the MDS is adequately addressed in the FPGA Test Procedure. The NICSD IV&V Team shall also review that the FPGA Test Procedure is consistent to NQ-2011.

- Non-Critical Code Analysis

  The NICSD SS Team examines portions of the code that are not considered safety-critical code to ensure that they do not cause hazards.

Any tools used in the performance of code inspection shall be documented in the NICSD SSAR. The NICSD SSAR shall document the results of the code inspections and include

recommendation for code and/or design changes.

In addition, detailed test requirements should be provided to ensure that adequate test coverage is provided by the test procedures.

14.5.2 FPGA Test Review

The NICSD SS Team shall perform an analysis by reviewing the FPGA Testing to ensure that software safety requirements have been implemented and that testing has proven that the implementation has successfully maintained, confirm that no new hazard is introduced in this phase, and document the analysis results in NICSD SSAR for this phase.

The NICSD SS Team shall address on the requirements for the FPGA logic evaluation as required in Section 11.2.1, and document the result in the NICSD SSAR for this phase.

14.6 Module Validation Testing Phase

The NICSD SS Team shall perform an analysis by reviewing the Module Validation Testing to ensure that software safety requirements have been implemented and that testing has proven that the implementation has successfully maintained, confirm that no new hazard is introduced in this phase, and document the analysis results in NICSD SSAR for this phase.

The NICSD SS Team shall address on the requirements for the FPGA logic evaluation as required in Section 11.2.1, and document the result in the NICSD SSAR for this phase.

14.7 System Validation Testing Phase

The NICSD SS Team shall perform an analysis of the System Validation Testing to ensure that software safety requirements have been implemented and that testing demonstrates required levels of system safety have been successfully maintained, and confirm that no new hazard is introduced in this phase. The NICSD SS Team shall document the analysis results in final NICSD SSAR for this phase. The final NICSD SSAR for this phase summarizes the software safety activities during every software life cycle phase. The summary in the NICSD SSAR for this phase shall provide evidence that the software safety program described in Section 14 has been properly carried out during every software life cycle phase.

14.8 Software Safety Change Analysis

The NICSD SSL shall review changes to software throughout the development life cycle to ensure that changes do not affect system safety.

15 Software Training Plan

15.1 Responsibilities

The NICSD PM, NICSD SDL, and other leads perform the NICSD Software Training Lead role. The NICSD PM shall be responsible for appointing managers of respective organizations in NICSD, providing human resource, indoctrination and training of the managers, and approval of

Position Guide Description for respective organizations in NICSD as specified in NQ-1002 (Reference (21)). The indoctrination and training shall be planned and performed in accordance with the AS-100A008 "Procedure for Indoctrination and Training." (Reference (14)) If required by customer, the NICSD SDL shall be responsible for establishing the System O&M Manual which is used as a System Training Manual.

The NICSD PM and managers in NICSD shall be responsible for preparation of the Position Guide Description of their organization in accordance with AS-100A009 "Procedure for Preparation of the Position Guides/Description" (Reference (15)), and for indoctrination and training of his/her section/group personnel in accordance with the Position Guide Description.

The NICSD PM and managers in NICSD shall be responsible for indoctrination and training of group members to level up technical ability, and make indoctrination and training plan in consideration of the ability of group members and requirement of assigned work. The indoctrination and training shall be planned and performed in accordance with the AS-100A008 "Procedure for Indoctrination and Training."

The NICSD PM and managers in NICSD shall make "Personnel List for Performing Safety Related Work" to list the personnel performing a safety related work from his/her group member using the format attached to NQ-1003 (Reference (22)).

The NICSD PM, and managers in NICSD shall evaluate, on an annual basis, the completeness of the indoctrination and training provided to the personnel, and record result in the "Personnel Indoctrination, Training Plan and Evaluation Record" in accordance with the AS-100A008. The manager of NICS-QA is responsible for summarizing the QA program assessment results of relevant organizations, and for reporting to the NICSD PM in accordance with NQ-1002.

The NICSD PM, NICSD SDL, and other leads shall be responsible for establishing requirements and planning for training and indoctrination of all personnel associated with the software life cycle and for ensuring that all training records are documented and archived, and require responsible manager to schedule necessary training for each personnel in accordance with the AS-100A008.

The NICSD SDL shall review the training record for each staff member to ensure that all development personnel are adequately trained any role assigned each staff member, with support from responsible managers.

The NICSD IV&V Lead shall review training records to ensure that all verification and validation personnel are adequately trained for their V&V activities (e.g., testing, code review, etc.), with support from responsible managers.

The manager of NICS-QA is responsible for vendor qualification control including PPDD and conducting a CG Survey as requested by NICSD SDL. The NICS-QA evaluates the supplier competence before ordering. The NICS-QA shall evaluate the PPDD personnel qualification control for FPGA development and testing.

The NICSD SDL is responsible for reviewing and approval of the Development Plan and ES made by PPDD to evaluate their resource and manpower levels.

15.2 Schedule

The NICSD PM, and managers in NICSD shall prepare "Personnel Indoctrination, Training Plan and Evaluation Record" to schedule the software training and complete in time to meet project needs in accordance with the AS-100A008 (Reference (14)).

15.3 General Training Activities

All NICSD personnel involved in the activities for safety-related products including the software development for the project shall be trained on the QA program course, applicable AS standards, and NQ standards identified by NQ-1003 (Reference (22)), and shall be registered in the personnel list for the safety-related works, prior to starting work on the project."

As described in the AS-100A008 (Reference (14)), the following courses are provided, and the maintenance training for each course is provided to maintain the initial knowledge or capability.

- Indoctrination/Training Course
- Codes and Standards Course
- QA Program Course
- Lead Auditor/Auditor Course
- Inspection & Test Personnel and Witness Inspector Course
- Project Specific Indoctrination/Training Course
- Root Cause Analysis Course

The NICSD PM and managers in NICSD shall prepare "Personnel Indoctrination, Training Plan and Evaluation Record" to specify training plan and select necessary training course for each personnel.

15.4 Project Training Activities

The NICSD SDL and other leads shall determine necessary training related to the following skills, as applicable to the job functions being performed, and require responsible manager to schedule project specific training as "Project Specific Indoctrination/Training Course."

- Software Development
- Software Management
- Design and Code Inspections
- Software testing
- Software tool to be used for software development, testing, and V&V
- Specific software skills or technologies applicable to the software project identified by the NICSD SDL, other leads, and managers in NICSD.

If the NICSD PM determines that additional training is necessary, the NICSD PM shall schedule additional training, or require responsible manager to schedule additional training.

15.5 Methods and Tools

The types of training are as follows as described in the AS-100A008 (Reference (14)).

- Lecture type
- Document Circulation type
- Self-study type

A trainer appointed by the NICSD PM or managers in NICSD shall schedule detail training including developing schedules, estimating resources, identifying special resources, staffing, and establishing exit or acceptance criteria for each training. The trainer shall determine the type of training, and specify training tools, techniques, and methodologies for each training. As described in Section 8.1.1, standard office software such as Microsoft® Office Power Point will be used for training when the lecture type training is selected.

15.6 Training Facilities

When preparing a training course, the responsible trainer shall determine the type of training facility that provides effective training, and shall ensure that such facilities are used. The NICSD PM, and managers in NICSD shall be responsible for providing effective training facilities to fulfill the training objectives to support the trainer.

15.7 Measurement and Metrics

As a one of metrics, the responsible trainer shall determine the sufficient time for training considering the effectiveness of the training. If the trainer determines that additional metric is necessary, the trainer can define additional metrics such as certification exams.

15.8 Records

The "Personnel Indoctrination, Training Plan and Evaluation Record," "Personnel List for Performing Safety Related Work" and training records shall be maintained as QA records in accordance with AS-100A008 (Reference (14)).

16 Software Plan Maintenance

When the changes to the SPP (Reference (2)) and input documents to NICSD are notified, each lead shall review the software plans, procedures, and instructions against the revised SPP and input documents.

Each lead shall also review the effectiveness of the software plans prepared by NICSD (i.e. NICSD SMP, SCMP, VVP, SQAP) to determine if changes are necessary. If any changes are required in the software plans, the responsible lead shall revise the software plans for internal review and approval.

The NICSD personnel responsible for implementing each software plan shall verify that the processes defined in their plan or plans are effective, adequate, suitable, sufficient, and implement the requirements in the software plans. If the NICSD personnel find editorial errors or typos in the software plans, the NICSD personnel shall notify to the responsible lead or manager using a "Document change request" sheet as described in NQ-2024 (Reference (31)).

The NICSD SQAP (Reference (55)) shall describe the method to report the problems identified through the IV&V activities and/or NICS-QA activities using Fuchu Site Nonconformance Notice Report (SNNR) and Fuchu Site Corrective Action Request (SCAR).

The responsible lead shall confirm the content of the "Document change request" sheets, SNNR, and SCAR, and correct and extend the plan appropriately.

The changes to the software plans shall be performed as follows.

- The changes in a document shall be reviewed and approved in accordance with Section 11 of NQ-2024. The changes in a document shall be documented in a Design Change Technical Report (DCTR) in accordance with NQ-2035 (Reference (38)).
- The changes in a document shall be identified in accordance with NQ-2035. The changes in a document shall be communicated using a Design Change Notice (DCN).

- The NICSD personnel responsible for implementing each software plan shall be retrained to use the updated plan as described in Section 15.4.
- The backfit to the existing work products shall be evaluated to determine the extent to which tasks shall be repeated in accordance with NQ-2035, and documented in a DCTR. The evaluation criteria shall include, as a minimum, assessments of change, change significance, software integrity level, and effects on budget, schedule, and quality.

17 Deviations from Software Plans

17.1 Deviation Policy

This section defines the procedures and criteria used to deviate from the requirements in the software plans prepared by NICSD (i.e. NICSD SMP, SCMP, VVP, and SQAP) as follows.

The information required for the deviation shall be described in the software plan relevant to the deviation, and shall include the followings.

- Task identification
- Rationale (Explanation justifying the deviation)
- Effect on software quality

The NICSD PM, NICSD SDL, other leads, and managers in NICSD responsible to each software plan shall each be responsible for approving each deviation.

17.2 Deviations from NICSD SMP

None

Table-A NICSD Output Documents

Table-A lists the types of document generated by NICSD through the lifecycle phases for the FPGA-Based systems. Table-A also shows the task and responsible lead, team, or organization for each document. The following documents and records shall be stored as quality record.

Documents	Task	Responsible of	Procedures	Other Outputs
Project Planning and Concept Definition Phase				
DIS	Prepare	SD Team	AS-200A014	PRM Record
	Review	SD Team		
	Approve	SDL		
NICSD SMP	Prepare	SD Team	Sections 2, 3, 6, and 10 of SPP	
	Review	SDL / SSL (Section 14)		
	Approve	PM		
NICSD SCMP	Prepare	SD Team	Section 7 of SPP	DVR[1)]
	Review	SCL		
	IV&V Review	IV&V Team		
	Approve	PM		
NICSD SQAP	Prepare	SQA Team	Section 5 of SPP.	DVR
	Review	SQAL		
	IV&V Review	IV&V Team		
	Approve	PM		
NICSD VVP	Prepare	IV&V Team	Section 4 of SPP	DVR
	Review	IV&V Lead		
	Approve	PM		
Software Test Plan	Prepare	IV&V Team	Section 9 of SPP	
	Review	IV&V Team		
	Approve	IV&V Lead		
MTP	Prepare	SD Team	---	DVR
	Review	SD Team		
	IV&V Review	IV&V Team		
	Approve	SDL		
EDS	Prepare	SD Team	NQ-2004 Sections 3.10.3.3 and 3.10.3.4 of SPP	RTM DVR
	Review	SD Team		
	IV&V Review	IV&V Team		
	Approve	SDL		
CGD Plan	Prepare	SD Team	AS-200A110	
	Review	SD Team		
	Approve	SDL		
PTER	Prepare	SD Team	AS-200A110	DVR
	Review	SDL		
	IV&V Review	IV&V Lead		
	Approve	PM		
PPS	Prepare	SD Team	AS-200A008	
	Review	SD Team		
	Approve	SDL		
NICSD SSAR	Prepare	SS Team	Section 14 of NICSD SMP, AS-200A132	DVR
	Review	SS Team		
	IV&V Review	IV&V Lead		
	Approve	SSL		

Documents	Task	Responsible of	Procedures	Other Outputs
NICSD VVR	Prepare	IV&V Team	NICSD VVP	PRM Record
	Review	IV&V Team		
	Approve	IV&V Lead		
NICSD MCL	Prepare	SD Team	NICSD SCMP	
	Review	SD Team		
	Approve	SDL		
BRR	Prepare	IV&V Team	NICSD VVP	
	Review	IV&V Team		
	Approve for issuance	IV&V Lead		
	Review and approve as QA record	SQAL		
Requirements Definition Phase				
Unit DDS	Prepare	SD Team	NQ-2005	RTM DVR
	Review	SD Team		
	IV&V Review	IV&V Team		
	Approve	SDL		
ECWD	Prepare	SD Team	NQ-2017	RTM DVR
	Review	SD Team		
	IV&V Review	IV&V Team		
	Approve	SDL		
Unit User's Manual	Prepare	SD Team	---	DVR
	Review	SD Team		
	IV&V Review	IV&V Team		
	Approve	SDL		
CDI	Prepare	SD Team	NQ-4001	
	Review	SD Team		
	Approve	SDL		
Procurement document	Prepare	SD Team	NQ-2025	
	Review	SD Team		
	Approve	SDL		
CG Survey Report	Prepare	NICS-QA	NQ-3005 Sections 8, 11 and 13.2.8 of NICSD SMP, PTER, CDI, PPS	
	Review	NICS-QA		
	Approve	SQAL		
CDR Report	Prepare	SD Team	Sections 8, 11 and 13.2.8 of NICSD SMP, PTER, CDI, PPS	
	Review	SDL		
	Approve	PM		
NICSD SSAR	Prepare	SS Team	Section 14 of NICSD SMP, AS-200A132	DVR
	Review	SS Team		
	IV&V Review	IV&V Team		
	Approve	SSL		
NICSD VVR	Prepare	IV&V Team	NICSD VVP	PRM Record
	Review	IV&V Team		
	Approve	IV&V Lead		
NICSD MCL (Updated)	Prepare	SD Team	NICSD SCMP	
	Review	SD Team		
	Approve	SDL		
BRR	Prepare	IV&V Team	NICSD VVP	
	Review	IV&V Team		
	Approve for issuance	IV&V Lead		
	Review and approve as QA record	SQAL		

Documents	Task	Responsible of	Procedures	Other Outputs
Design Phase				
Job Order	Prepare	SD Team	NQ-2025	
	Review	SD Team		
	Approve	SDL		
MDS	Prepare	PPDD	PPDD Procedure NICSD VVP NQ-2026	RTM DVR
	IV&V Review	IV&V Team		
	Approve	SDL		
FPGA Design Specification	Prepare	PPDD	PPDD Procedure NICSD VVP NQ-2026	RTM DVR
	IV&V Review	IV&V Team		
	Approve	SDL		
NICSD SSAR	Prepare	SS Team	Section 14 of NICSD SMP, AS-200A132	DVR
	Review	SS Team		
	IV&V Review	IV&V Team		
	Approve	SSL		
NICSD VVR	Prepare	IV&V Team	NICSD VVP	PRM Record
	Review	IV&V Team		
	Approve	IV&V Lead		
NICSD MCL (Updated)	Prepare	SD Team	NICSD SCMP	
	Review	SD Team		
	Approve	SDL		
BRR	Prepare	IV&V Team	NICSD VVP	
	Review	IV&V Team		
	Approve for issuance	IV&V Lead		
	Review and approve as QA record	SQAL		
Implementation and Integration Phase				
Source Code Review Sheet	Prepare	IV&V Team	NICSD VVP	
	Review	IV&V Team		
	Approve	IV&V Lead		
FPGA Test Procedure	Prepare	PPDD	PPDD Procedure NICSD VVP NQ-2026	RTM DVR
	IV&V Review	IV&V Team		
	Approve	SDL		
FPGA Test Report	Prepare	PPDD	PPDD Procedure NICSD VVP NQ-2026	DVR
	IV&V Review	IV&V Team		
	Approve	SDL		
PPDD Module MCL (including FPGA Control Sheet, VHDL source code, Fusemap)	Prepare	PPDD	PPDD Procedure NICSD SCMP NQ-2033 NQ-2026	
	Review	SD Team		
	Approve	SDL		
FPGA Logic Implementation Request/Record Sheet	Prepare	SD Team	NQ-2030	
	Review	SD Team		
	Approve	SDL		
Module Test Procedure	Prepare	PPDD	PPDD Procedure NICSD VVP NQ-2026	RTM DVR
	IV&V Review	IV&V Team		
	Approve	SDL		
NICSD SSAR	Prepare	SS Team	Section 14 of NICSD SMP, AS-200A132	DVR
	Review	SS Team		
	IV&V Review	IV&V Team		
	Approve	SSL		
NICSD VVR	Prepare	IV&V Team	NICSD VVP	PRM Record
	Review	IV&V Team		
	Approve	IV&V Lead		

Documents	Task	Responsible of	Procedures	Other Outputs
NICSD MCL (Updated)	Prepare	SD Team	NICSD SCMP	
	Review	SD Team		
	Approve	SDL		
BRR	Prepare	IV&V Team	NICSD VVP	
	Review	IV&V Team		
	Approve for issuance	IV&V Lead		
	Review and approve as QA record	SQAL		
Module Validation Testing Phase				
Module Test Report	Prepare	PPDD	PPDD Procedure NICSD VVP NQ-2026	DVR
	IV&V Review	IV&V Team		
	Approve	SDL		
PPDD Module MCL (updated)	Prepare	PPDD	PPDD Procedure NICSD SCMP NQ-2033 NQ-2026	
	Review	SD Team		
	Approve	SDL		
System O&M Manual	Prepare	SD Team	Section 13.5.8 of NICSD SMP, Sections 12.4 and 13.4 of SPP	DVR
	Review	SD Team		
	IV&V Review	IV&V Team		
	Approve	SDL		
Software Validation Test Plan (SVTP)	Prepare	IV&V Team	Section 9 of SPP	RTM DVR PRM Record
	Review	IV&V Team		
	Approve	IV&V Lead		
NICSD SSAR	Prepare	SS Team	Section 14 of NICSD SMP, AS-200A132	DVR
	Review	SS Team		
	IV&V Review	IV&V Team		
	Approve	SSL		
NICSD VVR	Prepare	IV&V Team	NICSD VVP	PRM Record
	Review	IV&V Team		
	Approve	IV&V Lead		
NICSD MCL (Updated)	Prepare	SD Team	NICSD SCMP	
	Review	SD Team		
	Approve	SDL		
BRR	Prepare	IV&V Team	NICSD VVP	
	Review	IV&V Team		
	Approve for issuance	IV&V Lead		
	Review and approve as QA record	SQAL		
System Validation Testing Phase				
Software Validation Test Report (SVTR)	Prepare	IV&V Team	Section 9 of SPP	PRM Record
	Review	IV&V Team		
	Approve	IV&V Lead		
CGD Report	Prepare	SD Team	NQ-4001	
	Review	SD Team		
	Approve	SDL		
FTER	Prepare	SD Team	AS-200A110	DVR
	Review	SDL		
	IV&V Review	IV&V Lead		
	Approve	PM		
CGD Package	Prepare	SD Team	AS-200A110	
	Review	SD Team		
	Approve	SDL		

Documents	Task	Responsible of	Procedures	Other Outputs
NICSD SSAR	Prepare	SS Team	Section 14 of NICSD SMP; AS-200A132	DVR
	Review	SS Team		
	IV&V Review	IV&V Team		
	Approve	SSL		
NICSD VVR	Prepare	IV&V Team	NICSD VVP	
	Review	IV&V Team		
	Approve	IV&V Lead		
NICSD MCL (Updated)	Prepare	SD Team	NICSD SCMP	
	Review	SD Team		
	Approve	SDL		
BRR	Prepare	IV&V Team	NICSD VVP	
	Review	IV&V Team		
	Approve for issuance	IV&V Lead		
	Review and approve as QA record	SQAL		

1) DVR: Design Verification Report

Table-B Compliance to SPP

Table-B Compliance to SPP

No.	SPP Section	Title	SMP Section(s)	Remark
1.	1	Introduction	N/A	Section Title
2.	1.1	Purpose	N/A	No requirement
3.	1.2	Use of the Software Program Plan	N/A	No requirement
4.	1.2.1	Vendor Plan Use	2, 4, 6	
5.	1.2.2	Licensing Basis Documents	N/A	No requirement
6.	1.2.3	[Deleted]	N/A	No requirement
7.	1.3	Scope	1	
8.	1.3.1	Use of Existing Software Plans and Processes	Table-C	
9.	1.3.2	Nonsafety Plan Requirements	N/A	This requirement is for nonsafety systems
10.	1.3.3	Defining Software	Comply	This NICSD SMP is applied to FPGA based Safety-Related Systems defined in Sec.13.3 of SPP.
11.	1.4	Roles and Responsibilities	N/A	Section Title
12.	1.4.1	Organization	5, Fig.5-1	
13.	1.4.2	Independence	5.2, Fig.5-1	
14.	1.4.3	Responsibilities	5.2, 15.1	
15.	1.4.4	Qualifications and Training	15	
16.	1.4.5	Organizational Interfaces	7.3.3 (3), Fig.5-1	
17.	1.5	Terms and Definitions	Comply	This SMP uses terms and definition in accordance with this SPP section.
18.	1.6	Acronyms	3.2	
19.	1.7	Secure Development and Operational Environment	8.3	
20.	1.8	Applicable Standards and References	4	
21.	1.9	Software Life Cycle Overview	Table 13-1, 13.1-13.6	
22.	1.10	Software Classification	N/A	This NICSD SMP is applied to FPGA based Safety-Related Systems
23.	1.11	General Policies for All Plans	N/A	No requirement
24.	1.11.1	Use of IEEE Standards	Comply	The SDDs for each system specify applicable IEEE Standards.
25.	1.11.2	Life Cycle Task Iteration Policy	13.9, 16	
26.	1.11.3	Deviation Policy	17.1	

Table-B Compliance to SPP

No.	SPP Section	Title	SMP Section(s)	Remark
27.	1.11.4	Control Procedures	4	
28.	1.11.5	Standards, Policies, and Conventions	4, 8.3	
29.	1.11.6	Schedule	7.3.3 (9),9	
30.	1.11.7	Use of Designees	5.2, Table 5-1, Table-A	
31.	1.11.8	Modifications to PDS and COTS	11.1, 11.2.1, 13.9, 14	
32.	1.11.9	Modifications to Configuration	13.7, 14	
33.	1.11.10	Use of Metrics	7.3.3 (6), 7.3.3 (8),9	
34.	1.12	Software Plan Maintenance	16	
35.	1.13	[Deleted]	16	
36.	2	Software Project Management Program Plan (SPMPP)	N/A	Section Title
37.	2.1	Introduction	N/A	No requirement
38.	2.1.1	Purpose	1	
39.	2.1.2	Scope	2, Table-A, 5.2.5	
40.	2.1.3	[Deleted]	N/A	No requirement
41.	2.1.4	Relationship of the SPMPP to Other SPP Sections	N/A	No requirement
42.	2.2	Project Organization	5, Fig.5-1	
43.	2.2.1	Process Model	2, 5, 7.3.3 (9), 9, 10, Fig.5-1	
44.	2.2.2	Organizational Structure	Fig.5-1	
45.	2.2.3	Organizational Boundaries and Interfaces	2, 8, 7.3.3 (9), 9, 13.3.3	
46.	2.2.4	Project Responsibilities	5.2, 9	
47.	2.3	Managerial Process	N/A	Section Title
48.	2.3.1	Management Objectives and Priorities	7.1, 7.3.3 (9), 9	
49.	2.3.2	Assumptions, Dependencies, and Constraints	11, 13.1.7, 13.2.8	
50.	2.3.3	Risk Management	7.2	
51.	2.3.4	Monitoring and Controlling Mechanisms and Metrics	7.3.1-7.3.4, 8.1, 8.1.1	
52.	2.3.5	Staffing Plan	7.4, 7.3.3 (9), 9, 15.1, Fig.5-1	
53.	2.4	Technical Process	N/A	Section Title
54.	2.4.1	Methods, Tools, and Techniques	8.1	
55.	2.4.2	Software Documentation	8.2, 10, Table-A	
56.	2.4.3	Secure Development and Operational Environment and Cyber Security	8.3	
57.	2.4.4	Project Support Functions	8.1.1	
58.	2.5	Work Packages, Schedule, and Budget	9	

Table-B Compliance to SPP

No.	SPP Section	Title	SMP Section(s)	Remark
59.	2.5.1	Work Packages	7.3.2, 9	
60.	2.5.2	Dependencies	9	
61.	2.5.3	Resource Requirements	7.3.1, 9	
62.	2.5.4	Budget and Resource Allocation	5.2.1, 7.3.1, 7.3.3 (9), 9	
63.	2.5.5	Schedule	7.3.3 (9), 9	
64.	3	Software Development Program Plan (SDPP)	N/A	Section Title
65.	3.1	Introduction	N/A	No requirement
66.	3.1.1	Purpose	1	
67.	3.1.2	Scope	2, Table-A	
68.	3.1.3	[Deleted]	N/A	No requirement
69.	3.1.4	Relationship of the SDPP to Other SPP Sections	N/A	No requirement
70.	3.2	Organization of Software Life Cycle Processes	Fig.5-1	
71.	3.3	Methods	4, Table-A	
72.	3.3.1	Schedule	7.3.2, 7.3.3 (9), 9	
73.	3.3.2	Configuration Management and Change Control	13.1.10, 13.7	See also NICSD SCMP
74.	3.3.3	Independent Verification and Validation	5.1, 5.2.3	See also NICSD VVP
75.	3.3.4	Testing	13.4.4, 13.5.3, 13.6.3	
76.	3.3.5	Software Safety Analysis	5.2.4, 14	
77.	3.3.6	Secure Development and Operational Environment Analysis	8.3	
78.	3.3.7	Baseline Review	10	
79.	3.3.8	Incomplete Requirements	13 para.5	
80.	3.3.9	Use of Previously Developed or Purchased Software	11.1, 11.2	
81.	3.4	Tools	8.1.2	
82.	3.5	Requirements Traceability Matrix	12	
83.	3.6	Life Cycle Figures	Table 13-1	
84.	3.7	Life Cycle Phases	Table-A	
85.	3.8	Plant-Level SPP Design Inputs	N/A	A requirement for NED activity. Outside the scope of this NICSD SMP
86.	3.9	Planning Phase	N/A	Section Title
87.	3.9.1	Overview	N/A	No requirement
88.	3.9.2	Planning Phase Inputs	13..1	
89.	3.9.3	Planning Phase Outputs	Table 3-1, Table-A, 8.3, 10, 12, Subsections of	

Table-B Compliance to SPP

No.	SPP Section	Title	SMP Section(s)	Remark
			Sec.13.1	
90.	3.10	Requirements Phase	N/A	Section Title
91.	3.10.1	Overview	13.2.3, 13.1.6, 13.2.6	
92.	3.10.2	Requirements Phase Input	13.2.1	
93.	3.10.3	Requirements Phase Outputs	Table 3-1, Table-A, 8.3, 10, 12, Subsections of Sec.13.2	
94.	3.11	Design Phase	N/A	Section Title
95.	3.11.1	Overview	11.2, 11.3, 13.1.7 (2), 13.2.8, 13.3.4, 13.3.5, 13.3.7	
96.	3.11.2	Design Phase Inputs	13.3.1	
97.	3.11.3	Design Phase Outputs	Table 3-1, Table-A, 6.2, 8.3, 10, 11, 12, Subsections of Sec.13.3	
98.	3.12	Implementation Phase	N/A	Section Title
99.	3.12.1	Overview	13.4.3, 13.4.4	
100.	3.12.2	Implementation Phase Inputs	13.4.1	
101.	3.12.3	Implementation Phase Outputs	Table 3-1, Table-A, 8.3, 10, 11.3, 12, Subsections of Sec.13.4	
102.	3.13	Testing and Integration Phase	N/A	Section Title
103.	3.13.1	Overview	13.9	
104.	3.13.2	Testing and Integration Phase Inputs	13.5.1	
105.	3.13.3	Testing and Integration Phase Outputs	Table 3-1, Table-A, 8.3, 10, 12, Subsections of Sec.13.5 and 13.6	
106.	3.14	Installation Phase	N/A	Section Title
107.	3.14.1	Overview	13.4.5, 13.4.9, 13.5.11, 13.6.9	
108.	3.14.2	Installation Phase Inputs	N/A	Non-Rewritable FPGA, one-time programmable devices is used. Because FPGA logic is implemented and fixed as physical contacts in the chips, there is no need for software installation.
109.	3.14.3	Installation Phase Outputs and Activities	13.5.8, 13.6.3	System Validation Testing shall is combined with PFT. System O&M Manual is prepared in Module Validation Testing

Table-B Compliance to SPP

No.	SPP Section	Title	SMP Section(s)	Remark
				Phase
110.	3.15	Operations Phase	N/A	Section Title
111.	3.15.1	Overview	N/A	Outside the scope of this NICSD SMP.
112.	3.15.2	Operations Phase Inputs	N/A	Outside the scope of this NICSD SMP.
113.	3.15.3	Operations Phase Outputs	N/A	System O&M Manual is prepared in Module Validation Testing Phase
114.	3.16	Maintenance Phase	N/A	Section Title
115.	3.16.1	Overview	N/A	Outside the scope of this NICSD SMP.
116.	3.16.2	Maintenance Phase Inputs	N/A (13.7)	Sec.13.7 describes the change control process.
117.	3.16.3	Maintenance Phase Outputs	N/A	Outside the scope of this NICSD SMP.
118.	3.16.4	Maintenance Phase Activities	N/A (13.7)	Sec.13.7 describes the change control process.
119.	3.17	Retirement Phase	13.8	
120.	6	Software Safety Program Plan (SSPP)	N/A	Section Title
121.	6.1	Introduction	N/A	Section Title
122.	6.1.1	Purpose	1	
123.	6.1.2	Scope	2	
124.	6.1.3	[Deleted]	N/A	No requirements
125.	6.1.4	Relationship of the SSPP to Other SPP Sections	N/A	No requirements
126.	6.2	Reference Documents	N/A	No requirements
127.	6.3	Software Safety Management	5.2.4, 14	
128.	6.3.1	Organization and Responsibilities	5.2.4, 7.3.1, 7.3.2, 7.3.3 (3), 8.3, 13, 14, 15.4, Table-A	
129.	6.3.2	Resources	7.3.1	
130.	6.3.3	Schedule	7.3.3 (9), 9	
131.	6.3.4	Qualifications and Training	15, 15.1, 15.4	
132.	6.3.5	Software Life Cycle	Subsections of Sec.13 and 14	
133.	6.3.6	Documentation Requirements	Table-A, Subsections of Sec.13 and 14,	
134.	6.3.7	Software Safety Program Records	Table-A, Subsections of Sec.13 and 14,	
135.	6.3.8	Software Configuration Management Activities	13 para.4	NICSD SCMP
136.	6.3.9	Software Quality Assurance Activities	(NICSD SQAP	NICSD SQAP

Table-B Compliance to SPP

No.	SPP Section	Title	SMP Section(s)	Remark
			addresses this requirement)	
137.	6.3.10	Software Verification and Validation Activities	(NICSD VVP addresses this requirement)	NICSD VVP
138.	6.3.11	Tool Support and Approval	8.1	
139.	6.3.12	Previously Developed or Purchased (COTS) Software	11.2.1, 11.2.2	
140.	6.3.13	Subcontract Management	14	
141.	6.3.14	Process Certification	10	
142.	6.4	Software Safety Analyses	N/A	Section Title
143.	6.4.1	Preparatory Analyses	13.14, 14.7	
144.	6.4.2	Software Safety Requirements Analysis Preparation	13.1.6, 14.2.1, 14.2.2	
145.	6.4.3	Software Safety Requirements Analysis	14.3.1	
146.	6.4.4	Software Safety Design Analysis	12, 13.1.9, 13.2.10, 13.3.10, 14.1, 14.2.1, 14.3.1, 14.4.1.-14.4.3	
147.	6.4.5	Software Safety Code Analysis	14.5.1	
148.	6.4.6	Software Safety Integration and Validation Test Analyses	14.5.2, 14.6, 14.7	
149.	6.4.7	Software Safety Installation Analysis	N/A	Non-Rewritable FPGA, one-time programmable devices is used. Because FPGA logic is implemented and fixed as physical contacts in the chips, there is no need for software installation.
150.	6.4.8	Software Safety Change Analysis	14.8	
151.	6.5	Post Development	N/A	The safety analysis to PIT is outside the scope of the NICSD SMP.
152.	6.5.1	Training	15	
153.	6.5.2	Deployment	N/A	Outside the scope of NICSD safety analysis activity.
154.	6.6	Plan Approval	14	
155.	6.7	Software Safety Analysis Reporting	14, 14.7	
156.	10	Software Training Program Plan (STrngPP)	N/A	Section Title
157.	10.1	Introduction	N/A	No requirements
158.	10.1.1	Purpose	1, 15.1, 15.3, 15.4, 15.8, Table-A	
159.	10.1.2	Scope	2, 15.1, 15.5, 15.6, Fig.5-1	
160.	10.1.3	[Deleted]	N/A	

Table-B Compliance to SPP

No.	SPP Section	Title	SMP Section(s)	Remark
161.	10.1.4	Relationship of the STrngPP to Other SPP Sections	N/A	
162.	10.2	Software Training Overview	N/A	
163.	10.2.1	Organization	Fig.5-1	
164.	10.2.2	Responsibilities	15.1, 15.5, Table-A	
165.	10.2.3	Schedule	7.3.3 (9), 9, 15.5	
166.	10.3	Training Activities	N/A	Section Title
167.	10.3.1	General Training Activities	15.1, 15.3, 15.5	
168.	10.3.2	Project Training Activities	15.4	
169.	10.4	Methods and Tools	15.4, 15.5	
170.	10.5	Training Facilities	15.6	
171.	10.6	Measurement and Metrics	15.1, 15.7, 15.8	