TOSHIBA
Leading Innovation >>>

UTLR-0020NP Part I Rev.1
February 2015

Topical Report

Licensing Topical Report for Toshiba NRW-FPGA-based Instrumentation and Control System for Safety-Related Application

Part I
Software Lifecycle and Development Process

Approved by
Instrumentation & Control Systems
Design and Engineering Dept.

Masayoshi Tahira

Toshiba Corporation
Nuclear Energy Systems & Services Division

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

TOSHIBA CORPORATION
NUCLEAR ENERGY SYSTEMS & SERVICES DIV.

Table of Contents

List of Figures

List of Tables

Note: Tables in Appendix are not listed here.

Note for Acronyms and References

All acronyms and references are listed in the Acronym and Reference Part, which is provided as a separate part of this LTR.

I-1 Introduction

This is Part I of the Licensing Topical Report (LTR) for Toshiba FPGA-based Safety-Related Instrumentation and Control Systems. Part I addresses the Toshiba software lifecycle and development process. The number provided on individual sections consists of a Roman numeral Part number, a dash, and the section number within that Part. Thus I-1.1 would refer to Part I, Section 1.1. Section numbers start at 1 in each Part of this LTR.

I-1.1 Background

Toshiba has extensive experience in supplying nuclear safety-grade Instrumentation and Control (I&C) systems in Japan. This experience ranges from supplying digital I&C systems, such as Power Range Neutron Monitors for individual plants, up to designing and manufacturing the world's first fully integrated digital CPU-based I&C systems for Advanced Boiling Water Reactors (ABWRs). These systems were first installed at Kashiwazaki-Kariwa Unit 6, and are in use at Kashiwazaki-Kariwa Unit 6 and Hamaoka Unit 5.

Following the installation of the CPU-based BWR digital system, Toshiba started development of I&C technology based on Non-Rewritable (NRW) Field Programmable Gate Arrays (FPGAs) and supplied the NRW-FPGA-based I&C products to Japanese Nuclear Power Plants under Toshiba's ISO 9001 program. NRW-FPGA-based products have been installed in 11 nuclear power plants including 254 NRW-FPGA-based units for non-safety-related systems, 91 units for safety-related process radiation monitors and 60 units for safety-related neutron monitoring systems.

Toshiba also has been working on establishing of a 10 CFR 50 Appendix B (Reference (a2)) Quality Assurance (QA) process to permit the use of Toshiba FPGA-based system in the US for safety-related applications in nuclear power plants. Toshiba implemented Appendix B QA processes in a phased approach as follows to ensure a smooth transition of the processes at the affected organizations.

- Original Process:
  Initial establishment of the Appendix B QA process in the system engineering organization, this process was applied to the development and the qualification of the Power Range Monitor (PRM) for a BWR-5. This process is referred as original process hereafter.

- Current Process:

Improved the original process by extending Appendix B QA process into design organization and closer to the manufacturing organization where other Toshiba NRW-FPGA-based I&C products will be developed, and which will be applied to modifications to the products developed under the previous process. This process is referred as current process hereafter in this LTR.

Toshiba has used the original process to develop and qualify a NRW-FPGA-based Power Range Monitor (PRM) for a BWR-5.

After the development of the PRM, Toshiba was selected as the Engineering, Procurement, and Construction (EPC) Contractor for two new Advanced Boiling Water Reactors (ABWRs) to be constructed at the South Texas Project (STP) site. South Texas Project – Nuclear Operating Company (STPNOC) selected the NRW-FPGA-based systems for the Reactor Trip and Isolation System (RTIS) and the Neutron Monitoring System (NMS).

STPNOC elected to license the NRW-FPGA platform using the Design Acceptance Criteria (DAC) inspection process. Key platform design information regarding platform independence, determinism, diversity, redundancy, and simplicity is included in the STP 3&4 COL and has been reviewed by USNRC Staff and the Advisory Committee for Reactor Safeguards (ACRS).

In April 2011, the schedule for procurement and engineering activities for the STP 3&4 project including the post-COL DAC Inspection activities has been extended and is no longer predictable. COL related activities continue.

Toshiba desires the USNRC platform review to continue, so this LTR has been drafted for submittal. This current LTR submittal consists of the following six Parts and a separate Acronym and Reference Part.

Part I describes software lifecycle and development processes.

Part II describes design description of the platform with application guide.

Part III describes the qualification results of the BWR-5 PRM and the ABWR Oscillation Power Range Monitor (OPRM).

Part IV describes the compliance to the Codes and Standards.

Part V is V&V report of the BWR-5 PRM.

Part VI is V&V report of the ABWR OPRM.

The Acronym and Reference Part lists all the acronyms and references used in all Parts except Part V and VI of the LTR. Part V and VI have their own acronym and reference lists because they are existing actual V&V reports of the BWR-5 PRM and the ABWR OPRM.

I-1.2 Purpose

The purpose of the LTR is to describe the features and the qualification of Toshiba NRW-FPGA-based Safety-Related Systems with an explanation of latest development and qualification process which is applied to US nuclear safety-related applications.

The development process and the qualification process introduced in this document are applied to all Toshiba NRW-FPGA-based Safety-Related Systems. The BWR-5 PRM and the ABWR OPRM Systems are discussed in the LTR.

The BWR-5 PRM was developed by the design process summarized in Sections I-3 and Appendix I-A, which is called the Original Process in this LTR. The qualification activities of the BWR-5 PRM, including EQ and EMC testing were completed using the Original Process.

Since the development of the BWR-5 PRM, Toshiba has improved their processes by moving the boundaries of 10 CFR 50 Appendix B (Reference (a2)) closer to manufacturing. The Current Process was applied to the ABWR OPRM; the qualification activities of the ABWR OPRM, including EQ and EMC testing were completed using the Current Process. The Current Process will be applied to any newly manufactured or modified Toshiba NRW-FPGA-based Safety-Related Systems. The LTR addresses the qualification results of the BWR-5 PRM based on the Original Process, and the qualification results of the ABWR OPRM based on the Current Process.

I-1.3 Scope

This LTR is being submitted to the USNRC for review and approval of Toshiba NRW-FPGA-based Safety-Related Systems as platform.

The NRW-FPGA-based systems have been implemented on several different plant systems, as described in Section I-1.1 in this LTR. The following systems are taken to describe the Toshiba NRW-FPGA-based Safety-Related Systems for qualification:

- Power Range Monitor (PRM) for BWR-5
- Oscillation Power Range Monitor (OPRM) for ABWR

This LTR also describes the adaptation of these systems to other types of boiling water reactors, including BWR-3, -4, -5, -6, and ABWR. In ABWR, PRM is called PRNM (Power Range Neutron Monitoring System).

In addition, the Toshiba NRW-FPGA-based systems can be applied to several other safety-related systems. While not descried in this LTR, the same modular, and structurally decomposed approach to system design as implemented in the systems described in the LTR allows the NRW-FPGA-based systems to be applied to:

- Reactor Protection System (RPS) in any commercially licensed US Light Water Reactor
- Main Steam Isolation Systems, combined with RPS functions into a single Reactor Trip and Isolation System (RTIS) in the ABWR DCD (Reference (a49))
- Suppression Pool Temperature Monitoring (SPTM) (also part of the RTIS)
- Startup Range Neutron Monitoring System (SRNM)
- Engineered Safety Features Actuation Systems (ESFAS)
- Radiation Monitoring Systems

In the Part I of the LTR, the following sections are organized to explain the software lifecycle and development process.

- Section I-1 provides introductory material like the report purpose and scope,
- Section I-2 describes the quality assurance programs and activities used by Toshiba for design, manufacturing and qualification of FPGA-based systems.
- Section I-3 describes Toshiba's lifecycle approach to FPGA logic and hardware development, including the validation and verification (V&V) processes used in this development.
- Appendix I-A summarizes the design processes of the Original Process and the Current Process.

I-1.4 Toshiba Organization

Toshiba's FPGA-based systems are developed by Toshiba Power Systems Company (PS). The branch of Toshiba PS that provides components for nuclear power plants is referred to as PS Nuclear Energy (PSNE). PSNE has several units: the Nuclear Energy Systems and Services Division (NED), Toshiba Keihin Product Operations (Keihin), and Toshiba Fuchu Complex (Fuchu Complex). NED is responsible for all PSNE activities. Keihin is a manufacturer of nuclear reactor components (e.g., reactor internals and core support structure), as well as the main steam turbines and generators. Fuchu Complex is a manufacturer of equipment for I&C systems including safety-related systems (e.g. reactor protection systems and neutron monitoring systems). Portions of Keihin and the Fuchu Complex have a 10 CFR 50 Appendix B QA program. These organizations are the Nuclear Energy Equipment Manufacturing Department (NEEMD) of Keihin and the Nuclear Instrumentation & Control Systems Department (NICSD) of Fuchu Complex.

Toshiba's FPGA-based systems are developed by two Toshiba organizations: NED and Fuchu Complex.

Several departments within NED are involved in the process documented in this LTR. These include:

- The NED Quality Assurance Department (NQAD) is responsible for establishment and issuance of the QA Program Description (QAPD) and PSNE top level policies and procedures that are applied to all activities affecting quality within PSNE. NQAD is also responsible for measuring and auditing the various functional organizations within PSNE.
- The NED Instrumentation & Control Systems Design and Engineering Department (ICDD) is responsible for system design and engineering of I&C products, including safety-related FPGA-based systems.

The following departments are involved in the process at the Fuchu Complex, which is divided into segments. One of the segments is the Power Systems Segment, known as Fuchu-PS. Fuchu-PS is composed of several departments. One of them is the Nuclear Instrumentation & Control Systems Department (NICSD). In 2006, NICSD was reorganized and split into two parts: NICSD and a separate department referred to as the module supplier in this report. The functions and responsibilities for these departments are:

- NICSD designs, tests, and assembles units*1 and equipment for safety-related and nonsafety-related systems for nuclear power plants including safety-related FPGA-based systems. NICSD has a 10 CFR 50 Appendix B QA program. NICSD controls suppliers through procurement activities including Commercial Grade

Dedication (CGD).
The module supplier designs, tests, and oversees manufacturing of modules[*2] for safety-related and nonsafety-related systems for nuclear, thermal, and hydroelectric power plants. The module supplier is responsible for the design and implementation of the FPGA logic and use of software tools for producing FPGAs. The module supplier works under an ISO 9001 QA program.

- The printed circuit board fabricator is an affiliated, wholly owned subsidiary company of Toshiba, located in the Fuchu Complex. The printed circuit board fabricator has responsibility for manufacturing of the printed circuit boards for the modules for the FPGA-based systems. The printed circuit board fabricator works under an ISO 9001 QA program.

Note *1: The unit is a chassis that has front slots and back slots to mount modules. Refer to Section II-2.1.3 for detailed description of the "unit."

Note *2: Each module consists of one or more printed circuit boards, on which the FPGAs and other circuitry are mounted, and a front panel. Refer to Section II-2.1.2 for detailed description of the "module."

The organizations involved in the work to generate FPGA-based safety-related products for US nuclear power plants are shown graphically in Figure I-1-1.

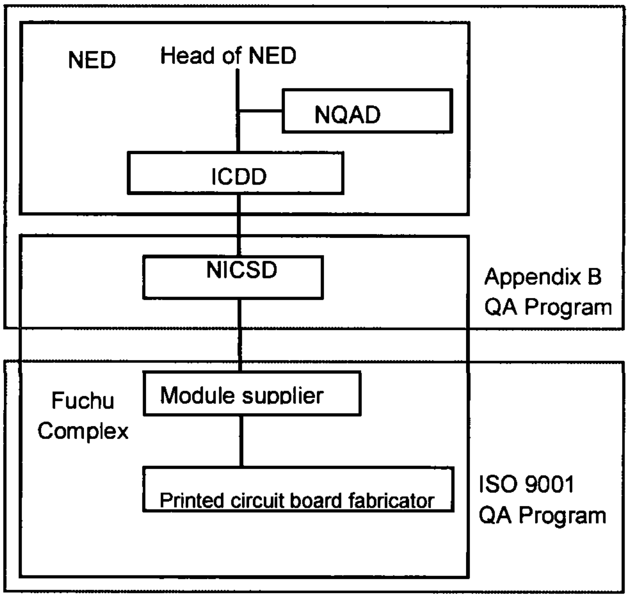


Figure I-1-1 Toshiba Organizations for US Safety-Related FPGA-Based Products

I-1.5 Current Process Overview

This section provides the overview of the current design process of the FPGA-based safety-related I&C systems with the changes from the original process.

Changes from the original process used to qualify the BWR-5 PRM system are listed in the Appendix I-A.

I-1.5.1 Process Overview

FPGA-based I&C systems do not use the application software like microprocessor based systems. However, the FPGA circuits are designed and implemented using software coding. Toshiba has developed their FPGA process lifecycle from years of experience using a software-like lifecycle. For the Toshiba plans, FPGA logic is referred to as software, for simplicity.

Figure I-1-2 provides the overview of the process and organizational responsibilities. The Instrumentation & Control Systems Design and Engineering Department (ICDD) of NED is responsible for system design for safety-related applications.

There are two groups in ICDD: the control system engineering group and the monitoring system engineering group. NED procures the assembled FPGA-based system from NICSD and delivers it to the customer.

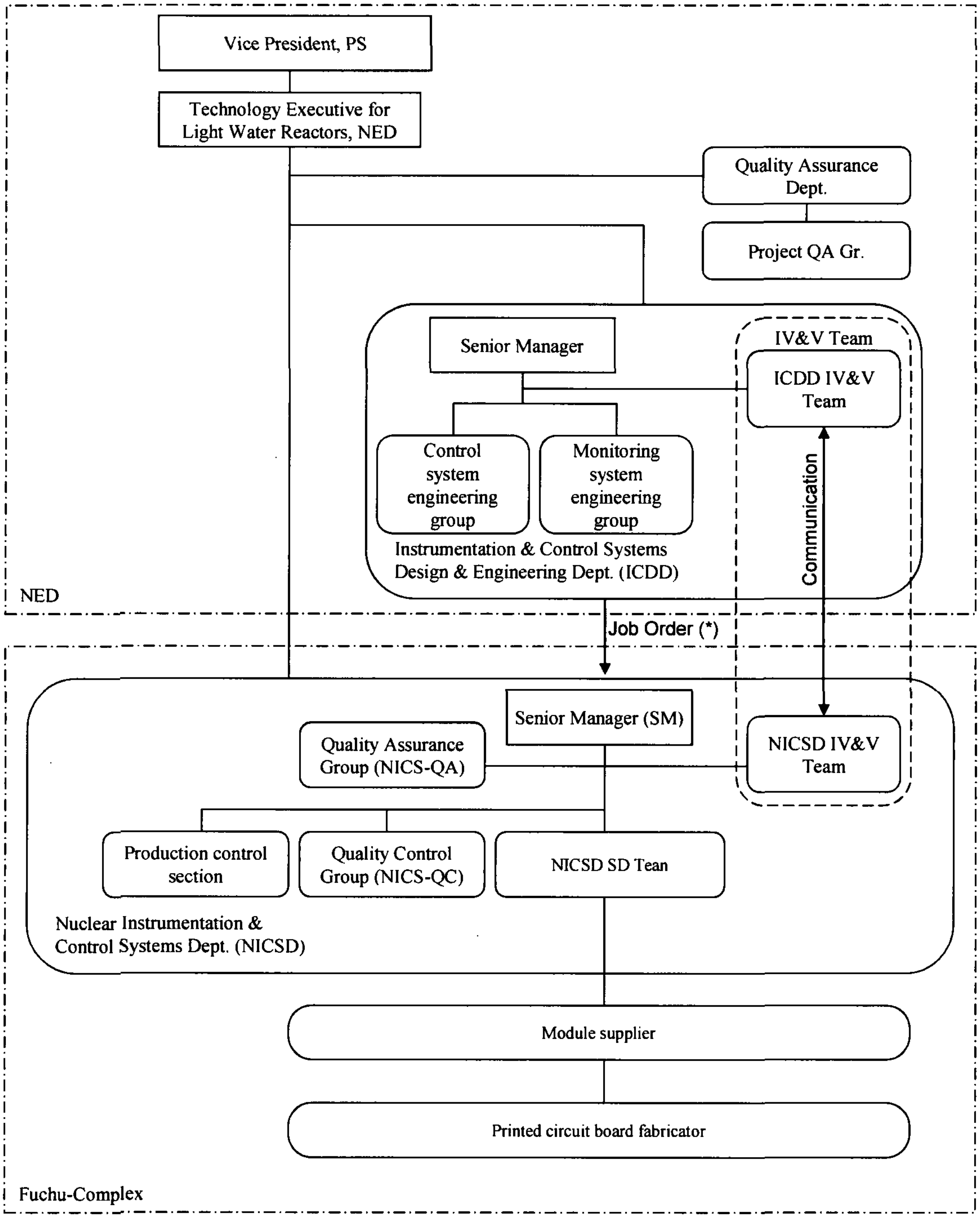
The NED Quality Assurance Department (NQAD) is responsible for quality assurance in NED. Responsibilities of the NQAD are described in QAPD (Reference (b1)).

NICSD is responsible for detailed design of the FPGA-based systems, procures the modules for FPGA-based system from the module supplier, and assembles the FPGA-based system from the modules. NICSD has their own set of software plans to augment their QA requirements.

The Quality Assurance Group in NICSD (NICS-QA) is responsible for quality assurance in NICSD. Software QA responsibilities are provided in the NICSD Software Quality Assurance Plan (NICSD SQAP) (Reference (c7)).

The module supplier designs the modules for FPGA-based system and tests the FPGAs and the modules. The module supplier procures manufacturing of the designed modules from the printed circuit board fabricator. NICSD oversees the module supplier 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 to ensure product quality.


Vice President, PS
Technology Executive for Light Water Reactors, NED
Quality Assurance Dept.
Project QA Gr.
Senior Manager
IV&V Team
ICDD IV&V Team
Control system engineering group
Monitoring system engineering group
Instrumentation & Control Systems Design & Engineering Dept. (ICDD)
Communication
NED
Job Order (*)
Senior Manager (SM)
Quality Assurance Group (NICS-QA)
NICSD IV&V Team
Production control section
Quality Control Group (NICS-QC)
NICSD SD Tean
Nuclear Instrumentation & Control Systems Dept. (NICSD)
Module supplier
Printed circuit board fabricator
Fuchu-Complex

*) A Job Order is issued from each group in ICDD to NICSD.

Figure I-1-2 Overview of Process and Organizational Responsibilities

I-1.5.2 FPGA Logic Lifecycle Overview

Figure I-1-3 shows the lifecycle phases for the FPGA-based safety-related systems. The following phases are defined:

(1) Project Planning and Concept Definition Phase

In the Project Planning and Concept Definition Phase, the product objectives and the software integrity level are defined. The basis for the design is established, and applicable regulations and standard industry practices to be used to guide digital system development are identified in this phase.

(2) Requirements Definition Phase

In the Requirements Definition Phase, NICSD develops the Unit Detailed Design Specifications, while the module supplier develops the Module Design Specifications under the CGD from NICSD. These specifications address the intended use of the system and the associated digital logic requirements. NICSD initiates development of a Software Validation Test Plan, while the module supplier develops Module Test Procedures. These test documents are written by engineers independently other than the engineers who designed the unit and module to be tested.

(3) Design Phase

In the Design Phase, FPGA Design Specifications are developed by the module supplier under the NICSD CGD process. The FPGA Design Specifications are developed to document the details of the FPGA design.

(4) Implementation and Integration Phase

In the Implementation and Integration Phase, the code is constructed and integrated based on the FPGA Design Specifications under the NICSD CGD process, where the module supplier develops FPGA Test Procedures. The test documents are written by engineers other than the engineers who designed the FPGA to be tested.

(5) Module Validation Testing Phase

In the Module Validation Testing Phase, the module supplier performs testing in accordance with written test procedures to demonstrate that the modules perform all intended functions within the predetermined design and that the modules do not perform unintended or undesirable functions. The module supplier performs Module Validation Testing and generates a test report, which includes a test log and a listing of any testing anomalies.

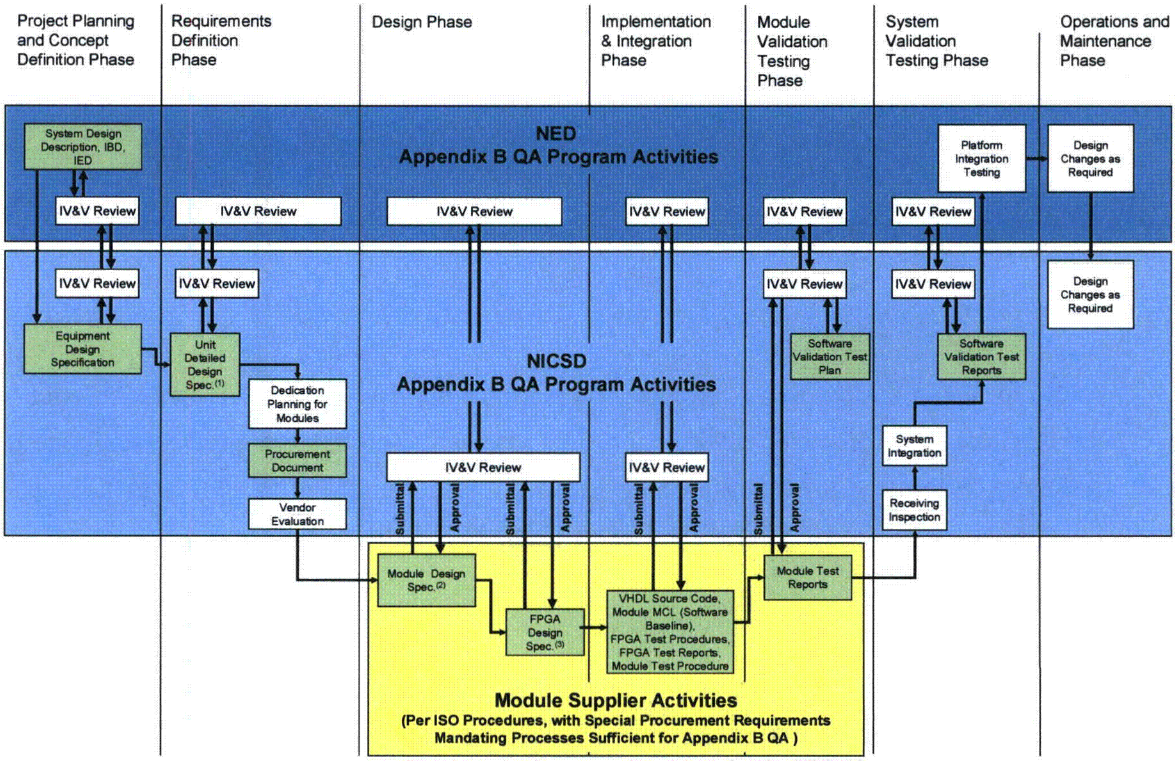
(6) System Validation Testing Phase

In the System Validation Testing Phase, testing is completed by NICSD in accordance with written test procedures to demonstrate that the unit and system performs all intended functions within the predetermined design and that the unit and system does not perform unintended or undesirable functions that are identified in the test scope.

(7) Operations and Maintenance Phase

In the Operations and Maintenance Phase, any problems are communicated to NED and NICSD for evaluation and resolution. If design changes are needed in the Operations and Maintenance Phase, change management process shall be invoked both in NED and NICSD.

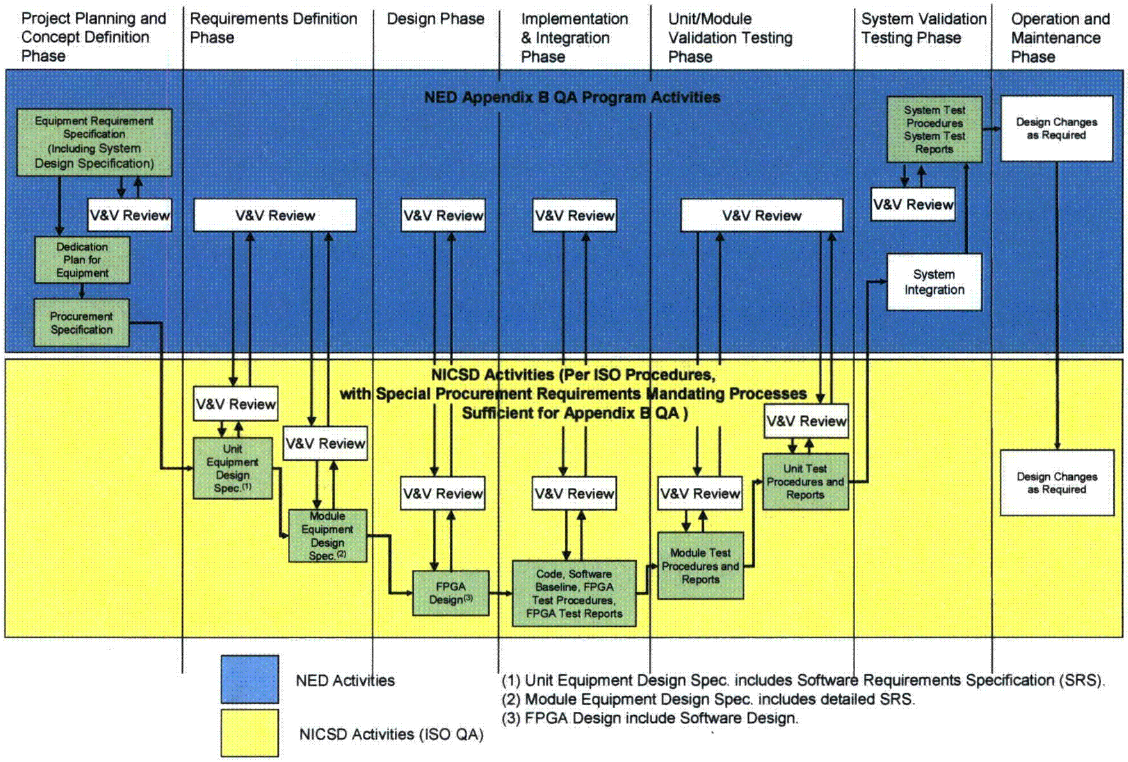
Engineers from ICDD and NICSD organize Independent Verification and Validation (IV&V) Team for the V&V of the FPGA logic. The IV&V Team conducts the V&V activities in every phase as shown Figure I-1-3.


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

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

Figure I-1-3 Lifecycle Phases in Current Process for FPGA-Based Safety-Related Systems

The original process is shown in Figure I-1-4. The PRM was developed under this original process. The significant difference from the current process is that NICSD activities were under ISO 9001 program.


Project Planning and Concept Definition Phase
Requirements Definition Phase
Design Phase
Implementation & Integration Phase
Unit/Module Validation Testing Phase
System Validation Testing Phase
Operation and Maintenance Phase
NED Appendix B QA Program Activities
Equipment Requirement Specification (Including System Design Specification)
V&V Review
Dedication Plan for Equipment
Procurement Specification
V&V Review
V&V Review
V&V Review
V&V Review
V&V Review
System Test Procedures System Test Reports
Design Changes as Required
System Integration
NICSD Activities (Per ISO Procedures, with Special Procurement Requirements Mandating Processes Sufficient for Appendix B QA)
V&V Review
Unit Equipment Design Spec.(1)
V&V Review
Module Equipment Design Spec.(2)
V&V Review
FPGA Design(3)
V&V Review
Code, Software Baseline, FPGA Test Procedures, FPGA Test Reports
V&V Review
Module Test Procedures and Reports
V&V Review
Unit Test Procedures and Reports
Design Changes as Required
NED Activities
NICSD Activities (ISO QA)

(1) Unit Equipment Design Spec. includes Software Requirements Specification (SRS).
(2) Module Equipment Design Spec. includes detailed SRS.
(3) FPGA Design include Software Design.

Figure I-1-4 Lifecycle Phases in Original Process for FPGA-Based Safety-Related Systems

I-1.5.3 Commercial Grade Dedication (CGD)

NED procures the assembled FPGA-based systems equipment from Nuclear Instrumentation & Control Systems Department (NICSD).

NICSD procures the modules for the FPGA-based equipment from the Toshiba groups that design and supply modules (which will be referred to as the "module supplier" throughout this LTR) under the Commercial Grade Dedication (CGD) program as defined in the CGD plan (Reference (c4)), and assembles the equipment from the modules under its Appendix B QA program. In the Original Process, NED procured the FPGA-based equipment from NICSD under NED CGD program since NICSD had not yet established their Appendix B QA program.

The logic embedded in FPGA chips on the module printed circuit board have been designed and tested by the module supplier under their ISO 9001 QA program. NICSD dedicates the FPGA logic for FPGA-based safety-related application under the NICSD CGD process. NICSD does not modify or customize the FPGA logics procured from the module supplier. The evaluation process for the FPGA logic under NICSD CGD process is described in the CGD plan.

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. During the Requirements Definition Phase, NICSD conducts a vendor evaluation of the module supplier before ordering from the module supplier. NICSD oversees the module supplier activities from the Design Phase through the Module Validation Testing Phase, accepting each commercial work product into the NICSD nuclear quality assurance program. After NICSD receives the modules from the module supplier, NICSD integrates FPGA-based systems and conducts System Validation Testing. After the System Validation Testing, NICSD ships the FPGA-based systems.

The NICSD Software Development (SD) Team is responsible for technical evaluation of FPGA logic, and prepares the selected dedication documents in the following list.

- CGD Plan
- Preliminary Technical Evaluation Report (PTER)
- Procurement Planning Sheet (PPS)
- Commercial Dedication Instruction (CDI)
- Procurement Document
- Critical Digital Review (CDR) Report
- CGD Report
- Final Technical Evaluation Report (FTER)
- CGD Package

The NICSD SD Team is responsible for determining the acceptance methods and criteria for Commercial Grade Items (CGIs) and Commercial Grade Services (CGSs). NICS-QA conducts a Commercial Grade (CG) Survey when required by the NICSD SD Team, and prepares a CG Survey Report. NICS-QC is responsible for conducting the source verification of supplier, receiving inspection of CGIs, and special test and inspection in accordance with the instruction specified by the NICSD SD Team.

The NICSD SD Team and the NICSD IV&V Team with support from the NICSD SQA Team perform an evaluation of FPGA logic. The NICSD Software Safety Team participates in the evaluations. The NICSD SD Team, NICSD IV&V Team, and NICSD Software Safety Team ensure completion, documentation, and maintenance of these evaluations.

The NICSD IV&V Team reviews the supplier's documents, and prepares Design Verification Reports (DVRs) as required in the NICSD VVP (Reference (c9)).

The NICSD Software Safety Team performs the safety analysis activity for module and FPGA design, Very High Speed Integrated Circuit Hardware Description Language (VHDL) source code, FPGA and module testing as required in the NICSD SMP (Reference (c3)), and documents the result of the analyses in the NICSD Software Safety Analysis Reports (SSARs).

I-2 QA Program

I-2.1 Quality Assurance Programs

The Power Systems Nuclear Energy (PSNE) division of the Toshiba Power Systems Company (Toshiba PS) has several established QA programs, based on International Organization for Standardization (ISO) 9001 and 10 CFR 50 Appendix B (Reference (a2)). PSNE established and has been maintaining a QA program complying with US nuclear safety regulations since April 2006.

The QA Program Description (QAPD, Reference (b1)) is the top level QA document of the 10 CFR 50 Appendix B QA program of PSNE. The QAPD includes methods pertaining to managerial and administrative control that meet the requirements of 10 CFR 50 Appendix B, USNRC Regulatory Guide 1.28-1985 (Reference (a8)), and American Society of Mechanical Engineers (ASME) Nuclear Quality Assurance (NQA)-1-1994, and NQA-1-2008 and the NQA-1a-2009 Addenda (Reference (a3)).

The PSNE Regulations and Procedures (R&Ps) make up some of the second level QA documents. These high level QA documents are applied to all PSNE organizational units.

The PSNE R&P "Reporting Procedure for Defects and Noncompliance under USNRC 10 CFR 21" (Reference (b2)) describes the procedure for ensuring compliance with the requirements of 10 CFR 21, "Reporting of Defects and Noncompliance" (Reference (a1)).

NED based in Toshiba's Isogo Nuclear Engineering Center is responsible for all PSNE activities except manufacturing. The 10 CFR 50 Appendix B QA program of NED is based on the PSNE QAPD, the R&Ps, and the NED AS standards (hereinafter referred to as AS standards).

Departments within NED, which are involved in the process documented in the LTR, include:

- The Instrumentation & Control Systems Design and Engineering Department (ICDD), which is responsible for system design and engineering of I&C products.
- The Quality Assurance Department, which is the key QA organization of PSNE.

The Power Systems Segment of Fuchu Complex (Fuchu-PS) is the detail design and manufacturing organization of electrical equipment for nuclear power plants, and has a QA

Manual that conforms to ISO 9001. NICSD is a department located at the Fuchu Complex which is part of PSNE. NICSD has a QA Program that utilizes the PSNE QAPD and conforms to 10 CFR 50 Appendix B. NICSD dedicates items and services procured from other organizations in the Fuchu-PS including the module supplier. Note that during the development of the PRM for the BWR-5, NICSD worked under their original ISO 9001 process and NED performed the CGD activities of all NICSD work. The functions and responsibilities for these departments are as follows.

- NICSD designs, tests, and performs manufacturing of safety-related systems for nuclear power plants under QAPD. NICSD performs CGD of items produced from commercial grade suppliers including the other departments in Fuchu-PS.
- The module supplier designs, tests, and performs the manufacturing of components for safety-related systems for nuclear power plants under Fuchu-PS's ISO 9001 QA Manual.

Section I-2.1.1 describes how the QA Program Description is used in PSNE including NED.. Section I-2.1.2 describes the QA program of NICSD and how NICSD dedicates the products from other organizations at Fuchu-PS. Section I-2.1.3 describes the major features of the module supplier's QA program related to activities for safety-related systems. Section I-2.2 of this Part of the LTR describes surveys and audits related to supplier procurements applicable to the LTR.

Section I-2.3 of this Part of the LTR describes the Critical Digital Review (CDR) process to evaluate software processes used by suppliers, and the results of CDRs. For the PRM Qualification Project, NED used the CDR process to evaluate the then ISO 9001 program of NICSD and Actel who was the key supplier for FPGA tools.

I-2.1.1 PSNE Quality Assurance Program Description

The PSNE QAPD (Reference (b1)) defines specific responsibilities and authority for control of design, documentation, procurement, processes, inspection, testing, nonconformance, corrective action, and QA records. In addition, the PSNE QAPD defines requirements for inspection and audits. NQAD is responsible for maintaining the PSNE QAPD.

In addition to controlling design and procurement, the PSNE QAPD also establishes the quality system document structure, which includes the following:

- PSNE Regulations and Procedures: Describing the measures that should be applied to all PSNE to support the QAPD. Those measures are associated with education, management review, contract agreement, equipment qualification and 10 CFR 21 issues. This series of standards is identified as "Regulations and Procedures (R&P)."

- NED standards: Providing requirements for activities to be performed in accordance with the PSNE QAPD. This series of standards is identified as "AS" standards.

AS standards prescribe design control, procurement control, and test control measures, as well as the software design and Commercial Grade Dedication (CGD) processes. Many of these AS standards are applied for the process documented in the LTR.

All NED activities for the process described in the LTR are performed under the PSNE QAPD, compliant with 10 CFR 50 Appendix B QA requirements.

I-2.1.2 NICSD QA Program

In 2008, NICSD established the QA program complying with 10 CFR 50 Appendix B (Reference (a2)) for their work in Fuchu Complex. This QA program is used for activities affecting the quality of nuclear safety-related items and services for nuclear power plants licensed in the United States. Using this program, NICSD meets the requirements of the PSNE QAPD (Reference (b1)). Thus, for design and manufacturing of nuclear safety-related items and services, NICSD works under the PSNE QAPD, the PSNE regulations and procedures, and the applicable AS standards.

In addition to applicable AS standards, NICSD established their own Nuclear Quality (NQ) Standards as the second level procedures to implement regulatory requirements.

NICSD personnel follow the process for performing and documenting design activities to assure that applicable US regulatory requirements, including the design basis as defined in 10 CFR 50.2 and as specified in the license application, are correctly translated into the design output documents.

The NICSD Software Management Plan (SMP) (Reference (c3)) defines the lifecycle process steps applied to development and qualification of FPGA products supplied by NICSD including design activities, V&V activities, software safety analysis activities, and software QA activities. The NICSD Software Quality Assurance Plan (SQAP) (Reference (c7)) was developed using IEEE Std 730 (Reference (a35)) as a guide. The NICSD SQAP describes the software quality assurance activities performed by NICSD, including the Commercial Grade Dedication (CGD) activities used to designate commercial grade items from the module supplier for use in safety-related applications. The details of software QA activities are described in Section I-3.4 of this Part of the LTR.

As mentioned in Section I-2.1, NICSD and the module supplier are jointly developing FPGA-based I&C systems. The module supplier is the organization for manufacturing of FPGA-based components in the Power Systems Segment of Fuchu Complex (Fuchu-PS). After the separation of NICSD and the module supplier in 2006, NICSD uses the module supplier for the FPGA-based component design and manufacturing, and controls the module supplier's work under the NICSD procurement control process. Especially, after the establishment of NICSD's 10 CFR 50 Appendix B QA Program (Reference (a2)) in 2008, NICSD and the module supplier have applied different QA programs for manufacturing of safety-related systems and components.

NICSD uses its Commercial Grade Dedication (CGD) process to accept the module supplier components into the NICSD QA program. NICSD performs dedication of Commercial Grade Items (CGIs) procured from the module supplier, based on the process described in EPRI NP-5652 (Reference (a42)), EPRI TR-102260 (Reference (a43)) and TR-106439 (Reference (a45)). During the software life cycle phases where the module supplier performs work, NICSD verifies the module supplier activities though CGD and IV&V activities as described in the CGD Plan (Reference (c4)).

I-2.1.3 Module Supplier QA Program

The module supplier works under their ISO 9001 QA program and maintains its own set of procedures for to support the FPGA-based component design, development, manufacturing, and test. NICSD reviews and accepts the module supplier procedures. NICSD reviews the commercial work performed and accepts it under NICSD's commercial grade dedication program. NICSD staff have the capabilities to perform the module supplier's work, and are thus technically competent to review and approve the module supplier's work.

I-2.2 Supplier Evaluations

Prospective suppliers are surveyed and/or audited to ensure that the supplier will reliably provide products meeting NED and NICSD's requirements. This section describes the surveys and audits performed that are applicable to activities covered by the LTR.

PSNE (both NED and NICSD) perform supplier qualification activities. PSNE's evaluations are performed in accordance with the QAPD (Reference (b1)). Key features of PSNE's supplier evaluation process include:

- Prospective suppliers are evaluated by survey or documentation review.
- A Survey Plan is prepared to document and identify the survey scope, requirements, audit personnel, activities to be surveyed, etc.
- The audit team includes one or more qualified auditors.
- A Survey Checklist is prepared and used.
- Survey results are documented in reports.
- Acceptable suppliers are registered on a Qualified Vendors List (QVL).
- Qualified suppliers for safety-related systems are audited or evaluated annually, and surveyed every three years.
- Commercial grade suppliers of CGI for safety-related systems, who are qualified by Commercial Grade (CG) Survey, are audited or evaluated annually, and surveyed every three years.

NICS-QA performs a CG Survey of a commercial grade supplier. The CG Survey determines if the critical characteristics that can be accepted by survey, as documented in the Commercial Dedication Instruction (CDI). Depending on the results of the CG Survey, NICSD may decide to place additional requirements in procurement documents when orders are placed with commercial grade suppliers. The following subsections describe how PSNE evaluates and controls their supplier by survey and audit.

I-2.2.1 Commercial Grade Survey of NICSD

In the original QA process, NED performed its first CG Survey of NICSD to evaluate the supplier's quality capability in 2005. The results of the survey were documented in the CG Survey Report (Reference (d1)). Based on the results of the survey, NICSD was registered on NED's Qualified Vendor List (QVL) in 2005 with conditions related to survey observations. NED performed a follow-up survey of NICSD in 2005 to cover critical characteristics to be verified by the CG Survey. The results of the follow-up survey were documented in the CG Survey Report (Reference (d2)). The CG Survey Report stated that the NED survey team recognized that the documented quality assurance program of NICSD was established and effectively implemented.

I-2.2.2 Commercial Grade Survey of Module Supplier

In the current QA process, NICSD performed the first survey of the module supplier as a preparatory survey of a prospective commercial grade supplier in 2009. The survey was performed to evaluate the capability of the module supplier to provide commercial grade items and services as a commercial grade supplier to NICSD. The first survey of the module supplier was performed as preliminary survey before the critical characteristics were identified, so the survey was compliance-based rather than performance-based evaluation. The module supplier was registered in the NICSD's Qualified Vendor List (QVL) as a commercial grade supplier with restriction to prohibit issuing any order prior to identification of critical characteristics, even though the survey was completed successfully. The results of NICSD's first survey of the module supplier were documented in the "Survey/Audit Report" (SE09SR-001 R0) (Reference (d3)). The survey report stated that the NICSD survey team recognized that the module supplier's documented quality system was established and effectively implemented with the condition described in the report.

NICSD performed the Commercial Grade (CG) Survey of the module supplier to resolve the restriction attached to the module supplier in the NICSD's QVL in 2010. The results of this CG Survey of the module supplier were documented in the "Survey/Audit Report" (SE10SR-001 R0) (Reference (d6)). The survey report stated that the NICSD survey team recognized the specified critical characteristics as acceptable, provided that the finding described in this report is resolved.

In 2011, the follow up CG Survey was performed to confirm the implementation of corrective actions, control of software tool, and control of Function Element (FE) for FPGA-based modules. These were identified as additional critical characteristics in the CDI while preparing software planning documents. The results of this CG Survey of Fuchu-PS were documented in the "Commercial Grade Survey Report" (SE10SR-001a R0) (Reference (d35). The survey report stated that the NICSD survey team recognized the result of this survey as acceptable, which resolved the earlier findings.

Because the module supplier is one department of Fuchu-PS, the module supplier is expressed as Fuchu-PS in the above survey reports and NICSD's QVL.

I-2.2.3 Survey of Printed Circuit Board Fabricator

NQA-1 (Reference (a3)) requires that the procurement documents to the supplier specify appropriate quality assurance program requirements in sub-tier procurement documents.

In the original QA process, NED issued a Job Order to NICSD indicating the QA program requirements for the PRM Qualification Project. NICSD and the printed circuit board fabricator agreed on the improvement of process control to prepare written procedures, to apply traceability sheets such as shop travelers for printed circuit boards manufacturing, and to issue certificates of conformance (C of C) from the printed circuit board fabricator. To demonstrate the improved process, NICSD issued an order of printed circuit board manufacturing to the printed circuit board fabricator. NICSD performed an audit of the printed circuit board fabricator in accordance with the supplier audit process of the ISO 9001 QA program in 2005. The NICSD audit team confirmed that the printed circuit board fabricator successfully performed the order. NICSD audited the printed circuit board fabricator again in 2007.

In the current QA process, the printed circuit board fabricator is a manufacturer of printed circuit boards and supplies printed circuit boards for FPGA-based modules in accordance with the purchase order issued by the module supplier. Since NICSD recognized that the printed circuit board fabricator is important for quality of FPGA modules, NICSD surveyed the printed circuit board fabricator in 2009. The results of the survey were documented in "Survey/Audit Report" (SE09SR-002 R0) (Reference (d4)). Even though NICSD does not directly acquire parts from the printed circuit board fabricator, the printed circuit board fabricator was recorded as an important sub-tier supplier in NICSD's QVL. During the survey, one issue was identified. The survey team recommended that the printed circuit board fabricator should record not only the check mark that shows that the measured value of the reflow soldering tub temperature is within documented limits, but also the actual measured value in a daily inspection list. This issue has been subsequently resolved.

NICSD performed the annual evaluation of the printed circuit board fabricator in 2010 and 2011. At both of these annual evaluations, no issues were identified. The results of these annual evaluations were documented in "Evaluation Report" (SAER10-002 (Reference (d7)), and SAER11-002 (Reference (d8))

I-2.2.4 Survey of Microsemi SoC (formerly Actel)

Actel Corporation was Toshiba's sole acceptable FPGA device and related tool supplier for safety-related equipment. Toshiba selected the Actel parts for many reasons. One important reason was Actel's agreement with the US Department of Defense (DoD) and National Aeronautics and Space Administration (NASA) to produce and support these devices for a thirty year period. While this agreement postpones the inevitable time when the devices will be obsolete, the agreement does not eliminate obsolescence as an issue. When Actel no longer produces and maintains these parts, Toshiba will evaluate other suppliers and select another FPGA supplier. While the process described in this LTR describes Actel parts and software tools, Toshiba expects to use this basic supplier selection process, with likely enhancements based on changes to the state of the art in FPGA design and development, as the basis for a new process for providing future FPGA-based systems. The new process might be different enough to require a new LTR, or at least a supplement to this LTR. Toshiba also notes that process improvements may be made in the FPGA design and development process defined in this LTR, as enhancements occur to software tools and the state of the art methods used in FPGA design and development. If this occurs, Toshiba expects to provide a supplement to this LTR as a part of a utility submission of a safety system, as suggested by the USNRC.

Microsemi Corporation acquired Actel Corporation in 2010. The Microsemi SoC Products Group (abbreviated as Microsemi SoC in this LTR) continues to supply the FPGAs used by Toshiba FPGA platform. The LTR uses both names (i.e. Actel and Microsemi SoC) interchangeably. This status makes Actel a key supplier to Toshiba; hence, NICSD performed a QA survey of Actel, the supplier of the FPGA components in 2005 and 2009.

In the original QA process for the PRM Qualification Project, NICSD performed the first audit of Actel in accordance with the supplier audit process of the ISO 9001 QA program of in July 2005. The audit team concluded that Actel maintained an ISO 9001 level quality assurance program that was considered sufficient to provide Toshiba with FPGA components on a commercial basis, including identification and control of design changes, procurement control (for fabrication and assembly), and inspection and testing of the FPGA parts of interest to Toshiba. Actel's quality process controls used in the areas of sub-tier supplier monitoring, inspection and test, and control of product changes were well defined. Also, Actel's product identification and controls of the commercial components were sufficient to maintain the traceability to design records, fabrication lots, and the manufacturing travelers. Based on the results of this QA audit, Actel was registered on the supplier list of Fuchu Complex as the supplier of commercial FPGA components.

In the current QA process, the survey team consisted of staff from NED, NICSD and the module supplier performed a QA survey of Actel in November 2009. At this time, NICSD had established their 10 CFR 50 Appendix B QA program, so this survey was performed as a survey of a commercial grade supplier. Even though NICSD does not purchase these parts directly, Actel was recorded as an important sub-tier supplier in NICSD's QVL. The results of this survey were documented in the "Survey/Audit Report" (SE09SR-004 R0) (Reference (d5)). The survey report states that the survey team recognized the Actel quality system was established, documented and effectively implemented. Identified findings and recommendations were closed by June 10, 2010. The module supplier prepared a survey report in accordance with the audit procedure defined by Fuchu-PS.

In December 2010, NICSD sent the annual evaluation inquiry to Microsemi SoC, who replied in February 2011. The results of the annual evaluation were acceptable and documented in the "Evaluation Report" (SAER10-004) (Reference (d9)). The evaluation report concluded that the supplier had the capability to provide items or services within the scope of activity without limitation.

I-2.3 Use of Critical Digital Review for External Suppliers

A Critical Digital Review (CDR) is a technical review of a software development process as defined in EPRI TR-106439 (Reference (a45)). CDR is a tool that can be used in the supplier selection and evaluation process (as part of CGD activities). Results of a CDR may identify additional activities to be performed by either the buyer or supplier to mitigate design issues, process deficiencies, or quality concerns. NED and NICSD uses this tool to control and enhance supplier processes related to FPGA logic development to ensure that quality of FPGA logic meets a level sufficient for nuclear safety-related applications. NED and NICSD perform CDRs using the guidance provided by EPRI TR-107339 (Reference (a47)). NED and NICSD perform CDRs to determine whether the processes at suppliers or sub-tier suppliers who provide software or software-like products are in accordance with the technical and QA requirements.

When the PRM Qualification Project was performed, NED implemented a CDR of NICSD, as a means of evaluating the architecture and processes NICSD would use to design, build, analyze, verify, and validate the FPGA-based system designs. Because software tools used in FPGA development are critical to the quality of the FPGA-based systems, NED and NICSD performed CDRs of the supplier of these tools, the Microsemi SoC as described in Section I-2.3.2.

The CDRs of NICSD and Microsemi SoC focused on:

- Architectural review
- Process review
- Hazard analysis for products and software tools
- Operating history survey

I-2.3.1 Critical Digital Review of NICSD

When the PRM Qualification Project was performed, NED implemented a CDR of NICSD for the project in 2005, as a means of evaluating the architecture and processes NICSD would use to design, build, analyze, verify, and validate the FPGA-based system designs. The CDR team reviewed the hardware architecture, the application architecture, the software configuration tools, and NICSD's hardware and software development and testing processes for FPGA-based I&C systems, using interviews with key NICSD personnel representing the above disciplines and technical reviews of design and development documentation, including internal design control procedures. The CDR report was prepared. The CDR reviewers found the NICSD development process to be rigorous and robust and the engineers to be of high caliber. The CDR Report concluded that the methods used for the FPGA-based PRM were suitable for use in producing safety-related devices for US nuclear utilities.

I-2.3.2 Critical Digital Review of Microsemi SoC

Toshiba concluded that a review of the Actel toolset was necessary, because the Actel toolset provides the translation and transformation of human-readable VHDL code into digital logic circuits, and embeds that logic in the FPGA. Accordingly, NED and NICSD engineers performed CDR reviews of the Actel toolset and Actel development practices. The first CDR was conducted in 2005 at the Actel headquarters offices in Mountain View, California. The second CDR was performed as a follow-up CDR to evaluate revisions to the Actel toolset in 2009. The CDR reports were prepared.

The CDR reviewers concluded that the programmed FPGAs generated by these tools were appropriate for safety-related use, provided that NICSD and the module supplier continue to implement the processes evaluated in the earlier NICSD CDR. The CDR reviewers concluded that the Actel tools, used with the Toshiba processes, were acceptable for use in transforming human-readable source code into digital logic embedded into FPGAs.

I-2.4 QA Process Applied to PRM Qualification Project

The Toshiba Power Range Monitor (PRM) was developed by using the original QA process. The changes from the original QA process are described in Appendix I-A.

In the original QA process, NICSD had not established the QA program complying with 10 CFR 50 Appendix B (Reference (a2)), and was not considered part of PSNE. NICSD, as a commercial grade supplier to NED, worked under the ISO 9001 based QA program. NED applied the Commercial Grade Dedication (CGD) process to items and services procured from NICSD. NED performed a CG Survey, and a Critical Digital Review of NICSD and Actel as described in Sections I-2.2.1, I-2.2.4, I-2.3.1, and I-2.3.2, to verify the software control process of the key suppliers. NED implemented the PRM qualification test at a test facility in US. To control the test under the 10 CFR 50 Appendix B QA program, NED trained test staff from NICSD to work under the NED 10 CFR 50 Appendix B QA program. NED prepared the qualification analysis report of PRM. NED performed these activities in accordance with PSNE QAPD and AS standards.

I-3 Software/Hardware Development Process

I-3.1 Generic Process

FPGA-based I&C systems do not use application software like microprocessor based systems. Toshiba FPGA-based systems use direct implementation of algorithms in logic within the FPGA. However, Toshiba uses the Very High Speed Integrated Circuit Hardware Description Language (VHDL) for designing and implementing FPGA circuits. This VHDL language looks much like software code.

Because VHDL is inherently parallel, logic is executed in parallel using logic gates, which start changing as soon as a new input arrives. A VHDL program mimics the behavior of an analog system. It also requires incorporation of timing specifications, such as gate delays and setup and hold times, into the design process.

The use of digital systems presents the concern that minor errors in design and implementation can cause unexpected system behavior. To minimize this potential problem, Toshiba's design qualification for the FPGA-based systems uses a high quality lifecycle process that incorporates disciplined specification and implementation of design requirements. This reduces the potential for common cause logic failures.

After careful evaluation of several different approaches to FPGA logic design, including approaches used by several industrial companies involved in safety-critical, high integrity design, Toshiba decided to use a logic design approach similar to that used with software. While there are several obvious differences between the software running in a CPU and hardwired logic embedded in an FPGA, there are several key similarities.

The most important similarity is that the VHDL language which defines the FPGA logic has many of the same characteristics as software created using procedural languages, including complexity, variable range, and abstraction. While the concept of a safety system is fairly simple, the large number of details, the number of FPGAs required to implement the safety system, and the project goal of creating a maintainable system, led Toshiba to decide to use a modified software lifecycle approach to FPGA logic design. This approach includes the same sorts of documentation and performance of the same kinds of reviews and tests that would be prepared for a CPU-based system. Toshiba decided to start with the IEEE software standards, USNRC regulations, and USNRC regulatory guides to define their process.

Toshiba modified the software processes for FPGA-specific issues, since the existing IEEE software standards, USNRC regulations, and USNRC regulatory guides were designed for traditional software lifecycles in CPU-based systems. This customization considered the differences between procedural-based software and hardwired logic, which requires Toshiba to modify the details of the standard software design process to fit the requirements for VHDL coding and logic design. The modifications to the software process were incorporated into the project quality assurance plan, QA standards, and the associated work instructions used by Toshiba engineers. The resulting FPGA-based logic design process documentation is very similar to that resulting from a traditional software process. Thus, Toshiba has elected to retain the word "software" in the titles and documents to be prepared for FPGA-based systems, to indicate the original source of the process and documentation requirements.

Table I-3-1 shows how the software-based processes were adapted for use in activities to be performed during development of FPGA logic. This table identifies the software tools required to perform FPGA logic development activities. These software tools are explained in Section I-3.3.10.

Table I-3-1 Software and Related FPGA Processes

Software Process Step	Typical Software Activity	FPGA Process Step	FPGA Logic Development Activity
Design	Translate system requirements into a Software Requirements Specification, Software Detailed Design, Software Code, and Testing Procedures	Design, Coding, Test Procedure Development	Translate system requirements into Unit Detailed Specifications containing requirements and detailed designs; translate Unit Detailed Specifications into Module Design Specifications containing requirements and detailed designs; translate Module Design Specifications into FPGA Design Specifications containing requirements, detailed FPGA design documents, testing procedures, and hardware description language
Verification	Verify translation of system requirements into Software Requirements Specification; verify translation of Software Requirements Specification into Software Detailed Design; verify translation of Software Detailed Design into code	Verification	Verify translation of system requirements into Unit Detailed Design Specifications; verify translation of Unit Detailed Design Specifications into Module Design Specifications; verify translation of Module Design Specifications into FPGA Design Specifications; verify translation of FPGA Design Specifications into code
Compile	Transform source code into object file	Logic Synthesis	Transform hardware description language source into logic netlist (Logic synthesis tool)
Software Module Test	Generate additional software to drive and monitor test operation of a software module and test the software module using stubs and drivers	FPGA Testing	Simulate Functional Element (FE) *1 and FPGA operation with the FPGA simulation tool For FEs, add FPGA inputs and outputs, program FPGA, stimulate FPGA with the FPGA simulation tool and FPGA adaptor
Link	Combine object files and libraries and possibly an operating system to produce executable image	Place & Route	Transform logic netlist into placed netlist (Place and route tool). Transform placed netlist into fuse map
Installation	Install the executable image in read-only memory	Implementation	Embed fuse map in FPGA (FPGA programming tool)
Test	Verify correct operation of interfaces between tested modules	FPGA Testing	Verify operation of the FPGA logic in software simulation and by stimulating a programmed FPGA with the FPGA simulation tool and FPGA adaptor

Note *1: Refer to Section II-2.1.1 for detailed description of the "Functional Element (FE)."

Table I-3-1 also shows design documents generated during development of FPGA logic. Figure

I-3-1 augments Table I-3-1 showing the detailed activities, outputs and software tools in each FPGA process step.

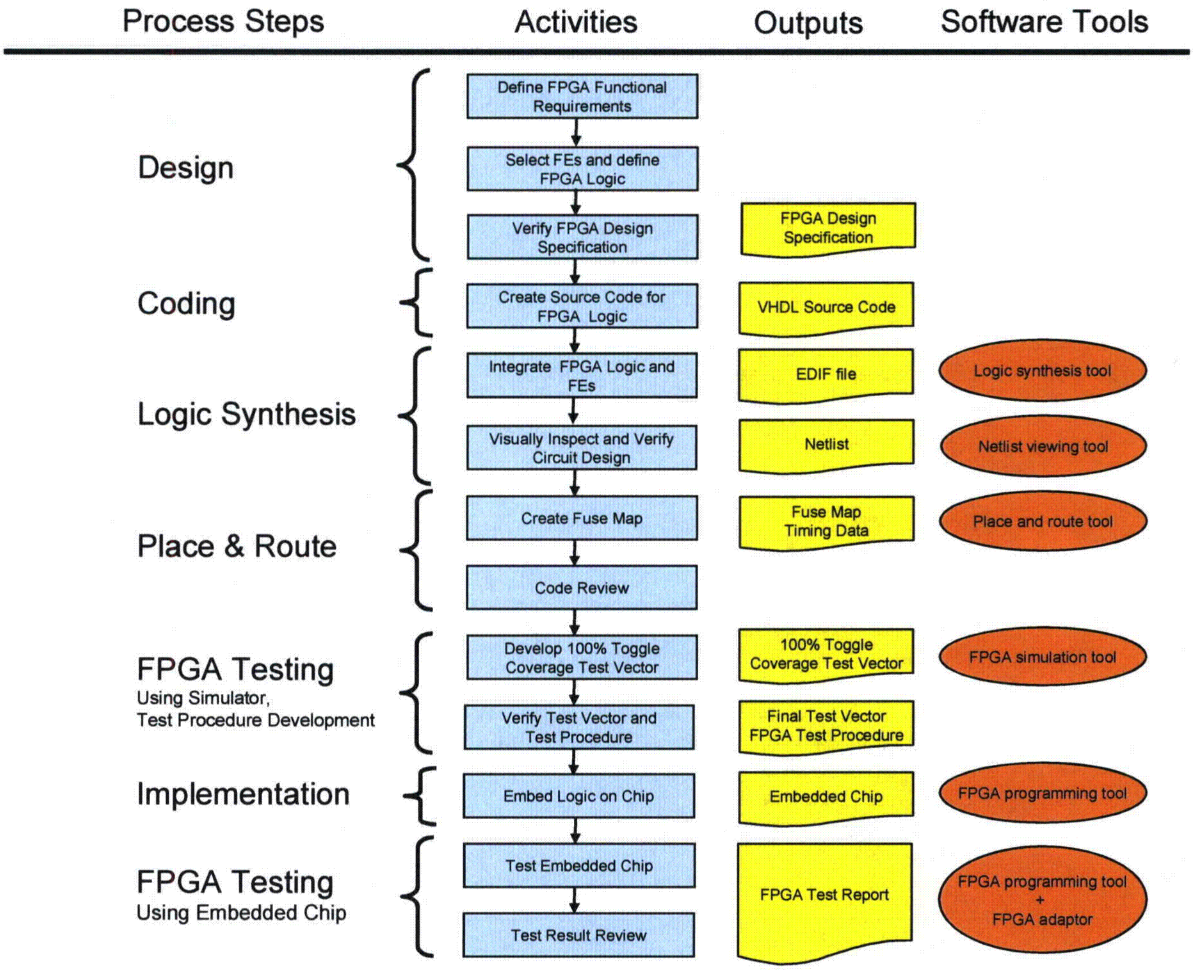

Process Steps
Activities
Outputs
Software Tools
Design
Define FPGA Functional Requirements
Select FEs and define FPGA Logic
Verify FPGA Design Specification
FPGA Design Specification
Coding
Create Source Code for FPGA Logic
VHDL Source Code
Logic Synthesis
Integrate FPGA Logic and FEs
EDIF file
Logic synthesis tool
Visually Inspect and Verify Circuit Design
Netlist
Netlist viewing tool
Place & Route
Create Fuse Map
Fuse Map Timing Data
Place and route tool
Code Review
FPGA Testing
Using Simulator,
Test Procedure Development
Develop 100% Toggle Coverage Test Vector
100% Toggle Coverage Test Vector
FPGA simulation tool
Verify Test Vector and Test Procedure
Final Test Vector FPGA Test Procedure
Implementation
Embed Logic on Chip
Embedded Chip
FPGA programming tool
FPGA Testing
Using Embedded Chip
Test Embedded Chip
Test Result Review
FPGA Test Report
FPGA programming tool + FPGA adaptor

Figure I-3-1 FPGA Process Steps

Having this level of design documentation means that all the logic in the system is documented, the designer's intent is written down, the system can be reviewed by someone other than the designer, and the system can be more easily maintained. For complex devices like FPGAs, software tools are necessary for programming the FPGA logic, as these devices are well beyond the complexity where manual methods are effective.

As part of this process, all designers work to the same VHDL coding guidance. Thus, the logic produced has many common design attributes, which a less disciplined process would not necessarily produce. This makes it possible for all designers to understand each other's work, without intense study of an unfamiliar design.

As with software, documenting the initial system requirements and decomposing those requirements through systems, units (chassis), modules, individual FPGAs, and down to FEs and VHDL logic made it possible for Toshiba to trace requirements through the decomposition, which requires the provided level of documentation to support a complete, thorough review.

I-3.1.1 Regulatory Criteria

Ultimately, the basis for the qualification of Toshiba FPGA-based I&C systems is the USNRC Standard Review Plan (SRP), NUREG-0800 (Reference (a4)), Chapter 7, "Instrumentation and Controls."

This section identifies regulations and industry standards to be applied for the qualification process, and the processes put in place by Toshiba to comply with these regulations and standards.

The SRP contains specific requirements for the digital aspects of instrumentation and control equipment. Toshiba used the SRP to gain understanding of US nuclear regulatory positions, and to verify that the plans, procedures, and processes created fulfill regulatory expectations. These requirements are contained in:

- Section 7.1 of SRP, "Instrumentation and Controls – Introduction."
- Appendix 7.0-A of SRP, "Review Process for Digital Instrumentation and Control Systems."
- BTP 7-14 (Reference (a5)), "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems."
- BTP 7-18, (Reference (a7)), "Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems."

Toshiba used the following regulatory guides to establish the requirements for the FPGA-based system processes:

- USNRC Regulatory Guide 1.152 Rev. 3 (Reference (a11)) endorsing IEEE Std 7-4.3.2-2003 "IEEE Standard Criteria for Digital Computers in Safety Systems of

Nuclear Power Generation Stations" (Reference (a30))

- USNRC Regulatory Guide 1.153 Rev. 1 (Reference (a12)) endorsing IEEE Std 603-1991 "IEEE Standard for Safety Systems for Nuclear Power Generating Stations" (Reference (a36))

Toshiba reviewed and used the guidance provided in the following software Regulatory Guides:

- USNRC Regulatory Guide 1.168 "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 1 (Reference (a13))
- USNRC Regulatory Guide 1.169 "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Reference (a14))
- USNRC Regulatory Guide 1.170 "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Reference (a15))
- USNRC Regulatory Guide 1.171 "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Reference (a16))
- USNRC Regulatory Guide 1.172 "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Reference (a17))
- USNRC Regulatory Guide 1.173 "Developing Software Lifecycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Reference (a18))
- USNRC Regulatory Guide 1.180 "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," Revision 1 (Reference (a19))

USNRC Regulatory Guide (RG) 1.152 Rev. 3 states that conformance with the requirements of IEEE Std 7-4.3.2-2003, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," is a method that the USNRC staff has deemed acceptable for satisfying the USNRC's regulations for high functional reliability and design requirements for computers used in safety systems of nuclear power plants.

The requirements specified in RG 1.168, Revision 1, and IEEE Std 1012-1998 (Reference (a38)) provide an approach that is acceptable to the USNRC staff for meeting the requirements of 10 CFR 50 and the guidance given in RG 1.152. USNRC RG 1.168 endorses and provides guidance for use of IEEE Std 1012-1998 as an acceptable methodology for implementing the verification and validation of safety system software, subject to certain exceptions listed in that Regulatory Guide.

IEEE Std 7-4.3.2-2003 and RG 1.168 require the performance of Verification and Validation in accordance with IEEE Std 1012-1998 for the highest software integrity level (SIL) (Level 4).

Toshiba developed a FPGA logic lifecycle process describing the specific tasks and responsibilities for FPGA-based system development in accordance with BTP 7-14, RG 1.152, IEEE Std 7-4.3.2-2003, RG 1.168, and IEEE Std 1012-1998.

Toshiba believes that the process implemented fulfills the requirements of RG 1.152 and IEEE Std 7-4.3.2, as well as V&V in RG 1.168, IEEE Std 1012, and IEEE Std 1028 (Reference (a39)).

Toshiba used the concepts from both RG 1.152 and RG 1.168 to develop the FPGA logic lifecycle. However, the lifecycle practices Toshiba uses for FPGA-based systems do not follow a traditional software programming lifecycle exactly. Toshiba modified the software lifecycle practices defined in these standards to meet the needs of Toshiba's FPGA logic processes.

Modifications to the standard lifecycle did not delete functions and processes; rather, the functions and processes were extended and enhanced. While additional levels of design documents exist in the Toshiba process, all documents are subjected to the peer reviews, testing, verification, validation, safety analysis, configuration management, change control, project controls, and other processes defined in the regulatory guides and IEEE standards.

Table I-3-2 maps the life cycle phases of the BTP 7-14, IEEE Std 1012, and the FPGA-based systems. As shown in the third column of Table I-3-2, Toshiba defined a lifecycle phases for the FPGA-based systems.

Table I-3-2 Mapping of Life Cycle Phases

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

Note 1: The "Design" FPGA process step shown in Figure I-3-1 is mapped to the "Design" Phase of Toshiba FPGA-based systems lifecycle shown in this table, while the other FPGA process steps are mapped to "Implementation and Integration" Phase.

Figure I-1-3 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. During the Requirements Definition Phase, NICSD conducts a vendor evaluation before ordering from the module supplier. NICSD oversees the module supplier activities from the Design Phase through the Module Validation Testing Phase under the NICSD CGD process. After NICSD receives the modules from the module supplier, NICSD integrates FPGA-based systems and conducts System Validation Testing. After the System Validation Testing, NICSD ships the FPGA-based systems to the customer. In the Operations and Maintenance Phase, Toshiba will support operations and maintenance activities.

The SRP BTP 7-14 states the following software life cycle process planning documentation is reviewed.

- Software Management Plan (SMP)
- Software Development Plan (SDP)
- Software Quality Assurance Plan (SQAP)
- Software Integration Plan (SIntP)
- Software Installation Plan (SInstP)
- Software Maintenance Plan (SMaintP)

- Software Training Plan (STrngP)
- Software Operations Plan (SOP)
- Software Safety Plan (SSP)
- Software Verification and Validation Plan (SVVP)
- Software Configuration Management Plan (SCMP)
- Software Test Plan (STP)

Toshiba FPGA-based system uses a 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. Thus, the Software Installation Plan (SInstP) is not applicable to the FPGA-based system. The FPGA-based system will be installed and tested as hardware system at customer site in accordance with a system installation procedure that will be prepared for plant specific application.

In the Operations and Maintenance Phase, Toshiba will support maintenance activities. Software maintenance activities by Toshiba are described in Section I-3.7. Software operation is responsibility of the customer. Toshiba will support operation activities by providing system operations and maintenance manuals if required by the customer. Toshiba will not prepare a separate Software Operation Plan (SOP) unless the customer requests it.

Considering the characteristics specific to FPGA-based system lifecycle, Toshiba established a software lifecycle process appropriate to FPGA-based system. In this section, the following subsections are organized to explain the Toshiba software and hardware development process for FPGA-based systems.

- Section I-3.1: Generic Process
- Section I-3.2: Software Management Plan
- Section I-3.3: Software Development Plan
- Section I-3.4: Software Quality Assurance Plan
- Section I-3.5: Software Integration Plan
- Section I-3.6: Software Integration Report
- Section I-3.7: Software Maintenance Plan
- Section I-3.8: Software Training Plan

- Section I-3.9: Software Safety Analysis
- Section I-3.10: Software V&V Plan
- Section I-3.11: Software V&V Report
- Section I-3.12: Software Configuration Management Plan
- Section I-3.13: Software Test Plan
- Section I-3.14: Secure Development and Operational Environment
- Section I-3.15: Software/Hardware Development Process Applied to PRM

I-3.2 Software Management Plan

NED and NICSD prepare an NED Software Management Plan (SMP) (Reference (c2)) and NICSD SMP (Reference (c3)) respectively to describe the project management methods and approach used to control schedule, budget, resources, and processes associated with the development, review, test, and software quality assurance of software products to ensure that the work products meet the specified requirements and are appropriate for use in nuclear power plants. The NED SMP and NICSD SMP will be retained from project to project. If project specific requirements are applied, a supplemental Software Management Plan may be generated separately as necessary. The generic Software Management Plan to be applied to NED activities is provided in the NED SMP and summarized below. The Software Management Plan to be applied to NICSD activities is provided in the NICSD SMP and summarized below.

I-3.2.1 Organizations

Section I-1.4 and Figure I-1-2 describe the organizations responsible for development of the FPGA-based systems software design in the Current Process.

I-3.2.2 Responsibilities of NED Project Manager and Leads

This section describes the responsibilities and authorities of the NED Project Manager (PM) and each lead performing safety-related activities in NED.

I-3.2.2.1 NED Project Manager

The NED Project Manager (PM) is responsible for the managerial process and technical direction of the software development activities. The NED PM has the responsibility of interfacing with customer and the authority to approve all commitments on a specific project with permission of the executive level. The NED PM controls the official external project communications specifically including those affecting customer commitments and communication with regulatory agencies, contractual and technical requirements, cost, schedule, and project risks. The Senior Manager (SM) of ICDD assigns an NED PM, to whom the SM delegates the SM's responsibilities and authority for the project.

The NED PM assigns the Independent Verification and Validation (IV&V) Team Lead and other V&V personnel in the ICDD IV&V Team and ensures independence of the ICDD IV&V Team from the design groups. The NED PM assigns the ICDD System Safety Lead to ensure independence of the ICDD System Safety Lead. The NED PM ensures financial independence of ICDD V&V activities and safety activities from design activities.

I-3.2.2.2 ICDD System Safety Lead

The ICDD System Safety Lead is responsible for safety analysis of system safety aspect, personnel training for safety analysis staff, and planning of safety analysis. The term "system safety" is used only when referring to NED safety analysis activities. The term "software safety" is used only when referring to NICSD safety analysis activities. The ICDD System Safety Lead assigns individuals responsible for specific system safety activities, as necessary. The ICDD System Safety Lead and assigned individuals who perform system safety activities are independent of the design groups and ICDD IV&V Team.

I-3.2.2.3 Group Manager

Each Group Manager (GPM) of the control system engineering group and monitoring system engineering group is responsible for system development, and personnel training except training for safety analysis.

I-3.2.2.4 IV&V Lead

The ICDD IV&V Lead of the ICDD IV&V Team is IV&V Lead responsible for the V&V activities of NED and NICSD. The ICDD IV&V Team performs the ICDD V&V activities technically, managerially, and financially independent of the system development. The ICDD IV&V Team oversees the system safety activities ensuring independence of the activities, and performs baseline reviews.

I-3.2.3 Responsibilities NICSD Project Manager and Leads

This section describes the responsibilities and authorities of the NICSD Project Manager (PM) and each lead performing safety-related activities in NICSD.

I-3.2.3.1 NICSD Project Manager (NICSD PM)

The NICSD PM is 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 an NICSD PM, to whom the SM delegates the SM's responsibilities and authority for a specific project. Through the life cycle, the NICSD PM is responsible for management of the schedule, budget, and resources. The PM assigns the NICSD IV&V Lead and ensures independence of resources and budget between the NICSD IV&V Team and NICSD Software Development Team (NICSD SD Team). The NICSD PM also assigns an NICSD Software Safety Lead (NICSD SSL) independent of the NICSD SD Team and NICSD IV&V Team. The NICSD PM is responsible for ensuring independence of the design, V&V, software quality assurance, and software safety analysis functions. The NICSD PM ensures 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.

I-3.2.3.2 NICSD Software Development Lead (NICSD SDL)

The NICSD SDL is 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 builds an NICSD Software Development Team (NICSD SD Team).

I-3.2.3.3 NICSD Software Configuration Lead (NICSD SCL)

The NICSD SDL assigns an NICSD Software Configuration Lead (NICSD SCL) who is responsible for configuration management of software and hardware. The NICSD SCL is responsible for preparing an NICSD Software Configuration Management Plan (NICSD SCMP).

I-3.2.3.4 NICSD IV&V Lead

The NICSD IV&V Lead is responsible for the NICSD V&V activities, and assigns other V&V personnel. The NICSD IV&V Team performs the NICSD V&V activities technically, managerially, and financially independent of the software development. The NICSD IV&V

Team reviews the software safety analysis reports, and performs baseline reviews. The NICSD IV&V Lead has overall responsibility for software testing. The NICSD IV&V Lead builds an NICSD IV&V Team containing test engineers.

I-3.2.3.5 NICSD Software Safety Lead (NICSD SSL)

The NICSD SSL is responsible for carrying out safety analysis of software safety aspect. The NICSD SSL builds an NICSD Software Safety Team. The NICSD Software Safety Lead and the NICSD Software Safety Team member are independent of the NICSD SD Team and NICSD IV&V Team.

I-3.2.3.6 NICSD Software QA Lead (NICSD SQAL)

The manager of NICS-QA performs the NICSD SQAL role. The NICSD SQAL provides oversight of the NICSD SD Team, the NICSD IV&V Team and the NICSD Software Safety Team from QA perspective. The NICSD SQAL builds an NICSD Software QA team (NICSD SQA Team).

The manager of NICS-QA is provided with a direct line of communication to senior management on all quality-related matters through the NED Quality Assurance Department as described in the Power Systems Company Nuclear Energy (PSNE) QA Program Description (QAPD) (Reference (b1)).

The manager of NICS-QA is responsible for all internal audit activities within NICSD.

I-3.2.4 Management Objectives and Priority

The NED PM ensures that all planning documents are prepared on schedule, in accordance with the PSNE QAPD (Reference (b1)), and that they meet the project requirements.

The NED PM requires the SMs, GPMs, and other leads involved in the project to guide and supervise the personnel involved in the project to work in compliance with the Toshiba internal rules and the project standards for their occupational safety and product quality, and to work with integrity.

The NICSD PM requires the NICSD SDL, other leads, and managers in NICSD involved in the project to guide and supervise their subordinates involved in the project to work in compliance with the Toshiba internal rules and the project standards for their occupational safety and product quality, and to work with integrity.

I-3.2.5 Risk Management

The NED PM is responsible for risk management of the entire project including schedule, budget, resources, and technical issues, and must take appropriate actions to minimize project risks. The NED PM uses design review meetings and periodic ICDD-NICSD Project Meetings to identify risks. The design review meetings are used to evaluate the design, development and modification to meet the requirements, or to evaluate the status of readiness in fabrication, testing, or sub-contractor's process. Note that the design review meeting does not mean "Design Reviews" that are specified as one of design verification method and required to perform independently. When the NED PM identifies any risks that may have considerable impacts on the project, the NED PM reports the risks to the customer in a timely manner.

The NICSD PM is responsible for project risk management including schedule, budget, and resources, and must take appropriate actions to minimize the risks associated with the NICSD activities. The NICSD SDL, other leads, and managers in NICSD reports to the NICSD PM any concerns related to project risk as a part of periodic NICSD Management Meetings. At the periodic ICDD-NICSD Project Meetings, the NICSD SDL reports the concerns related to project risk identified at the periodic NICSD Management Meetings to ensure that the NED PM is informed.

I-3.2.6 Monitoring and Controlling Mechanisms

Project management is performed throughout the software life cycle. In addition to the schedule, budget, and resource metrics, the NED PM and NICSD PM ensure that appropriate metrics are generated and used for appropriate process correction and control.

The project phases and control mechanisms are as follows:

I-3.2.6.1 Initiation

A project begins with either the award of a contract or initiation of Toshiba internal development. NED is responsible for producing the preliminary schedule considering resource availability according to the approved schedule and budget. A Sub-master Engineering Schedule (SES) is developed to setup the milestones of the project. The SES is shared among ICDD and NICSD. The NICSD PM produces the NICSD Engineering Schedules (NICSD ESs), which consider resource availability and allocates these resources according to the approved schedule and budget with support from the NICSD SDL and other leads.

I-3.2.6.2 Planning and Scheduling

The NED PM is responsible for defining, planning, scheduling, costing, and resourcing the project with the assistance and data provided by the appropriate management and technical staff. Work packages from NED include plant system design documents and job orders to NICSD. A Project Control Document List (PCDL) is prepared to list project documents for the project. The PCDL lists project control documents which are controlled by NED including plans, procedures, procurement documents, technical specifications, and quality specifications specific to the project. NQAD conducts reviews of the procurement documents. NED Engineering Information Systems Department is responsible for retaining QA records.

The NICSD PM is 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 an NICSD Project Control Document List (NICSD PCDL). The NICSD PCDL list project control documents which are controlled by NICSD including plans, procedures, design documents, drawings, procurement documents, and test documents specific to the project. The NICSD PM ensures that all software tools used are listed, including the software version as needed, and accepted for their intended use. NICSD procures the modules from the module supplier under NICSD CGD process. NICSD has the responsibility to ensure that the CGD activities in NICSD are conducted correctly. NICSD has the responsibility to ensure that activities in both the module supplier and the printed circuit board fabricator are conducted correctly. NICS-QA will conduct an internal audit of NICSD and a CGD survey of the module supplier.

I-3.2.6.3 Execution

Development processes by NED are performed in accordance with the NED SMP (Reference(c2)). The NED PM convenes design review meetings. The NED PM convenes periodic ICDD-NICSD Project Meetings to check and monitor the project progress and to track issues identified.

Development processes by NICSD are performed in accordance with the NICSD SMP (Reference (c3)). The NICSD PM convenes periodic NICSD Management Meetings. The NICSD SDL reports the status of the project to the NICSD PM at the periodic NICSD

Management Meetings. The NICSD SDL, responsible leads and engineers attend and report the project status including the progress in the module supplier at the periodic ICDD-NICSD Project Meetings. NICSD confirms the status of the module supplier activities, and verifies that the module supplier follows their FPGA life cycle development process correctly.

I-3.2.6.4 Closeout

The NED PM ensures that all process requirements are complete, that the system has been evaluated and accepted by the customer, that deliveries and signoffs are complete, and that final disposition of documentation is performed according to the NED SMP (Reference (c2))
The NICSD PM ensures 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 documentation is performed according to the NICSD SMP (Reference (c3)).

I-3.3 Software Development Plan

This section explains the development process for an FPGA-based system intended for use in safety-related applications for US nuclear power plants.

ICDD prepares the NED SMP (Reference (c2)) to describe the generic life cycle process implemented by NED when establishing the system conceptual requirements and design inputs to NICSD during the Project Planning and Concept Definition Phase. NICSD prepares a Software Development Plan (SDP) describing generic life cycle process by NICSD. The SDP is included as one section in the NICSD SMP (Reference (c3)). The NED SMP and NICSD SMP will be retained from project to project. If project specific requirements are applied, a supplemental Software Management Plan may be generated separately as necessary.

The following sections describe the SDP for development of the FPGA-based safety-related systems stating which tasks are a part of each life cycle, and stating the life cycle inputs and outputs.

I-3.3.1 Project Planning and Concept Definition Phase

I-3.3.1.1 Project Planning and Concept Definition Phase Inputs for NED

Plant specific documents, regulations, and applicable industry codes and standards are inputs to the Project Planning and Concept Definition Phase. ICDD defines design inputs and documented in a Design Input Sheet (DIS). The DIS identifies the applicable design inputs, including design bases such as specified in license application, performance requirements, regulatory requirement, codes and standards.

I-3.3.1.2 NED Planning Document

ICDD prepares the NED SMP (Reference (c2)) to describe generic life cycle process by NED including establishment of system conceptual requirements and design inputs to NICSD during the Project Planning and Concept Definition Phase. ICDD uses the standard nuclear QA program PSNE QAPD (Reference (b1)) for software quality assurance and configuration management activities. The ICDD IV&V Team prepares the NED Verification and Validation Plan (NED VVP) (Reference (c6)). The NED VVP defines the generic software V&V process performed by NED and documents required throughout the V&V process. The NED SMP and NED VVP will be retained from project to project. If project specific requirements are applied, supplemental planning documents may be generated separately as necessary.

I-3.3.1.3 NED Design Documentation

ICDD prepares a separate System Design Description (SDD) for each FPGA-based system. The SDD describes functions, comprehensive system design description, operation, system interfaces, field inputs and outputs, specific requirements for components, and system and equipment design data of each system.

In addition to the SDD, ICDD prepares Interlock Block Diagrams (IBDs) and Instrumentation Electrical Diagrams (IEDs). The IBDs describe operation interlocks and protective functional information. ICDD prepares the IED to depict the I&C system configuration and functions. The SDDs, IBDs, and IEDs include system level requirements.

I-3.3.1.4 Job Order to NICSD

ICDD issues a Job Order Sheet to procure FPGA-based systems from NICSD. NED uses the Job Order Sheet for subcontracting design, manufacturing of items and services. The Job Order Sheet identifies requirements for subcontracting design, manufacturing of items and services including scope of work, technical requirements, QA requirements, and documentation requirements as applicable.

I-3.3.1.5 Project Planning and Concept Definition Phase Inputs to NICSD

Regulations and regulatory guides specified in the NED documents attached to the NED Job Order Sheet are inputs to the Project Planning and Concept Definition Phase.

The SDD, IEDs, IBDs, NED SMP, NED VVP, procurement specification, and other technical and quality assurance requirement documents attached to the NED Job Order Sheet are design inputs to NICSD for the Project Planning and Concept Definition Phase.

The NICSD SD Team prepares a Design Input Sheet (DIS) to identify the design inputs for the project.

I-3.3.1.6 NICSD Planning Documents

The NICSD SD Team prepares an NICSD SMP (Reference (c3)) which contains a Software Management Plan, Software Development Plan, Software Safety Plan, and Software Training Plan. The NICSD SD Team prepares an NICSD Software Configuration Management Plan (NICSD SCMP) (Reference (c8)). The NICSD SQA Team prepares an NICSD Software Quality Assurance Plan (NICSD SQAP) (Reference (c7)). The NICSD IV&V Team prepares an NICSD V&V Plan (NICSD VVP) (Reference (c9)). The NICSD SMP, SCMP, SQAP, and VVP will be retained from project to project. If project specific requirements are applied, supplemental planning documents may be generated separately as necessary.

The NICSD SD Team prepares 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 IV&V Team prepares a Software Test Plan.

I-3.3.1.7 Equipment Design Specification (EDS)

Based on the SDD, IBDs, and IEDs, the NICSD SD Team prepares an EDS that breaks down the system level requirements into the equipment design requirements, and defines the specification of the FPGA-based system. The EDS defines functional requirements, hardware and software design requirements for lower level design, and environmental condition including equipment qualification and EMC qualification. The EDS also defines data communication protocol and architecture for the external system communication.

I-3.3.1.8 CGD Planning

I-3.3.1.8.1 Identification of Previously Developed Software (PDS) and Commercial-off-the-Shelf (COTS)

NICSD purchases the modules comprising the FPGA-based equipment from the module supplier. The FPGA logics embedded in an FPGA on the module printed circuit board are designed and tested by the module supplier 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. NICSD does not modify or customize the FPGA logics procured from the module supplier. The evaluation process for the FPGA logic under NICSD CGD process is described in Section I-3.3.2.5.

The FPGA logic is comprised of combinations and connections of software elements called functional elements (FEs). The module supplier, 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 the module supplier. The evaluation process for the FEs under the NICSD CGD process is described in Section I-3.3.2.5. The NICSD CGD process has been completed and documented. Modifications to the FEs are not planned for a specific project purpose. In the case that the design changes are required to an FPGA-based safety-related system, NICSD evaluates the contents of each design change to determine whether new development of FEs is necessary. Result of design change evaluation is documented in a Design Change Technical Report (DCTR). If new FE development is necessary as the result of design change evaluation, NICSD instructs the module supplier to develop new FEs, and then evaluates and dedicates the new FEs. The supplemental evaluation is performed for the new FEs in a manner described in Section I-3.3.2.5. The evaluations required in Section I-3.3.2.5 are also applied to the existing FEs.

I-3.3.1.8.2 CGD Plan

The NICSD SD Team prepares the Commercial Grade Dedication (CGD) Plan (Reference (c4)) for FPGA-based systems to describe the generic plan for dedicating the commercial grade items comprising the equipment for FPGA-based systems. The CGD Plan will be retained from project to project. If project specific requirements are applied, supplemental dedication plan may be generated separately as necessary. The CGD Plan documents methods for safety classification of the system and for determining whether the commercial grade dedication is applicable, and describes the activities required for the dedication of the commercial grade items and services.

I-3.3.1.8.3 Preliminary Technical Evaluation Report (PTER)

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

I-3.3.1.8.4 Procurement Planning Sheet (PPS)

The NICSD SD Team prepares a Procurement Planning Sheet (PPS) to schedule the procurement and vendor evaluation activities, so that the procurements activities are carried out in planned, documented and systematic manner.

I-3.3.1.9 Software Safety Analysis

Safety analysis activity is performed for every phase by ICDD and NICSD. In this phase, the ICDD System Safety Lead performs a safety analysis on the ICDD design and documents the result in the preliminary NED Software Safety Analysis Report (NED SSAR). The NICSD Software Safety Team performs a safety analysis on the equipment design documents and prepares an NICSD Software Safety Analysis Report (NICSD SSAR) for each FPGA-based system. The detailed analysis methodology is explained in Section I-3.9.

I-3.3.1.10Requirements Traceability Matrix

ICDD performs requirements management activities by preparing the Project Planning and Concept Design Phase Requirements Traceability Matrix (RTM). The RTM in this phase includes the base requirements that are collected from the SDDs, IBDs and IEDs. The base requirements include safety critical requirements. ICDD ensures that the base requirements cover all regulatory and application specific requirements. 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 reviews the RTM.

I-3.3.1.11Configuration Management

NED generates a PCDL to list project documents controlled by NED, and updates the PCDL in each software lifecycle phase as necessary.

The NICSD SD Team generates an NICSD Master Configuration List (NICSD MCL) for each FPGA-based system and conducts a configuration management assessment to ensure the following activities occur, as planned in the NICSD SCMP (Reference (c8)).

- All phase activities are completed with 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.

After the configuration management assessment, the NICSD IV&V Team performs a baseline review as described in Section I-3.3.1.13. The detailed software configuration management activities are explained in Section I-3.12.

I-3.3.1.12Verification and Validation

The NICSD IV&V Team produces an NICSD Verification and Validation Report (VVR) documenting the V&V activities performed by NICSD in this phase. The NICSD VVR is updated at the end of each life cycle phase. In this phase, the ICDD IV&V Team produces the NED VVR documenting the V&V activities performed by ICDD, evaluation of the NICSD VVR and summary of V&V activities of this phase. The NED VVR is updated at the end of each life cycle phase.

I-3.3.1.13Baseline Review

The ICDD IV&V Team performs baseline reviews at the end of the Project Planning and Concept Definition Phase and the System Validation Testing Phase for which ICDD is responsible, as required in the NED VVP. The System Validation Testing Phase baseline review is the final baseline review and confirms the completion of the system development before shipment to customer. The ICDD IV&V Team issues a Baseline Review Report (BRR) after each review.

The NICSD IV&V Team performs a baseline review at the end of each phase and completes the phase activities as required in the NICSD VVP. The NICSD IV&V Team issues a BRR after each review.

Each of the baseline reviews confirms disposition of each design, documentation, and test nonconformance identified during the phase. Software safety work products are included in the baseline review.

I-3.3.2 Requirements Definition Phase

I-3.3.2.1 Unit Detailed Design Specification (Unit DDS)

A Unit DDS is provided for each specific unit which comprises the FPGA-based system. The Unit DDSs satisfy the requirements for Software Requirements Specification (SRS) in a traditional CPU based software life cycle. The Unit DDSs also include the hardware requirements specification for the module. This specification includes definition of communication links and interfaces with other units and external systems, providing the external communication link and interfaces documentation. The NICSD SD Team prepares the Unit DDS. Based on the design requirements specified in the EDS, the Unit DDS defines unit design specifications and provides hardware and software design requirements for module level design.

I-3.3.2.2 Equipment Schematic

The NICSD SD Team designs hardware connections in the system based on the IBDs, IEDs, EDS, and Unit DDSs. If a safety related cabinet is designed for FPGA-based system, the NICSD SD Team prepares an Elementary Control Wiring Diagram (ECWD) to define detailed electrical and hardware connections between units and electrical components placed in the safety related cabinet for the FPGA-based system.

I-3.3.2.3 Equipment User's Manual

The NICSD SD Team prepares a user's manual for each unit comprising the FPGA-based system with reference to the module supplier design.

I-3.3.2.4 Commercial Dedication Instruction

The NICSD SD Team prepares a Commercial Dedication Instruction (CDI) for each module type comprising the unit. This document identifies the specific critical characteristics for each module type and includes a technical evaluation, acceptance plan with acceptance criteria, and methods for acceptance. The acceptance methods identified in the CDI are reflected in the procurement document or the receiving inspection procedure for the item and service.

The NICSD SD Team also prepares separate CDIs for unit chasses, cables and other components comprising FPGA-based system.

I-3.3.2.5 Vendor Evaluation

I-3.3.2.5.1 Vendor Evaluation for Module Supplier

The NICSD SD Team conducts a vendor evaluation with support from the NICSD IV&V Team, the NICSD SQA Team, the NICSD Software Safety Team, and NICS-QA. The evaluation is conducted before issuing a Job Order to the module supplier.

The module supplier has development procedures for FPGA-based products. The module supplier procedures are evaluated by NICSD through the technical evaluation. Applicable revisions of the module supplier procedures, which are verified through the technical evaluation, are specified in the procurement document to the module supplier.

The following are evaluated at a minimum.

- The module supplier's control over the critical characteristics identified in the PTER or CDIs
- Software development tools as described in Section I-3.3.10
- The module supplier procedures
- The module supplier's control over the personnel qualification for FPGA development and testing

I-3.3.2.5.2 Evaluation of FPGA Logic

The following tasks are performed before issuing a Job Order to the module supplier.

- 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 the documentation required for the application.

The NICSD SD Team documents the results of the evaluation in the PTER. If the evaluation acceptance criteria are not met, the FPGA logic should be re-engineered and re-evaluated. The NICSD SD Team updates the PTER as necessary, and finalizes the PTER as the Final Technical Evaluation Report (FTER) to reflect the completion of the FPGA logic development and the results of any additional evaluations that were required. NICSD also performs an independent review and safety analysis for the module supplier documents.

I-3.3.2.5.3 Evaluation of FEs

Each FE is evaluated to ensure it meets the required quality level prior to incorporation into the design. The NICSD VVP identifies 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 performs the evaluation of FEs as a part of their technical evaluation activity. If supplemental requirements for FEs are necessary, the NICSD SD Team adds supplemental requirements to the procurement documents to the module supplier.

The evaluation process includes the following activities:

- Review of development process and its documentation
- Review of the FEs (e.g., design and test documents including full pattern test results)
- Review of the supplier software quality assurance program
- Review of the supplier configuration control
- 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 NICSD SD Team documents the result of the evaluation in the PTER. If the evaluation acceptance criteria are not met, the FEs should be re-engineered and re-evaluated. The NICSD SD Team updates the PTER as necessary, and finalizes the PTER as the Final Technical Evaluation Report (FTER) to reflect the completion of this group of FEs and the results of any additional evaluations that were required.

I-3.3.2.5.4 Software Coding Conventions and Guidelines Document Review

The programmable logic coding conventions and guidelines document establishes the VHDL coding practices to be followed in the FPGA logic design. The programmable logic coding conventions and guidelines document is equivalent to the software coding conventions and guidelines document in a normal software lifecycle. The guideline document provides coding practices that will result in readable, consistent, correct, maintainable, reliable, and efficient VHDL source code. The NICSD SD Team performs a review of the programmable logic coding conventions and guidelines document provided by the module supplier as a part of their technical evaluation activity. The NICSD SD Team documents the results of the review in the PTER. If supplemental requirements for the programmable logic coding conventions and guidelines document are necessary, the NICSD SD Team adds the supplemental requirements to procurement document to the module supplier.

I-3.3.2.5.5 Vendor Evaluation for Commercial Supplier (other than Module Supplier)

The NICSD SD Team conducts a vendor evaluation with support from the NICSD IV&V Team, SQA Team, Software Safety Team, and NICS-QA. A CG Survey is conducted to evaluate supplier control over the critical characteristics if required by the CDI.

I-3.3.2.6 Procurement Documentation

The NICSD SD Team prepares a procurement document for each module type comprising the unit and for unit chasses, cables and other components comprising the FPGA-based system. The procurement documents include technical requirements and QA requirements. The technical requirements are the applicable design requirements for the commercial grade items derived from the Unit DDS. The QA requirements identify applicable quality assurance requirements for the commercial grade items and services. The procurement document also identifies the procedures to be followed by the module supplier for building software.

I-3.3.2.7 Software Safety Analysis

The NICSD Software Safety Team performs a safety analysis on the unit design documents and prepares an NICSD Software Safety Analysis Report (SSAR) for each FPGA-based system. The ICDD System Safety Lead evaluates the NICSD SSAR and prepares an NED SSAR.

I-3.3.2.8 Requirements Traceability Matrix

At the end of this phase, the NICSD SD Team updates the RTM to maintain forward and backward traceability between the EDS and the Unit DDS. The NICSD IV&V Team performs an independent review of the RTM.

I-3.3.2.9 Configuration Management

The NICSD SD Team updates the NICSD MCL and conducts a configuration management assessment as described in Section I-3.3.1.11.

I-3.3.2.10 Verification and Validation

The NICSD IV&V Team updates the NICSD Verification and Validation Report (VVR) to report the completion of NICSD V&V activities for this phase. The ICDD IV&V Team updates the NED VVR documenting the V&V activities performed by ICDD, evaluation of the NICSD VVR and summary of V&V activities of this phase.

I-3.3.2.11 Baseline Review

The NICSD IV&V Team performs a baseline review and issues a BRR as described in Section I-3.3.1.13.

I-3.3.3 Design Phase

I-3.3.3.1 Job Order to Module Supplier

The NICSD SD Team issues a job order using the Engineering Communication Sheet (ECS) form to procure the modules from the module supplier. In the job order, the NICSD SD Team specifies applicable procurement documents which include module design requirements, required delivery date, and versions of the software tools that can be used for FPGA products. The job order also includes requirements for the module supplier submittal documentation. The NICSD SD Team approves the design and test documents submitted by the module supplier. The job order is completed after the NICSD SD Team verifies technical and quality adequacy of the submitted documents.

I-3.3.3.2 Module Design Specification (MDS)

The combination of a Module Design Specification (MDS) and FPGA Design Specifications fulfills the requirement for a software design description and a hardware/software architecture description.

The MDS consists of a combination of the hardware and software detailed design descriptions necessary to define the modules. This specification includes identification of communication links and interfaces both internal and external.

The MDS satisfies the requirements identified in the Unit DDS and provides sufficient detail to allow someone other than the author of the MDS to create, review, and test the module function. The MDS translates the software requirements into a description of the programmable logic structure, programmable logic components, interfaces, and data necessary for implementation.

The module supplier submits the MDS to NICSD for review and approval. The NICSD IV&V Team performs an independent review of the MDS. The NICSD SD Team approves the MDS if the verification results are acceptable.

NICSD confirms that the module supplier followed the FPGA life cycle development process correctly and confirms the status of the module supplier activities.

I-3.3.3.3 FPGA Design Specification

The combination of a Module Design Specification (MDS) and FPGA Design Specifications fulfill the requirement for a software design description and a hardware/software architecture description.

The FPGA Design Specification consists of a combination of the hardware and software detailed design description necessary to define the FPGAs. This specification includes communication links and interfaces with other FPGAs on the module. It also provides the internal communication link and interfaces documentation.

The FPGA Design Specification satisfies the requirements identified in the MDS, and provides sufficient detail to allow someone other than the author of the FPGA Design Specification to create, review, and test the FPGA functions. The FPGA Design Specification translates the software requirements into a description of the software structure, software components, interfaces, and data necessary for implementation.

The module supplier submits an FPGA Design Specification to NICSD for review and approval after NICSD approval of the MDS. The NICSD IV&V Team performs an independent review of the FPGA Design Specification. The NICSD SD Team approves the FPGA Design Specification if the verification results are acceptable.

NICSD confirms that the module supplier followed the FPGA life cycle development process correctly and confirms the status of the module supplier activities.

The NICSD SD Team performs a software coding readiness review. This review ensures:

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

I-3.3.3.4 Initiation of Software Validation Test Plan (SVTP) Development

The NICSD IV&V Team initiates the development of the SVTP for System Validation Testing including test case specification, and development of the testing procedure.

The SVTP outlines the methodology of how various tests will be used to verify that the integrated programmable logic meets the requirements stated in the EDS and Unit DDS. The SVTP identifies environments, cases (including inputs, procedures, outputs, and expected results), resources (including tools, personnel, and equipment), methodologies, and acceptance criteria.

I-3.3.3.5 Software Safety Analysis

The NICSD Software Safety Team performs a safety analysis on the module and FPGA design documents and prepares an NICSD Software Safety Analysis Report (SSAR) for each FPGA-based system. The ICDD System Safety Lead evaluates the NICSD SSAR and prepares an NED SSAR.

I-3.3.3.6 Requirements Traceability Matrix

During this phase, the module supplier prepares and submits RTMs to NICSD for each module showing forward and backward traceability between the unit design and the module design, and between the module design and the FPGA design. The NICSD IV&V Team performs an independent review of the RTMs.

I-3.3.3.7 Configuration Management

The NICSD SD Team updates the NICSD MCL and conducts a configuration management assessment as described in Section I-3.3.1.11.

I-3.3.3.8 Verification and Validation

The NICSD IV&V Team updates the NICSD Verification and Validation Report (VVR) to report the completion of NICSD V&V activities for this phase. The ICDD IV&V Team updates the NED VVR documenting the V&V activities performed by ICDD, evaluation of the NICSD VVR, and summary of V&V activities of this phase.

I-3.3.3.9 Baseline Review

The NICSD IV&V Team performs a baseline review and issues a BRR as described in Section I-3.3.1.13.

I-3.3.4 Implementation and Integration Phase

Unlike a microprocessor-based system, the FPGA that Toshiba selected requires software installation to be performed before hardware assembly. There are no provisions for conditional software releases since they are not applicable to the NRW-FPGA-based technology.

I-3.3.4.1 Software Coding and Coding Review (VHDL Source Code)

The module supplier writes VHDL source code to implement the FPGA design, which includes safety critical functions, consistent with the coding guidelines. The NICSD IV&V Team performs a VHDL source code review and issues a source code review sheet.

I-3.3.4.2 FPGA Testing

FPGA Testing is performed taking two separate approaches. The first approach uses a VHDL simulator, and the second approach uses a programmed FPGA. The FPGAs used for FPGA Testing are prepared in the same manner as those FPGAs to be mounted onto production module printed circuit boards.

FPGA Testing is considered as the software functional testing in the traditional CPU based software life cycles. The FPGA Testing is performed to ensure that the FPGA logic satisfies the requirements provided in the design documents, to identify and correct code design errors prior to system integration, and to verify that the FPGA logic interfaces properly. The NICSD IV&V Team performs an independent review of an FPGA Test Procedure. The NICSD SD Team approves the FPGA Test Procedure if the verification results are acceptable.

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

NICSD confirms that the module supplier followed the FPGA life cycle development process correctly and confirms the status of the module supplier activities.

The module supplier performs the FPGA Testing in accordance with the test procedures approved by NICSD under oversight by NICSD IV&V Team.

A summary of test activities, including a basis for determining the rigor of testing and the test results, is prepared and documented in an FPGA Test Report. The NICSD IV&V Team performs an independent review of FPGA Test Report, and the NICSD SD Team approves the FPGA Test Report.

NICSD confirms that the module supplier followed the FPGA life cycle development process correctly and confirms the status of the module supplier activities.

I-3.3.4.3 FPGA Implementation

After the FPGA Test Report is reviewed and approved by NICSD, the module supplier submits electronic media and a Module MCL which includes the FPGA control sheet, VHDL source code, FPGA logic (fuse map) and related configuration items for review by NICSD. The FPGA control sheet identifies the configuration items including the FPGA Design Specification, FPGA Test Procedure, FPGA Test Report, VHDL source code, fuse map, and software development tool version.

NICSD establishes a baseline of the FPGA logic to control configuration items as follows.

The NICSD SD Team receives the electronic media and Module MCL. The NICSD SD Team prepares a master media and copy media, and prepares configuration records such as a list of fuse-map registration numbers. NICS-QC reviews the media and configuration records as a configuration status accounting for the baseline of FPGA logic. After successful completion of review, the NICSD SD Team stores approved master media, copy media and configuration records in their locked configuration control.

The NICSD SD Team sends an FPGA Logic Implementation Request/Record Sheet and approved FPGA logic (fuse map) to the printed circuit board fabricator via the module supplier to implement the FPGA logic into the FPGA chip. The fuse map file in the copy media controlled by NICSD is used by the printed circuit board fabricator to implement the FPGA logic into the FPGA chip.

The NICSD QC inspector witnesses the FPGA logic implementation into the FPGA, and the NICSD QC inspector checks whether the FPGA logic implementation has been carried out correctly by verifying the checksum indicated on the programming tool. This oversight is a key part of commercial grade dedication of the modules from a configuration management point of view.

The FPGAs which pass the inspection are mounted on the printed circuit board and assembled as a module by the printed circuit board fabricator. The printed circuit board fabricator delivers the module to the module supplier.

I-3.3.4.4 Software Safety Analysis

The NICSD Software Safety Team performs a safety analysis on the coding and FPGA test activities and prepares an NICSD Software Safety Analysis Report (SSAR) for each FPGA-based system. The ICDD System Safety Lead evaluates the NICSD SSAR and prepares an NED SSAR.

I-3.3.4.5 Requirements Traceability Matrix

During this phase, the module supplier prepares and submits RTMs to NICSD for each FPGA type showing forward and backward traceability between the FPGA Design Specification and the FPGA Test Procedure. The NICSD IV&V Team performs an independent review of the RTMs.

I-3.3.4.6 Configuration Management

The NICSD SD Team updates the NICSD MCL and conducts a configuration management assessment as described in Section I-3.3.1.11. After the configuration management assessment, the NICSD IV&V Team performs a baseline review.

I-3.3.4.7 Verification and Validation

The NICSD IV&V Team updates the NICSD Verification and Validation Report (VVR) to report the completion of NICSD V&V activities for this phase. The ICDD IV&V Team updates the NED VVR documenting the V&V activities performed by ICDD, evaluation of the NICSD VVR, and summary of V&V activities of this phase.

The NICSD VVR for this phase includes the list of the following documents that result from V&V activities of this phase. The listed documents satisfy the requirements for a software build procedure and report in a traditional CPU based software life cycle. The combination of the Source Code Review Sheet and FPGA Test Report satisfies the requirement for a software implementation review report in a traditional CPU based software life cycle.

- Source Code Review Sheet
- FPGA Test Report
- FPGA Control Sheet (including the names of the VHDL source code files)
- Procurement document (Output of Requirements Definition Phase)

The procurement document to the module supplier identifies the procedures to be followed by the module supplier for software building. The module supplier procedures ensure that only approved fuse map are embedded to FPGAs. NICSD oversight ensures that each FPGA label correctly identifies the logic embedded in each FPGA.

I-3.3.4.8 Baseline Review

The NICSD IV&V Team performs a baseline review and issues a BRR as described in Section I-3.3.1.13.

I-3.3.5 Module Validation Testing Phase

In the Module Validation Testing Phase, the module supplier performs Module Validation Testing using Module Test Procedures under oversight of NICSD.

I-3.3.5.1 Module Validation Testing

The module supplier submits a Module Test Procedure which includes test cases and test procedures for review and approval by NICSD. The NICSD IV&V Team performs an independent review of the Module Test Procedure. The NICSD SD Team approves the Module Test Procedure if the verification results are acceptable. NICSD verifies that the module supplier followed the FPGA life cycle development process correctly and confirms the status of the module supplier activities.

The module supplier performs module testing in accordance with the Module Test Procedure approved by NICSD. The module supplier documents the result of the Module Validation Testing in a Module Test Report. The NICSD IV&V Team performs an independent review of the Module Test Report. The NICSD SD Team approves the Module Test Report.

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

NICSD verifies that the module supplier followed the FPGA life cycle development process correctly and confirms the status of the module supplier activities.

I-3.3.5.2 Receiving of Modules

After Module Test Reports are approved by NICSD, the module supplier delivers the modules to NICSD. An NICSD receiving inspector performs receiving inspections.

I-3.3.5.3 System Operations and Maintenance Manual (System O&M Manual)

The NICSD SD Team prepares a System Operations and Maintenance (O&M) Manual for each FPGA-based system when required by the customer. The contents of the System O&M Manual will be based on the requirements documents provided by the customer.

In addition, the System O&M Manual may be used as a system training manual by the customer. The system training manual contents will be described in the requirements documents supplied by the customer.

I-3.3.5.4 Software Safety Analysis

The NICSD Software Safety Team performs a safety analysis on the module validation test activities and prepares an NICSD Software Safety Analysis Report (SSAR) for each FPGA-based system. The ICDD System Safety Lead evaluates the NICSD SSAR and prepares an NED SSAR.

I-3.3.5.5 Requirements Traceability Matrix

During this phase, the module supplier prepares and submits RTMs to NICSD for each module showing forward and backward traceability between the Module Design Specification and the Module Test Procedure. The NICSD IV&V Team performs an independent review of the RTMs.

I-3.3.5.6 Configuration Management

The module supplier updates and submits the Module MCL to include the identification of the Module Test Report to NICSD. The NICSD SD Team reviews and approves the Module MCL whether configuration items for each module are controlled by the module supplier appropriately. NICSD updates the NICSD MCL to reflect the Module MCL updates.

The NICSD SD Team conducts a configuration management assessment as described in Section I-3.3.1.11.

I-3.3.5.7 Verification and Validation

The NICSD IV&V Team updates the NICSD Verification and Validation Report (VVR) to report the completion of NICSD V&V activities for this phase. The ICDD IV&V Team updates the NED VVR documenting the V&V activities performed by ICDD, evaluation of the NICSD VVR, and summary of V&V activities of this phase.

I-3.3.5.8 Baseline Review

The NICSD IV&V Team performs a baseline review and issues a BRR as described in Section I-3.3.1.13.

I-3.3.6 System Validation Testing Phase

I-3.3.6.1 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 are documented in a Software Validation Test Report (SVTR). The NICSD IV&V Team prepares the SVTR. The testing is planned to demonstrate that all safety-related functions identified in the base requirements are operational.

The NICSD IV&V Team identifies any failures in System Validation Testing that may require changing 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 regression testing on the modified FPGA logic and all interfaces between unmodified and modified FPGA logic.

I-3.3.6.2 CGD Package

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

- CGD Report
  The NICSD SD Team prepares a CGD Report for each module type, unit chassis, cables, and other equipment. This report identifies the commercial grade items verified through the dedication, documents the results of acceptance activities with the list of documents used for dedication activity and acceptance records.
- Final Technical Evaluation Report (FTER)
  The NICSD SD Team prepares a Final Technical Evaluation Report (FTER) for each FPGA-based system. This report consolidates the results of CGD activities including vendor evaluation, FPGA logic and FE evaluation, and software tool evaluation results for each FPGA-based system.
- CGD Package
  The NICSD SD Team prepares a CGD Package. This package contains the list of documents used for dedication planning, FTER, CDIs, and CGD Reports.

I-3.3.6.3 Software Safety Analysis

Safety analysis activity is performed for every phase by ICDD and NICSD. In this phase, the NICSD Software Safety Team performs a safety analysis on the system validation test activities and prepares a final NICSD Software Safety Analysis Report (SSAR) for each FPGA-based system. The ICDD System Safety Lead evaluates the final NICSD SSAR, and prepares the final NED SSAR based on the evaluation of NICSD results and an evaluation of software safety at the plant system level. Any elements of the system that require rework from this evaluation will result in test procedure change or design change. Affected testing procedures; test cases; and system, modules, and FPGAs are controlled by formal change control process, and are evaluated by the NICSD Software Safety Team through appropriate portions of the safety analysis process.

I-3.3.6.4 Requirements Traceability Matrix

The traceability from the system requirements in EDS and Unit DDS is ensured by the RTM showing forward and backward traceability between the system requirements in EDS and Unit DDS and test documents used for the System Validation Testing including hardware test specifications and the Software Validation Test Plan for each project. The NICSD SD Team finalizes the RTM to maintain traceability from the Project Planning and Concept Definition Phase through the System Validation Testing Phase. The NICSD IV&V Team performs an independent review of the RTM.

I-3.3.6.5 Configuration Management

After successful completion of the System Validation Testing, NICSD updates the NICSD MCL to include the SVTR.

The NICSD SD Team conducts a configuration management assessment as described in Section I-3.3.1.11.

I-3.3.6.6 Verification and Validation

The NICSD IV&V Team finalizes the NICSD Verification and Validation Report (VVR) documenting the NICSD V&V activities performed from the Project Planning and Concept Definition Phase through the System Validation Testing Phase.

The ICDD IV&V Team finalizes the NED VVR documenting the ICDD V&V activities performed from the Project Planning and Concept Definition Phase through the System Validation Testing Phase, and evaluation of the NICSD VVR.

I-3.3.6.7 Final Inspection before Shipping

After System Validation Testing, NICSD QC inspectors perform a final inspection.

I-3.3.6.8 Baseline Review

The NICSD IV&V Team performs a baseline review and issues a BRR as described in Section I-3.3.1.13.

The ICDD IV&V Team performs the final Baseline Review to complete the software development including the V&V activities. The ICDD IV&V Team issues a BRR as described in Section I-3.3.1.13.

I-3.3.6.9 Production Release (Shipment)

Once a software build meets the requirements of the System Validation Testing, it is released as production software through the baseline review process. A Factory Acceptance Test (FAT) including hardware tests and electronic safety tests of equipment, which is not considered part of the FPGA lifecycle, is also performed combined with the System Validation Testing. A software quality assurance audit is performed on the software build as part of the baseline review for this phase.

I-3.3.7 Operations and Maintenance Phase

The Operations and Maintenance Phase begins with the completion of the System Validation Testing Phase. NED and NICSD address any problem that occurred after the System Validation Testing and perform any necessary activities, which may include updating the design documents, NICSD MCL, VHDL source codes, RTM, NICSD SSAR, NED SSAR, NICSD VVR and NED VVR. To perform these activities, NICSD implements the established software change control procedure in the NICSD SCMP.

I-3.3.8 Retirement Phase

In the Retirement phase, support for the FPGA-based system is terminated. At this phase, the customer may contact Toshiba for removal of the equipment. Toshiba will help with proper disposal of equipment and documentation supplied to plants.

I-3.3.9 Life Cycle Task Iteration Process

It should be noted that the use of the lifecycle model includes the nested pass, because development processes frequently need to be iterated. Figure I-3-2 shows the concept of a nested pass. In the figure, the left arrows indicate the primary pass corresponding to the progress of development process. If a non-conformance is found, e.g. at the Module Validation Testing Phase, the process pauses at the phase in which the non-conformance is found. The cause of non-conformance is identified, and then corrective actions are 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 are updated. After the nested pass returns to the paused phase, the development process restarts.

When an input document to NICSD is changed, each lead reviews the software plans, procedures, and instructions. The responsible lead evaluates the backfit to existing work products to determine the extent to which tasks need to be repeated.

The modifications made to any FPGA logic after the completion of System Validation Testing are analyzed for appropriate regression testing under the configuration management process described in the NICSD SCMP. The process used is the same that Toshiba uses to resolve anomalies during development, with the addition of the requirement to notify existing customers if errors are found that are in already shipped or accepted systems.

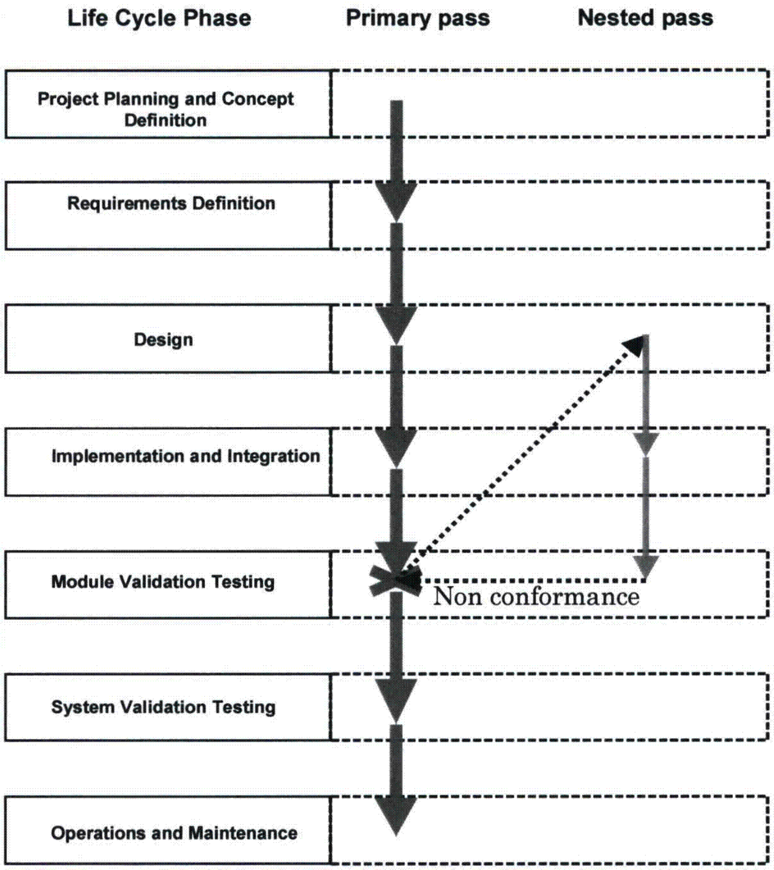

Life Cycle Phase
Primary pass
Nested pass
Project Planning and Concept Definition
Requirements Definition
Design
Implementation and Integration
Module Validation Testing
Non conformance
System Validation Testing
Operations and Maintenance

Figure I-3-2 Life Cycle Iteration Process

I-3.3.10 Software Development Tool Control

The software tools shown in Table I-3-3 are used for the software design, development, and implementation of FPGAs. These software tools are categorized as SIL2 software.

Table I-3-3 Software Development Tools

Tool Name	Application
Logic synthesis tool	The logic synthesis tool synthesizes logic from VHDL source codes and produces netlists. As by-products of logic synthesizing, the logic synthesis tool performs syntactic check of the VHDL source codes and adequacy check of the synthesized logic.
Netlist viewing tool	The netlist viewing tool depicts the logic block diagrams according to the netlists. The netlist viewing 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 viewing tool is integrated as a function in the integrated development environment, which is the FPGA development package Toshiba uses for NRW-FPGA development.
Place and route tool	The place and route tool converts one or more gate-level netlists into a fuse map file. To generate the fuse map file, the place and route 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 place and route tool also generates logic cell and route specific gate-level delay information that the FPGA simulation tool uses for simulation.
FPGA simulation tool	The FPGA simulation tool is used for simulation of an FPGA using the gate-level netlists and gate-level delay information generated by the place and route tool, for testing in FPGA simulation, for analysis of internal FPGA timing, for generation of test signals for the FPGA adaptor to test FPGAs, and for measurement of the toggle coverage rate for given test vectors.
FPGA programming tool	The FPGA programming tool embeds the fuse map generated by the place and route tool into the FPGA chips.

The module supplier uses the controlled software tools for software development. NICSD evaluates software tool control process implemented by the module supplier. The NICSD SD Team prepares a Preliminary Technical Evaluation Report (PTER) to report the results of the evaluation. The PTER includes the software tool report in a standard CPU based software life cycle.

When the module supplier requests to change the version of a software tool, the NICSD SDL requires the NICSD IV&V Team to review the software tool evaluation documentation provided by the module supplier. This evaluation includes checking that any errors identified by Microsemi SoC do not affect the existing FPGA designs, including those designs that have been provided to utilities as well as documenting the evaluation that no additional evaluations of Microsemi SoC need to be performed. If errors are identified that might have propagated into existing designs, appropriate corrective action will be designed and performed. The NICSD IV&V Team documents the review result in the NICSD Verification and Validation Report

(VVR). After the successful review by the NICSD IV&V Team, the NICSD SDL approves the use of the new version software tools. The NICSD SD Team updates the PTER to reflect the result of any additional software tool evaluations.

After the approval by NICSD, the module supplier is permitted to use these software tools for their software development. Some of these software tools controlled by the module supplier such as the netlist viewing tool are also used by NICSD IV&V activity. The software tools used by NICSD IV&V activity are specified in the NICSD VVP. The printed circuit board fabricator, under NICSD and the module supplier oversight, uses the FPGA programming tools to embed the FPGA logic into the FPGA chip.

The Microsemi SoC supplies FPGAs and software tools. Microsemi SoC publishes product change, product discontinuation, and general customer notifications. When error notifications are distributed by Microsemi SoC, the module supplier evaluates the error notices to identify possible problems in using the software in the FPGA design as well as the possibility of possible problems in materials already shipped to customers. If potential problems are identified, the module supplier engineer documents the result of the evaluation, and submits the document to NICSD for review. If potential problems are identified for developed or manufactured FPGA products, NICSD engineers contact NED for review and support.

I-3.4 Software Quality Assurance Plan

This section describes the approach, management, organization, responsibilities, and methodologies used to ensure that the development of software products meets the specified requirements for the safety-related FPGA-based system.

I-3.4.1 Software Quality Assurance Planning

ICDD uses the standard nuclear QA program: PSNE QAPD (Reference (b1)) and AS standards for software quality assurance and configuration management activities. NICSD prepares an NICSD Software Quality Assurance Plan (NICSD SQAP) (Reference (c7)) to describe the software quality assurance program that NICSD utilizes to develop and procure the FPGA-based safety-related I&C systems. The NICSD SQAP will be retained from project to project. If project specific requirements are applied, supplemental software quality assurance plan may be generated separately as necessary. The NICSD Software QA Lead (SQAL) is responsible for preparing and implementing the NICSD SQAP. The NICSD SQAP was developed using IEEE Std 730 (Reference (a35)) as a guide. The NICSD SQAP describes the software quality assurance activities performed by NICSD, including the Commercial Grade Dedication (CGD) activities used to designate commercial grade items from the module supplier for use in safety-related applications.

I-3.4.2 Software QA Activities

NICSD has two groups responsible for quality. NICS-QA is responsible for ensuring the process as Staff QA. The NICS-QC is responsible for ensuring items as the line QA/QC group. For software quality assurance activities, both of these groups work together as a Software QA (SQA) Team which is organizationally independent from the NICSD SDL and SD Team. NICS-QA performs verification of the software design activities through internal audits, Commercial Grade (CG) Surveys, and surveillance. NICS-QC performs more direct validation of items including oversight, witness, receiving inspection, test, and inspection.

I-3.4.2.1 SQA Activities for FPGA-based Safety-Related I&C Systems Life Cycle

NICS-QA has the responsibility to ensure that the FPGA-based safety-related I&C systems life cycle is correctly and sufficiently performed. For that purpose, NICS-QA conducts internal audits of each organization inside NICSD at least once a year. In the internal audit, the audit team verifies adequacy of the activities performed under the software life cycle by checking objective evidence using written checklists. The NICSD SQA Team conducts surveillance at the end of each life cycle phase. In the software surveillance, the NICSD SQA Team reviews the NICSD V&V Reports, and Baseline Review Reports prepared by NICSD IV&V Team, to confirm the adequacy of the verification activities. If necessary, the NICSD SQA Team conducts direct surveillance of the NICSD IV&V Team to confirm that the IV&V and baseline review activities are performed appropriately in accordance with the applicable procedures and plans.

NICSD has a responsibility to review and approve the module supplier activities through CGD and IV&V activities. NICS-QA conducts a CG Survey of the module supplier when required by a Commercial Dedication Instruction (CDI). In the CG Survey, the survey team verifies capability of the module supplier to control critical characteristics identified in the CDI. NICS-QC is responsible for verifying and validating that the module supplier products implemented in the FPGA-based system are correctly manufactured and tested without discrepancies.

I-3.4.2.2 SQA Activities for Using FEs

NICSD procures the FPGA-based modules which include the FPGA logic comprised of FEs from the module supplier. The NICSD IV&V Team is responsible for ensuring that all documentation including records and associated data regarding FEs are prepared and controlled by the module supplier and that nonconformances are appropriately identified and dispositioned. The NICSD SQA Team is responsible for ensuring that the FEs used by the module supplier are adequately controlled in accordance with applicable procedures during the CG Survey process and through oversight of the module supplier.

I-3.4.2.3 SQA Activities for Using Software Tools

The NICSD SDL is responsible for controlling software tools used for software development and implementation as described in Section I-3.3.10. The NICSD SDL is responsible for specifying the software tools and their revisions to be used for manufacturing of the modules in a job order to the module supplier as described in Section I-3.3.3.1. NICS-QA is responsible for oversight of the procurement process including the acceptance of the product.

I-3.4.2.4 SQA Activities for Test Equipment Software

The NICSD SDL and NICSD IV&V Lead are responsible for identifying and verifying the test equipment software for module, unit, and system testing. NICS-QA is responsible for ensuring that adequate control is in place and used for the test equipment software through CG Surveys. NICSD IV&V Team is responsible for evaluation of test equipment software through V&V activities. For the module supplier activities, NICSD has a responsibility to review and approve the module supplier activities through CG Survey and through V&V activities. The CG Survey team assigned by the manager of NICS-QA verifies the adequacy of the module supplier control process for test equipment software when it is identified as a Critical Characteristic of module.

I-3.5 Software Integration Plan

The FPGA integration process is well defined in the software development plan of the NICSD SMP, a separate software integration plan will not be prepared.

As described in Section I-3.3.4.2, 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. The FPGA Testing corresponds to the software module testing and the software integration testing in a traditional CPU software life cycle.

After the FPGA Testing, integration of software (i.e. FPGA logic) into production hardware (i.e. FPGA) is done at FPGA implementation as described in Section I-3.3.4.3. The FPGA chip is mounted onto a printed circuit board and integrated to a module assembly. The module is tested at Module Validation Testing. The Module Validation Testing can be considered equivalent to the as module integration test in a traditional CPU based software life cycle.

After the Module Validation Testing, the modules are mounted to the unit chassis, and configured with the unit. The units along with connecting cables are integrated into FPGA-based system. The integrated FPGA-based system is tested at System Validation Testing as described in Section I-3.3.6.1. The System Validation Testing is equivalent to the system integration test in a traditional CPU software life cycle.

I-3.6 Software Integration Report

As mentioned in above section, the FPGA Testing, Module Validation Testing, and System Validation Testing correspond to integration tests. The test reports and V&V reports issued for each testing correspond to integration reports.

I-3.7 Software Maintenance Plan

Maintenance is the process of maintaining and enhancing system performance after installation and acceptance in the plant. Maintenance includes repairing, managing, and implementing pre-planned solutions for nonconforming items and enhancements to software and systems for improving performance or controllability issues. All Maintenance phase activities use the software life cycles under which the systems were implemented.

In Operations and Maintenance Phase, Toshiba will support maintenance activities. Toshiba will provide a system operations and maintenance manual to support maintenance activities.

Antifuse type FPGAs are one-time programmable devices. Therefore, after an FPGA-based product is completed, no changes to the system logic are possible without replacing the older FPGA on a module or replacing the module itself. Any changes to the system must be made under strict change-control procedures, which meet the BTP 7-14 (Reference (a5)). These change control activities are implemented as required in NICSD SCMP (Reference (c8)). Change control process in the Operations and Maintenance Phase are as follows:

- Identify software improvement needs and change request
- Evaluate the scope and impact of required change
- Implement design change and reapply necessary software lifecycle activities
- Update the necessary Configuration Items (CIs) and update baseline

All changes must be thoroughly verified and validated. After an approved change is made, documentation of the change must be archived.

Maintenance activities consist of maintenance of the FPGA logic to remove latent errors, to address revised requirements, or to accommodate modifications in the operating environment.

NED has overall responsibility for maintenance, including determination of whether a design change is necessary. NICSD is responsible for providing to NED any required or suggested changes identified by NICSD. If NED decides to change the design, NED requests NICSD to perform the change activity.

Modifications and enhancements to FEs and FPGAs require that the NICSD and the module supplier design group follow the lifecycle process described in this LTR to address those activities that focus on the design and development of the required or desired changes. After the installation in the nuclear power plant, any modifications are tested at Toshiba and then installed and tested at the plant.

I-3.8 Software Training Plan

Training is a vital aspect of Toshiba organization. Adequate training is necessary to support the development of safe, reliable, high quality software products and to support the long-term use and maintenance of those software products.

This section describes the software training activities to be carried out for staff responsible for design, development, review, and test of systems.

In addition to the training of Toshiba personnel, future applications will require training to be provided to the customer. The scope of project-specific customer training depends upon how the customer will operate and maintain the system. The details of the application-specific training will be documented in a project specific training plan.

I-3.8.1 Qualification and Training Activities by NED

The NED SMP (Reference (c2)) includes qualification and training requirements for NED personnel.

The Senior Manager (SM) and the Group Managers (GPMs) of ICDD are responsible for training and qualification of ICDD personnel except the IV&V Team and the safety staff. The ICDD IV&V Lead is responsible for training and qualification of the ICDD IV&V Team members, and the ICDD System Safety Lead is responsible for training and qualification of the safety staff. The GPMs are responsible for documenting the training as a QA record, and retaining the record.

I-3.8.2 Qualification and Training Activities by NICSD

The NICSD SMP (Reference (c3)) includes a Software Training Plan (STrngP).

The NICSD PM, NICSD SDL, and other leads perform the role of software training lead. The NICSD PM is responsible for appointing managers of respective organizations in NICSD, providing human resource, indoctrination and training of the managers, and approval of the Position Guide Description for the organizations. If required by the customer, the NICSD SDL is responsible for establishing the System O&M Manual which can be used in the customer's personnel training.

The NICSD PM and managers in NICSD are responsible for preparation of the Position Guide Description of their organization and for indoctrination and training of their section/group personnel in accordance with the Position Guide Description.

The NICSD PM and managers in NICSD prepares the “Personnel List for Performing Safety Related Work” to list the personnel performing safety-related work from their group.

The NICSD PM, NICSD SDL, and other leads are 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. They are also responsible for requiring the responsible manager to schedule the necessary training for their personnel.

The manager of NICS-QA is responsible for vendor qualification control including the module supplier. NICS-QA evaluates the supplier competence before ordering. NICS-QA evaluates the module supplier's qualification control for FPGA development and testing. NICS-QA documents the vendor qualification control in a CG Survey Report. The NICSD SDL is responsible for reviewing and approval of the development plan and work schedule made by the module supplier to evaluate their resource and manpower levels.

I-3.9 Software Safety Analysis

At the Project Planning and Concept Definition Phase, the NED and NICSD plans system and software safety analysis activities to establish the processes and activities intended to ensure that the nuclear safety concerns for the software products classified as safety-related are properly considered during the applicable software development life cycle phases.

I-3.9.1 Project Planning and Concept Definition Phase

The ICDD System Safety Lead plans NED system safety analysis activities. The NED Software Safety Plan (SSP) is included in the NED SMP (Reference (c2)). If plant specific documents or plant safety analysis information exists, the ICDD System Safety Lead is responsible for identifying and documenting of the system safety requirements including the requirements derived from the plant specific documents and plant safety analysis information. The ICDD System Safety Lead performs a safety assessment on the Project Planning and Concept Definition Phase outputs (SDD, IED, and IBD) and issues an NED Software Safety Analysis Report (NED SSAR), which is an input for NICSD software safety analysis activities.

The NICSD Software Safety Lead (NICSD SSL) plans software safety analysis activities to be performed by NICSD. The NICSD Software Safety Plan (SSP) is included in NICSD SMP (Reference (c3)). The NICSD SSL is responsible for software safety analysis activities with coordination through the ICDD System Safety Lead. The NICSD Software Safety Team performs safety analysis for the safety requirements identified in the NED SSAR using the method in the NICSD SSP. The NICSD Software Safety Team documents the safety activity result in an NICSD SSAR issued for each phase.

I-3.9.1.1 EDS Review

The NICSD Software Safety Team reviews the Equipment Design Specification (EDS) to ensure that each system safety requirement defined in the SDD, which is also identified in the NED

SSAR, is adequately addressed in the EDS.

I-3.9.1.2 Hazard Analysis

The NED SSAR includes the preliminary hazard analysis. The NICSD Software Safety Team updates the preliminary hazard analysis in each software life cycle. If plant specific documents or plant safety analysis information are not available, Fault Tree Analysis (FTA) will be used for the safety analysis based on the information in the EDS. The results of the analysis are documented in the NICSD SSAR for this phase.

I-3.9.2 Requirements Definition Phase

I-3.9.2.1 Unit DDS Review

The NICSD Software Safety Team reviews the Unit DDSs to ensure that each system safety requirement defined in the EDS is adequately addressed in the Unit DDSs. The results of the safety analysis are documented in the NICSD SSAR for this phase.

I-3.9.2.2 Hazard Analysis

The NICSD Software Safety Team performs a hazard analysis to identify risks requiring additional mitigation and to evaluate the effectiveness of the mitigation measures. Design controls that mitigate the risk and reduce it to negligible levels are identified for all non-negligible risks.

I-3.9.3 Design Phase

I-3.9.3.1 Design Document Review

The NICSD Software Safety Team reviews the Module Design Specifications (MDSs) to ensure that each system safety requirement defined in the Unit DDS is adequately addressed in the MDSs.

The NICSD Software Safety Team reviews each FPGA Design Specification to ensure that each system safety requirement defined in the MDSs is adequately addressed in the FPGA Design Specification.

I-3.9.3.2 FPGA Design Analysis

The NICSD Software Safety Team confirms that the FPGA design include no hazard to the safety to maximize design integrity and minimize the likelihood of common cause failure.

I-3.9.3.3 Hazard Analysis

During the Design Phase, the NICSD Software Safety Team performs a safety assessment to confirm that potential hazards associated with design are adequately resolved to eliminate or at least mitigate possible safety concerns. The NICSD Software Safety Team performs a hazard analysis to identify risks requiring additional mitigation and to evaluate the effectiveness of such mitigations. The NICSD SSAR documents the result of this analysis.

The ICDD System Safety Lead evaluates the NICSD SSAR and documents an NED SSAR based on the evaluation.

I-3.9.4 Implementation and Integration Phase

I-3.9.4.1 Code Analysis

The NICSD Software Safety Team performs a code analysis including analysis of critical and noncritical code from a safety viewpoint to ensure that safe coding practices are implemented. Critical code means a code which performs the safety function(s), while non-critical code means a code which does not perform the safety functions such as a code used for human-machine interface or test functions.

I-3.9.4.2 FPGA Testing Review

The NICSD Software Safety Team reviews FPGA Testing and FE testing from a safety viewpoint to ensure that the software is capable of meeting the system safety requirements. This review makes sure that all safety functions allocated to FPGAs are tested and that acceptance criteria are appropriate. The review of the testing is documented in the NICSD SSAR.

I-3.9.5 Module Validation Testing Phase

The NICSD Software Safety Team reviews the Module Validation Testing from a safety viewpoint to ensure that software safety requirements have been implemented and that testing has proven that the implementation has successfully maintained required levels of system safety requirements. This review makes sure that all safety functions allocated to modules are tested and that acceptance criteria are appropriate. The analysis results are documented in NICSD SSAR for this phase.

I-3.9.6 System Validation Testing Phase

The NICSD Software Safety Team performs an analysis of the System Validation Testing from a safety viewpoint to ensure that software safety requirements have been implemented and that testing demonstrates the required levels of system safety have been successfully maintained. The NICSD Software Safety Team documents the analysis results in a 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 final NICSD SSAR provides evidence that the software safety analysis described in Section I-3.9 has been properly carried out during every software life cycle phase.

The ICDD System Safety Lead evaluates the final NICSD SSAR and documents a final NED SSAR based on the evaluation.

I-3.9.7 Software Safety Change Analysis

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

I-3.10 Software V&V Plan

The software V&V Plan to be applied to all NRW-FPGA applications is provided in the NED VVP (Reference (c6)) and the NICSD VVP (Reference (c9)) and summarized below. A separate software V&V Plan according to plant specific application may be prepared as necessary by the ICDD IV&V Team and by the NICSD V&V Team covering the requirements of IEEE Std 1012 (Reference (a38)) as modified by Regulatory Guide 1.168 (Reference (a13)).

I-3.10.1 Verification and Validation Overview

I-3.10.1.1 Organizations

The overall organizations for the FPGA-based systems are explained in Section I-3.2.1 of this LTR. Engineers from ICDD and NICSD organize IV&V Teams for the V&V of the FPGA logic. The engineers from ICDD and the engineers from NICSD in the IV&V Teams work with each other as one IV&V Team. The ICDD IV&V Team performs the V&V activities defined in this NED VVP independently of the design groups.

I-3.10.1.2 Master Schedule

The IV&V activities and milestones are developed and controlled using a Sub-master Engineering Schedule (SES) for ICDD IV&V activities and an NICSD Engineering Schedule (NICSD ES) for NICSD IV&V Team activities as described in the NED and NICSD SMPs (Reference (c2) and (c3)).

I-3.10.1.3 Software Integrity Level (SIL)

For safety systems, Toshiba applies SIL 4 as defined in Annex A of IEEE Std. 1012-1998 (Reference (a38)).

I-3.10.1.4 Resources

ICDD and NICSD prepare appropriate human resources for V&V activities, meeting the following conditions. All IV&V Team members shall:

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

I-3.10.1.5 Responsibilities

The NED PM assigns the IV&V Lead, and the NICSD PM assigns the NICSD IV&V Lead.

The ICDD IV&V Lead is responsible for the V&V activities of NED and oversees the NICSD activities. The NICSD IV&V Lead is responsible for the V&V activities of NICSD. In addition, the NICSD IV&V Lead assigns the following lead if the NICSD IV&V Lead decides to delegate the testing responsibilities and authority:

- Software Test Lead is responsible for defining test plans, test procedures, and test cases as well as overseeing the performance of testing.

The IV&V Team is also responsible for properly performing and documenting the Baseline Reviews at the end of each life cycle phase. Throughout V&V activities, the IV&V Lead is responsible for ensuring that all anomalies, including those from IV&V reviews and tests, are documented, processed, and closed as much as practicable to minimize impact on the project.

I-3.10.2 Verification and Validation Activities

I-3.10.2.1 Management

Management of V&V is performed throughout the lifecycle phases. The management tasks include the following:

(1) Establishment and Update of the V&V plans

ICDD and NICSD establish their V&V plans and maintain the plans throughout the life cycle phases.

(2) Baseline Change Assessment

The ICDD and NICSD IV&V Team assess the effects of baseline change, and iterate necessary V&V activities based on the assessment.

(3) Management Review

The NED PM oversees the ICDD IV&V Team activities; the NICSD PM oversees the NICSD IV&V Team activities.

(4) Management and Technical Review Support

The ICDD IV&V Team attends the baseline review meetings, which are held every phase to ensure that the required activities during that phase are completed.

(5) Organizational and Supporting Process Interface

The ICDD IV&V Team attends the project management meetings when the ICDD IV&V Lead considers it necessary.

I-3.10.2.2 Project Planning and Concept Definition Phase

The ICDD and NICSD IV&V Teams perform the following activities during this phase as a minimum.

(1) Preparation of V&V Plan

The V&V activities are defined in detail in the NED VVP (Reference (c6)) and NICSD VVP (Reference (c9)). If necessary, a project specific VVP will be prepared to define project specific V&V activities.

(2) Preparation of Software Test Plan

The NICSD IV&V Team prepares a Software Test Plan.

(3) Document Review

ICDD design engineers generate top level design documents including the System Design Descriptions (SDDs), Interlock Block Diagrams (IBDs), and Instrumentation Electrical Diagrams (IEDs). The ICDD IV&V Team reviews these top level design documents and the NED SSAR.

NICSD design engineers generate an EDS based on the top level design documents. The NICSD IV&V Team reviews the EDS and the NICSD SSAR.

(4) RTM Efforts

ICDD design engineers generate top the level RTM based on the top level design documents; NICSD design engineers develop the RTM to the EDS, tracing the requirements in the top level design documents. The ICDD IV&V Team reviews the top level part of the RTM, and the NICSD IV&V Teams reviews the RTM for the EDS. These RTMs are extended into design and test documents in the following life cycle phases.

(5) Security Review

The NICSD IV&V Team reviews that the security requirements are correctly reflected in this phase design documents.

(6) V&V Reporting

See Section I-3.11 for V&V reports.

(7) Baseline Review

The ICDD and NICSD IV&V Teams perform a baseline review to complete this phase.

I-3.10.2.3 Requirements Definition Phase

The ICDD and NICSD IV&V Teams perform the following activities during this phase as minimum.

(1) Document Review

The NICSD IV&V Team reviews the Unit Detailed Design Specifications (DDSs) and NICSD SSAR.

(2) RTM Efforts

NICSD design engineers prepare the RTM tracing the requirements of the Project Planning and Concept Definition Phase and this Requirements Definition Phase. The NICSD IV&V Team reviews the RTM.

(3) Security Review

The NICSD IV&V Team reviews that the security requirements are correctly reflected in this phase design documents.

(4) V&V Reporting

See Section I-3.11 for V&V reports.

(5) Baseline Review

The NICSD IV&V Teams perform a baseline review to complete this phase. The ICDD IV&V Team attends the baseline review for this phase.

I-3.10.2.4 Design Phase

The following V&V activities are performed during this phase.

(1) Preparation of a Software Validation Test Plan (SVTP)

The NICSD IV&V Team prepares an SVTP.

(2) Document Reviews

The module supplier design engineers prepare Module Design Specifications and FPGA Design Specifications. The NICSD IV&V Team performs reviews of these design documents, and the SSAR. The NICSD IV&V Team reviews that the functional requirements of each module defined in the MDS are adequately addressed in the FPGA Design Specification. The NICSD IV&V Team checks the module supplier's control of the FEs that are used for safety-related applications by checking that the FE documents registered in the FE library are appropriately maintained.

(3) RTM Efforts

The module supplier design engineers prepare the RTM tracing the requirements of this

Design Phase and all previous phases. The NICSD IV&V Team reviews the RTM.

(4) Security Review

The NICSD IV&V Team reviews that the security requirements are correctly reflected in this phase design documents.

(5) V&V Reporting

See Section I-3.11 for V&V reports.

(6) Baseline Review

The NICSD IV&V Teams perform a baseline review to complete this phase. The ICDD IV&V Team attends the baseline review for this phase.

I-3.10.2.5 Implementation and Integration Phase

The following V&V activities are performed during this phase:

(1) VHDL Source Code Review

The module supplier generates VHDL source code. The NICSD IV&V Team reviews the VHDL source code to confirm that the code satisfies the design requirements. The NICSD IV&V Team reviews that the programming style of the code for the FPGA is consistent to the programmable logic coding conventions and guidelines document from a safety viewpoint. The NICSD IV&V Team reviews that the interface requirement of each FPGA defined in the MDS are consistent.

(2) Software Tool Message Review

The module supplier design engineers convert the VHDL source code into a netlist and convert the netlist into a fuse map using software tools. The module supplier design engineers check messages from the software tools to confirm that the logic synthesis is performed without errors or problematic warnings. The NICSD IV&V Team verifies the result of the message checks.

(3) Signal Timing Analysis Review

The module supplier has design rules that require signal timing analysis of the FPGAs. The NICSD IV&V Team evaluates the results of the signal timing analysis to verify that the signal timing requirements are satisfied.

(4) Netlist Review

The NICSD IV&V Team reviews the netlist.

(5) Document Review

The module supplier design engineers prepare FPGA Test Procedures, Module Test Procedures, and FPGA Test Reports. The NICSD IV&V Team performs a review of these module supplier documents and the NICSD SSAR. The NICSD IV&V Team reviews that the functional requirements in the FPGA Design Specification and interface requirements in the MDS are adequately addressed in the FPGA Test Procedures.

(6) FPGA Testing

The FPGA Testing is performed by the module supplier design engineers.

(7) Software Tool Control Review

The NICSD IV&V Team reviews the module supplier control of the software tools used in their design and testing.

(8) RTM Efforts

The module supplier design engineers prepare the RTM tracing the requirements of this Implementation and Integration Phase and all previous phases. The NICSD IV&V Team reviews the RTM.

(9) Security Review

The NICSD IV&V Team reviews that the security requirements are correctly reflected in this phase test documents.

(10) V&V Reporting

See Section I-3.11 for V&V reports.

(11) Baseline Review

The NICSD IV&V Teams perform a baseline review to complete this phase. The ICDD IV&V Team attends the baseline review for this phase.

I-3.10.2.6 Module Validation Testing Phase

The following V&V activities are performed during this phase:

(1) Document Review

The NICSD IV&V Team performs review of the module test reports, System O&M Manuals, Software Validation Test Plan (SVTP), and SSAR.

(2) Module Validation Testing

The module supplier performs the Module Validation Testing.

(3) Test Equipment Software Review

The NICSD IV&V Team reviews the module supplier control of the test equipment software.

(4) RTM Efforts

The module supplier design engineers prepare the RTM tracing the requirements of the Module Test Procedures and the Module Design Specifications. The NICSD IV&V Team reviews the RTM.

(5) Security Review

The NICSD IV&V Team reviews that the security requirements are correctly reflected in this phase test documents.

(6) V&V Reporting

See Section I-3.11 for V&V reports.

(7) Baseline Review

The NICSD IV&V Teams perform a baseline review to complete this phase. The ICDD IV&V Team attends the baseline review for this phase.

I-3.10.2.7 System Validation Testing Phase

The following V&V activities are performed during this phase:

(1) Document Review

The NICSD IV&V Team performs a review of the Software Validation Test Report (SVTR), and the final NICSD SSAR. The ICDD IV&V Team reviews the final NED SSAR.

(8) Unit Validation Testing

The NICSD test personnel perform unit validation testing as a part of System Validation Testing.

(2) System Validation Testing

The NICSD test personnel perform System Validation Testing.

(3) Test Equipment Software Review

The NICSD IV&V Team reviews the NICSD control of the test equipment software.

(4) RTM Efforts

NICSD design engineers prepare the RTM to ensure that the units and system validation test procedures cover all functional requirements defined in the EDS and Unit DDSs. The NICSD IV&V Team reviews the RTM.

(5) Security Review

The NICSD IV&V Team reviews that the security requirements are correctly reflected in this phase test documents.

(6) V&V Reporting

See Section I-3.11 for V&V reports.

(7) Baseline Review

The ICDD and NICSD IV&V Teams perform a baseline review to complete the process activities from the Project Planning and Concept Definition Phase through the System Validation Testing Phase.

I-3.11 Software V&V Report

The ICDD IV&V Team and NICSD IV&V Team documents the results of their V&V activities in software V&V reports. An NED Verification and Validation Report (NED VVR) is first prepared at the Project Planning and Concept Definition Phase, and is updated at the end of each life cycle phase, documenting the V&V activities planned for the life cycle phase as described in Section I-3.10. When the NICSD IV&V Team performs V&V activities, the NICSD IV&V Team prepares an NICSD Verification and Validation Report (NICSD VVR). The NICSD VVR is first prepared at the Project Planning and Concept Definition Phase, and is updated at the end of each life cycle phase. The ICDD IV&V Team includes the NICSD VVR in the NED V&V

Report after the NICSD reports are issued.

In addition, the V&V reports include problem reporting with the corrective actions taken and evaluation of metrics.

I-3.12 Software Configuration Management Plan

This section explains the configuration management process for FPGA-based system intended for use in safety-related applications in US nuclear power plants.

I-3.12.1 Software Configuration Management Planning

NED uses PSNE QAPD and AS standards for configuration management activities.

NICSD prepares an NICSD SCMP (Reference (c8)) using IEEE Std 828-1990 (Reference (a37)) as a guide as endorsed by Regulatory Guide 1.169 (Reference (a14)). The NICSD SCMP will be retained from project to project. If project specific requirements are applied, supplemental configuration management plan may be generated separately as necessary.

The NICSD SCMP (Reference (c8)) describes the configuration management activities performed by NICSD, including the configuration management associated with the commercial grade dedication work.

I-3.12.2 Configuration Management Activities

Software configuration management is the process for identifying software Configuration Items (CIs), controlling the implementation of changes to those CIs, recording and reporting the status of changes, and verifying the completeness and correctness of the released items.

The NICSD Software Configuration Lead (NICSD SCL) is responsible for the software configuration management activities in NICSD including the configuration management associated with the commercial grade dedication work.

I-3.12.2.1 Configuration Management

Configuration Items (CIs) are made up of project documents and software elements including the source code for FPGA logic, the fuse map file for FPGA implementation, and the software tools. Each CI is given a unique identification. A document number and a revision number are given to each CI for identification purpose.

NED generates a PCDL to list the project documents controlled by NED, and updates the PCDL in each software lifecycle phase as necessary. NICSD generates an NICSD PCDL to list the project documents controlled by NICSD, and updates the NICSD PCDL in each software lifecycle phase as necessary. NICSD generates an NICSD MCL to list CIs controlled by NICSD, and updates the NICSD MCL in each software lifecycle phase. The NICSD MCL is also used for a traditional hardware configuration control process. The printed circuit board, mechanical drawings, and other hardware aspects are equally controlled using the NICSD MCL.

NICSD's process for establishment of baseline of the FPGA logic, review, and release of fuse maps is described in Section I-3.3.4.3.

I-3.12.2.2 Configuration Control

NED performs change control for the project documents, and documents result of change evaluations in a Design Change Notice (DCN). NICSD conducts change control if a baseline CI change is necessary. Any project member can issue a change request. A Document Change Request (DCR) or Engineering Communication Sheet (ECS) including the necessary information for the change request can be used. A report from a supplier can be used as input information for a change request. The responsible design group identifies the design change and evaluates the impact of change. The Design Change Technical Report (DCTR) is used to record the evaluation of the impact of proposed change and the result of design change. If the change has impact outside NICSD and the module supplier, the NICSD SDL requests NED review of the design change using an ECS prior to implementing the design change.

I-3.12.2.3 Configuration Status Accounting

The NICSD SCL or his designee performs a configuration status accounting for the NICSD Master Configuration List (MCL) and Module MCL in each phase. The NICSD SCL or his designee confirms the latest status of the CIs in the NICSD MCL and Module MCL. The NICSD SCL or NICSD SCL's designee reports the status of the each CI or any concerns related to configuration management at periodic ICDD-NICSD Project Meetings.

I-3.12.2.4 Configuration Management Assessment

The NICSD SC Team conducts a configuration management assessment for the NICSD MCL and

Module MCL in each phase before baseline review by the NICSD IV&V Team. The NICSD SC Team is responsible for preparing a configuration management assessment report ensuring the following items.

- Required activities are completed with required outputs
- Adequacy of quality assurance as defined in NICSD SQAP (Reference (c7))
- Appropriate configuration controls (according to NICSD SCMP) are in place to monitor design activities including document revision and track changes control.

This process allows the NICSD IV&V Team to initiate a baseline review.

I-3.12.2.5 Configuration Audits and Baseline Reviews

NICS-QA conducts an NICSD internal audit, and evaluates whether the NICSD SCMP (Reference (c8)) is implemented appropriately. NICS-QA performs a Commercial Grade (CG) Survey of the module supplier, and evaluates whether the module supplier has acceptable methods, processes, and procedures for configuration management and implements the configuration management appropriately.

The NICSD IV&V Team performs a baseline review at the end of each phase as described in Section I-3.3.1.13. NICS-QA also participates in the baseline review and evaluates that the configuration management activities are correctly performed, especially that the CIs in the NICSD MCL are correctly generated and controlled.

I-3.13 Software Test Plan

The NICSD IV&V Team prepares a Software Test Plan. The Software Test Plan defines the processes and activities used to test the software during the Implementation and Integration Phase through the System Validation Testing Phase. The Software Test Plan defines the scope, approach, resources, and schedule of the testing activities. The Software Test Plan covers the tests described in the following subsections.

I-3.13.1 FPGA Testing

In the Implementation and Integration Phase, the module supplier performs FPGA Testing in accordance with test procedures approved by NICSD under oversight by the NICSD IV&V Team as described in Section I-3.3.4.2. The FPGA Testing is performed taking two separate approaches. The first approach uses a VHDL simulator, and the second approach uses a programmed FPGA.

I-3.13.2 Module Validation Testing

In the Module Validation Testing Phase, the module supplier performs Module Validation Testing to verify that the module performs its intended functions after FPGAs are integrated into module printed circuit board in accordance with test procedures approved by NICSD under oversight by the NICSD IV&V Team as described in Section I-3.3.5.1.

I-3.13.3 System Validation Testing

In the System Validation Testing Phase, NICSD performs System Validation Testing to verify proper functionality of the fully integrated software as described in Section I-3.3.6.1.

I-3.14 Secure Development and Operational Environment (SDOE)

The discussion provided in this section fulfills the regulatory expectations documented in Digital Instrumentation and Controls Interim Staff Guidance 6, Revision 1, for a Vulnerability Assessment for the computers and networks used for system design and development and for the product installed in a nuclear facility. Toshiba concludes that the elements described in this section of the LTR demonstrate that an adequate secure development and operational environment (SDOE) have been established and will be maintained.

Toshiba concludes that their SDOE processes meet the regulatory expectations provided in USNRC RG 1.152, Revision 3, in Regulatory Positions 2.1 through 2.5, inclusive.

I-3.14.1 Toshiba's Secure Development Environment

Toshiba concludes that the protection provided for networks and computers used at the Isogo Engineering Center and at the Fuchu Complex is sufficient to provide a Secure Development Environment. Toshiba further concludes that sufficient computer and physical site security are provided to protect Toshiba's computers and network storage, ensuring that Toshiba's highly proprietary documents, including VHDL code, are adequately protected from the Project Planning and Concept Definition Phase through to the Retirement Phase, from unwanted, inappropriate, undocumented modifications in any computer file.

Toshiba uses multiple echelons of defensive protection. Each echelon is controlled independently and monitored with diverse equipment. Toshiba has designed and applied computer and network protections to provide sufficient security to protect Toshiba's proprietary information. Toshiba's echelons of protection are routinely evaluated, modified, and upgraded to continuously provide effective protection for Toshiba's proprietary information, including the plans, procedures, and instructions used by Toshiba staff; design documents; verification and validation evaluations and reports; system safety evaluations and reports; code and code libraries; test plans, procedures, and reports; production records; and other information

Toshiba's corporate policy restricts discussion, access to, and documentation of their networks and computer protection to maintain an adequate level of security.

I-3.14.2 Secure Operational Environment in Each Life Cycle Phase

Throughout the system lifecycle, Toshiba applies their safety system lifecycle to ensure a consistent application of design, verification and validation, system safety analysis, management, quality assurance, and equipment qualification practices. Toshiba understands the concepts in RG 5.71 (Reference (a21)), and recognizes that safety systems shall be considered Level 4 systems under this regulatory guide. Throughout the system design, any errors or omissions identified in any phase of the lifecycle will be added to the documents under a change control and configuration management process, to ensure that these errors and omissions are handled properly and incorporated into the design.

During the Project Planning and Concept Definition Phase, Toshiba defines the requirements for a system, as well as establishing the graded approach for programmable logic development. Toshiba engineers assess the requirements to identify potential weakness or vulnerabilities of the systems, and establish appropriate counter measures as necessary. Protecting the system from external influences is a key part of this design, to ensure that any access to the system is controlled and that the possibility of undesirable influences from external systems is eliminated, minimized, or at least mitigated to the maximum extent practicable. Absence of remote access and use of uni-directional communication from a safety system to a nonsafety system are important points in the assessment. Use of a non-rewritable FPGA provides significant mitigation of vulnerabilities in an installed system. Requirements are established in this phase, which will be expanded, detailed, implemented, reviewed, analyzed for safety impacts, and tested in subsequent life cycle phases. Communication links are carefully defined, to minimize the possibility of an external system being able to adversely affect the system being designed.

Toshiba requires that all access to safety systems built with the NRW-FPGA technology be located in a vital area and at the same level of protection (Level 4 in USNRC RG 5.71). Guidance and requirements provided in USNRC DI&C-ISG-04 (Reference (a22)) are also incorporated during the design.

During the Requirements Definition Phase, Toshiba defines the security requirements for the external interfaces, the physical system, the functional system, and the programmable logic. The requirements include those defined in the previous phase, which ensures that a secure operational environment will exist in the finished system. These requirements are subject to the V&V activities including independent reviews, traceability analyses, and validation testing throughout the software lifecycle phases. The requirement traceability activities ensures that only requirements defined in the upstream are implemented in the final system, and prevents the introduction of unnecessary or extraneous requirements in the Requirements Definition Phase. Toshiba currently reuses the physical modules in products, as is evidenced by the design of power range neutron monitors for various BWRs. Toshiba can also reuse FPGAs. Toshiba does not incorporate commercial products or products developed by others in the Toshiba-designed programmable logic. Toshiba does incorporate Toshiba-designed Functional Elements into the logic, under strict configuration management and evaluation controls, to ensure appropriate use of these Functional Elements. The requirements incorporated into a system are limited to those that are required to implement a given system, support review and test of FPGAs and modules, support test of modules and units, and provide support for maintenance and troubleshooting after installation in the plant. Communication links are carefully considered in the system designs, with the preference for uni-directional or one-way communication out of the safety system being designed and into other systems. When data has to be received from other systems, communication links are carefully analyzed for vulnerabilities, and identified, known communication link vulnerabilities are eliminated. These vulnerabilities are eliminated by incorporation of additional design requirements, which are verified and validated. System hardware requirements are generated for control of access to cabinets in which the equipment is installed, including application and use of locks on cabinet doors and provision of alarm contacts for each cabinet door.

During the Design Phase, the security requirements defined in the Requirements Definition Phase are translated into designs for both modules and FPGAs. The concepts and requirements for a secure operational environment are incorporated into the Toshiba design. Hardware mechanisms in the programmable logic are defined which ensure that communication links are protected. The design includes hardware and programmable logic features that implement the system, unit, module, and FPGA requirements, while ensuring that the design elaboration does not introduce security vulnerabilities. Capabilities will continue to be provided to ensure that the system is secure and that the security features do not jeopardize the system's ability to perform its safety function or functions. The design activities incorporate only those functions provided in the Requirements Definition Phase, which are the design features that implement the functional requirements, provide support for review and test of FPGAs and modules, provide support for test of modules and units, and provide support for maintenance and troubleshooting after installation in the plant.

During the Implementation and Integration Phase, the FPGA design is translated into programmable logic using Functional Elements. The NICSD IV&V Team verifies the translation. The NICSD IV&V Team conducts security reviews to indentify any potential susceptibilities to inadvertent access from external, by searching for hidden functions or vulnerable features embedded in the code. If any vulnerable feature found, the feature is removed or appropriate measures are taken. Based on the tested nature of Functional Elements and the requirement that all code be implemented using only 100% tested Functional Elements, the basic building blocks of the programmable logic are verified and validated to be free of unnecessary and inappropriate coding. There are no database structures to consider. The implementation is direct, simple, and an exact implementation of the design, with none of the vulnerabilities and means of creating vulnerabilities that are inherent in software designs. The design reviews and verification and validation activities ensure that only the required logic is provided, with no "extra" features. The implementation is direct, and reflective of the design. The secure environment in which the coding is done and the libraries maintained ensures that only the code required is implemented in a given FPGA. Multiple violations of company plans, procedures, processes, and instructions would be required to introduce inappropriate programmable logic. The security reviews evaluates the programmable logic and ensures that hidden functions or vulnerable features are not included. Only the FPGA logic necessary to implement the required functionality is included in the FPGA. No portion of the programmable logic is based on commercial-off-the-shelf logic. Since there are no operating systems, software, or microprocessor emulators in the FPGAs, the vulnerabilities normally associated with these features do not exist in the FPGA, in the module, in the unit, or in the system. Testing is performed during this phase on small pieces of code, starting with Functional Elements, and all of an FPGA in both simulation using a software tool and stimulation using automated hardware and software tools. Both simulation and stimulation testing are performed using the same test vectors, as described in the LTR Section II-2.1.7.

During the Module Validation Testing and the System Validation Testing Phases, testing is performed on modules with integrated FPGAs, on units (i.e., chassis) with the required modules, and on the complete, integrated system. Since security is included in the requirements, detailed design, and coding phases, security is verified and validated by independent review and testing activities during each phase, as well as during each testing phase. External communication links with other systems are tested, including tests to ensure that malformed messages are handled appropriately by this system. Equipment qualification testing is performed using the same programmable logic that Toshiba intends to ship in the final system. The secure operational environment will be demonstrated during all testing, but especially during System Validation Testing or Factory Acceptance Test (FAT). Testing up to FAT will demonstrate that the implementation eliminates or mitigates all identified vulnerabilities, with emphasis on communication links that provide data to the system under test. Testing will also demonstrate that the system is correctly configured, that no unauthorized pathways exist, and that the system operates as required.

During the Operation Phase, the system implemented by Toshiba is operated and reviewed by the nuclear utility to ensure any remaining security vulnerabilities are identified and either eliminated or mitigated through physical changes to the plant or systems, through re-design of an external systems, or through changes to the Toshiba system.

During the Maintenance Phase, Toshiba shall determine and document the lifecycle phases necessary to implement the identified corrections, which shall include performance of the security activities identified herein.

During the Retirement Phase, Toshiba shall help with proper disposal of equipment and documentation supplied to plants that are replacing NRW-FPGA systems, to ensure that other utilities using the same equipment are not jeopardized by inappropriate, unauthorized access to equipment as well as inappropriate access to Toshiba proprietary information.

I-3.14.3 Secure Plant Operational Environment

The programmable logic for each of Toshiba's NRW-FPGA systems is permanently installed in anti-fuses during production at the factory. Changes to the programmable logic would require:

- Removal of the module from the plant system,
- Reverse engineering the programmable logic,
- Creation of appropriate modifications to the programmable logic,
- Removal and replacement of soldered-on FPGAs,

- Re-soldering the FPGA onto the printed circuit board, and
- Reinstallation of the module in the plant.

An attack using this method would require the attacker:

- To have spare printed circuit boards to swap with the installed boards,
- To have valid access to the locked racks in which this equipment is installed,
- Ability to retrieve the programmable logic from probing the integrated circuit (or access to Microsemi SoC's abilities to read the contents of their integrated circuits),
- Ability to decompile the routing from the anti-fuse states,
- Ability to design changes to a program that would still work in normal conditions and only fail on a trigger (when most of the FPGA is in used, leaving little space for such attack programs and leaving a working module),
- Ability to test the modified VHDL for operation outside of the plant system, and
- To have valid access to re-install the modified module without anyone noticing that the system alarmed when the module was removed and that the alarm cleared when the module was re-installed, in all four divisions.

Utilities will not have the capability to change the programming in these modules. Toshiba will not provide the VHDL for these modules. The possibility for an attack through the path described above is very small and requires resources that an attacker would probably consider excessive for the small chance of success.

Toshiba further concludes that these protective controls, measures, and features provided in the systems described in this LTR (and similar systems designed using the same technology) will not adversely affect reliable performance. Toshiba also concludes that the protective controls, measures, and features involved will not adversely affect the reliable performance of any function, including those that are safety related or important to safety.

Communication links are another possible attack vector. Each division of Power Range Monitors (PRMs) and Startup Range Neutron Monitors (SRNMs) provides one-way point-to-point communication links to Toshiba equipment within the division. The possibilities for attack onto the PRM or SRNM through this path do not exist, since these communication links are point-to-point links to Toshiba equipment within the division. Each division of the PRMs and the SRNMs has divisional one-way communication links to non-safety systems through gateways. The possibilities of for attack through this path are unlikely, since these communication links are hardware restricted as uni-directional, point-to-point links and the gateway provides a firewall function.

Communication links exist from the nonsafety core monitoring computer into each division of

PRM to provide a means to upload gain adjustment factors for the individual Local Power Range Monitors (LPRMs). A safety related divisional PRM requests upload of this data to its division only on manual operator request, accepts data only when the single division or channel is bypassed, and only loads the data into the individual LPRM modules when an operator accepts the data for each LPRM on each LPRM module. Appropriate protections are built into the communication link, and manual operator verification is required to accept the single piece of data into each LPRM module. Malformed, short, or long messages are rejected with no adverse effect on the PRM or LPRM. Messages with invalid data would be rejected by the operator. The message structure and data contents are well defined and limited to a specific structure, which offers no reasonable means for an attack. The possibility for attack into the PRM through this path is small.

Each reactor trip channel or division provides their votes to trip to the other channels or divisions, using fixed format messages on one-way point-to-point fiber optic communication links, using Toshiba's internal protocol. Loss of communication on any link is alarmed. Loss of communication with one division results in the affected division or divisions transitioning to a 2-out-of-3 instead of a 2-out-of-4 voting scheme. Loss of multiple divisions results in each division outputting a trip or isolation request out to the load drivers. This is a safety-related system communicating with another safety-related system. Therefore, these point-to-point communication paths are protected from outside attacks, since the safety systems and communication links reside in secure, protected areas, with locked cabinets, and no external communications from nonsafety to safety systems. The possibilities for a successful attack onto the reactor trip system through this path are unlikely.

Communication links can be provided from each division of the reactor trip system to an external system, for sending data and status information to an external system. As these links are one-way, point-to-point fiber optic links, an attack from an external system through these links is physically not possible. An attack pathway in to the reactor trip system through communication links does not exist.

I-3.14.4 SDOE implementation in Toshiba Design and Development Organizations

SDOE is established in NICSD and the module supplier for the FPGA-based safety-related systems in accordance with their internal procedure, which was prepared based on Draft Regulatory Guide DG-1249 (Proposed Revision 3 of Regulatory Guide 1.152), "Criteria for Use of Computers in Safety Systems of Nuclear Power Plant" (Reference (a11)). Toshiba has verified that the Toshiba approach to SDOE is consistent with the finalized RG 1.152, Revision 3. NED follows the Toshiba Information Security Rules and Guidelines (ISRGs) listed in Table 8-1 of the NED SMP (Reference (c2)) as described in item number 1 of Section I-3.14.4.1.

I-3.14.4.1 Basic Policies

NICSD and the module supplier follow the following policies to establish and maintain SDOE to protect FPGA-based safety-related systems from potential weaknesses or vulnerabilities of the digital safety systems throughout the software life cycle.

1. The design documents, code, records, and all other work products associated with the FPGA systems are 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. Toshiba ISRGs are listed in Table 8-1 of the NED SMP (Reference (c2)).
2. No remote access to the safety system is provided. There is no ability to access a computer, node, or network resource that performs a safety function or that can impact the safety function from a computer or node that is located in an area with less physical security than that of the safety system.
3. The development systems shall be isolated from external networks. The development systems have a dedicated network, but this network is not connected to any other networks.
4. The development systems are located in an isolated room with secure access control.
5. Product software is stored in one-time media which is off-line and physically protected.
6. The identification control and password control are required for computers where the development activities for digital safety systems are implemented in accordance with Toshiba internal guidelines which are available for review at Toshiba site. If required by security evaluations, more rigorous access controls to the networks and computers may be applied as appropriate.
7. The physical protection is applied to the development work area and the storage area for the documents and software products. Appropriate control measures shall be employed in the testing area.
8. The security information critical to SDOE is not combined with software life cycle output documents and records information.

I-3.14.4.2 Responsibilities

To establish and manage the SDOE, the following roles and responsibilities are maintained.

- The NICSD PM requires the NICSD SDL and other leads to ensure the existence of and compliance with the requirements for the SDOE.
- The NICSD IV&V Team performs a security assessment for each life cycle phase, and documents the assessment results in NICSD Verification and Validation Report (VVRs) in accordance with the NICSD VVP (Reference (c9)).
- For electronic document control system used by NICSD, the NICSD PM is responsible for registration of users to the system and supervision of access control to the systems.
- The NICSD PM, NICSD SDL, and other leads are responsible for ensuring that team members are cleared for the access to the protected information, systems and areas.

I-3.15 Software/Hardware Development Process Applied to PRM

The software and hardware development process applied to the Power Range Neutron Monitor (PRM) (i.e., the original process) is equivalent to the current process delineated in above sections. The life cycle processes have not changed, but that group and group responsibilities have changed. Appendix I-A of this Part of the LTR describes the difference between the current process and the original process.

I-4 Maintenance Process of SER

Toshiba continuously improve the procedure for the Toshiba FPGA-based I&C Platform. After issuance of the USNRC Safety Evaluation Report (SER), some parts of the product might have to be modified to replace obsolete integrated circuits, provide capabilities that do not exist in the current product, etc. The overall lifecycle process might require updates to reflect changes in Toshiba management structures or quality programs as well.

The improved procedure will include processes for evaluation of the change against the Licensing Topical Report (LTR) and SER. Changes will be processed through the lifecycle of NRW-FPGA-based I&C Platform, which includes equipment qualification testing.

Considering such cases, to the extent that product or process changes are confirmed to be within the established criteria in the LTR and in the SER, the Toshiba FPGA-based I&C platform will be considered consistent and current with the latest LTR and SER. If the product and process changes are judged to be within the LTR and SER, Toshiba will consider the platform to still be within the LTR and SER, but will still provide a comprehensive list of changes to the licensee, such that the licensee evaluates the changes consistent with the requirements of 10 CFR 50.59. If revisions are required to the LTR and SER, then Toshiba will ensure that the LTR is updated to reflect those changes and then reviewed and approved by the USNRC before allowing products developed or maintained under the new process to be installed in US nuclear power plants.

The SER maintenance process is described as follows:

(1) Identify the change(s)

(2) Evaluate impact from the following points:

a. Major Platform Changes including but not limited to
  - Change to basic system architecture
  - Change type of FPGA
  - Add modules, capabilities, or systems not described in the LTR
  - Use new software tools used that could affect the VHDL code

b. Significant Process Changes including but not limited to:
  - Major lifecycle process changes
  - QA program changes that reduce Toshiba's commitment to quality standards
  - Elimination or reduction of software safety evaluations

- Elimination or reduction of independent third party review process

c. Changes that would decrease commitments in the current SER including but not limited to:
 - Reduction in commitments to quality standards listed in the LTR
 - Reduction in performance or Environmental Qualification characteristics
 - Reduction in other USNRC approval bases or assumptions, including regulations and standards

(3) Prepare an SER impact report, including the following contents:

a. Identified change(s)
b. Evaluation process
c. Results of the evaluation
d. Results of safety analyses and V&V
e. Results of equipment qualification testing, if required

(4) Determine a path forward for the impact report

a. If SER impacts exist, submit to the USNRC
b. If no SER impacts exist, provide to the utility

Appendix I-A. Changes from Original Process

This appendix provides a comparison between Toshiba's current process for all NRW-FPGA-based I&C products to be developed including the development and qualification of the OPRM for ABWR, and Toshiba's original process which was applied to the development and the qualification of the PRM for a BWR-5. The original process is documented because Toshiba will continue to supply FPGAs, modules, and units developed under the original process, although modification to these items will be performed under the new process.

While the responsibilities have changed, and 10 CFR 50 Appendix B QA has been extended into Fuchu as shown in Table I-A-1, the work products produced and the FPGA lifecycle were not changed, as shown in Table I-A-2 and Table I-A-3. Table I-A-2 and Table I-A-3 illustrate the changes in roles and responsibilities made when Appendix B was extended into Fuchu, and NICSD was split into NICSD and the module supplier. Table I-A-4 shows a comparison table for codes and standards applied to the current process and original process.

Table I-A-1 Changes in Scope of Appendix B QA Program

Organization	Current Process	Original Process
NED	Appendix B QA Program	Appendix B QA Program
ICDD	Appendix B QA Program	Appendix B QA Program
NICSD	Appendix B QA Program	ISO 9001 QA Program
The module supplier	ISO 9001 QA Program	
The printed circuit board fabricator	ISO 9001 QA Program	ISO 9001 QA Program

NED	Nuclear Energy Systems and Services Division
ICDD	Instrumentation & Control Systems Design and Engineering Department
NICSD	Nuclear Instrumentation & Control Systems Department

Table I-A-2 Changes of Division of Responsibilities for Software Lifecycle Activities

Life Cycle Phases	Current Process			Original Process			Notes
	Activity	Deliverables	Responsible organization	Activity	Deliverables	Responsible organization	
Project Planning and Concept Definition Phase	Identification of design inputs for system design by NED and equipment design by NICSD using Design Input Sheets' (DISs)	DIS for system design DIS for equipment design	ICDD NICSD SD Team	Identification of design inputs for development of equipment requirements	DIS	ICDD	
	Preparation of System Design Description (SDD)	SDD (Design Documentation)	ICDD	Preparation of Equipment Requirement Specification	ERS	ICDD	
	Preparation of Interlock Block Diagram (IBD)	IBD (Design Documentation)	ICDD	(Preparation of ERS)	(included in ERS)	ICDD	
	Preparation of Instrumentation Electrical Diagram (IED)	IED (Design Documentation)	ICDD	(Preparation of ERS)	(included in ERS)	ICDD	
	Preparation of Equipment Design Specification (EDS)	EDS	NICSD SD Team	(Preparation of ERS)	(included in ERS)	ICDD	
	Review of existing Software Management Plan (SMP)	NED SMP NICSD SMP	ICDD NICSD SD Team	Preparation of software management plan	Toshiba ICDD internal procedure	ICDD	
	Review of existing Software Configuration Management Plan (SCMP)	NICSD SCMP	NICSD SD Team	Preparation of Software Configuration Management Plan (SCMP)	(included in SQAP)	ICDD	

Life Cycle Phases	Current Process			Original Process			Notes
	Activity	Deliverables	Responsible organization	Activity	Deliverables	Responsible organization	
Project Planning and Concept Definition Phase	Review of existing Software Quality Assurance Plan (SQAP)	NICSD SQAP	NICSD SQA Team	Preparation of Software Quality Assurance Plan (SQAP)	SQAP	ICDD	
	Review of existing Verification and Validation Plans (VVPs)	NED VVP NICSD VVP	ICDD IV&V Team NICSD IV&V Team	Preparation of Verification and Validation Plan (VVP)	NED VVP NICSD VVP(ISO)	NED V&V team NICSD	
	Preparation of Software Test Plan	Software Test Plan	NICSD IV&V Team	Preparation of Software Test Plan	System Validation Testing Plan	ICDD	
	Preparation of Master Test Plan (MTP)	MTP	NICSD SD Team	Preparation of Master Test Plan (MTP)	MTP	ICDD	MTP in the Original Process is for EQ testing. MTP in the Current process is a whole test plan for the FPGA Testing, Module Validation Testing, and System Validation Testing, Equipment Qualification test, EMC test and other functional tests.
	Software safety analysis for Project Planning and Concept Definition Phase	NED SSAR NICSD SSAR	ICDD NICSD Software Safety Team	Preliminary hazard analysis for Project Planning and Concept Definition Phase	Preliminary Hazard Analysis Report (PHAR)	ICDD	
	V&V of Project Planning and Concept Definition Phase by IV&V Teams	NICSD VVR NED VVR	NICSD IV&V Team ICDD IV&V Team	V&V of the Project Planning and Concept Phase	VVR	NED V&V team	

Life Cycle Phases	Current Process			Original Process			Notes
	Activity	Deliverables	Responsible organization	Activity	Deliverables	Responsible organization	
Project Planning and Concept Definition Phase	Generation of NICSD Master Configuration List (MCL)	NICSD MCL	NICSD SD Team	Generation of Master Configuration List (MCL)	MCL	ICDD	
	Baseline review	Baseline Review Reports (BRRs)	NICSD IV&V Team ICDD IV&V Team	(document review is included in V&V activities)	(included in VVR)	NED V&V team	
Requirements Definition Phase	Preparation of Unit Detailed Design Specification (Unit DDS)	Unit DDS	NICSD SD Team	Preparation of Unit Design Specification	Unit Equipment Design Specification	NICSD	
	Preparation of unit user's manual	Unit User's Manual	NICSD SD Team	Preparation of unit user's manual, to complete before shipment	Unit User's Manual	NICSD	User's Manual for the EQ testing was issued in the Original Process.
	Safety analysis for Requirements Definition Phase	NICSD SSAR NED SSAR	NICSD Software Safety Team ICDD	Hazard analysis for Requirements Definition phase	PHAR	ICDD	
	V&V of Requirements Definition Phase by IV&V Teams	NICSD VVR NED VVR	NICSD IV&V Team ICDD IV&V Team	V&V of Requirements Definition Phase	VVR (including verification of NICSD VVR)	NED V&V team	
	Update of NICSD MCL	NICSD MCL (Updated)	NICSD SD Team	Update of MCL	MCL (Updated)	NICSD	
	Baseline review	BRR	NICSD IV&V Team	(document review is included in V&V activities)	(included in VVR)	NED V&V team	

Life Cycle Phases	Current Process			Original Process			Notes
	Activity	Deliverables	Responsible organization	Activity	Deliverables	Responsible organization	
Design Phase	Preparation of Module Design Specification (MDS)	MDS	The module supplier	Preparation of Module Equipment Design Specification	Module Equipment Design Specification	NICSD	
	Preparation of FPGA Design Specification	FPGA Design Specification	The module supplier	Preparation of FPGA Specification	FPGA Design Specification	NICSD	
	Preparation of Software Validation Test Plan (SVTP)	Software Validation Test Plan (SVTP)	NICSD IV&V Team	---	---	---	In Original Process, preparation of a SVTP is initiated in Module Validation Testing Phase prior to System Validation Testing
	Safety analysis for Design Phase	NICSD SSAR NED SSAR	NICSD Software Safety Team ICDD	Hazard analysis for Design phase	PHAR	ICDD	
	V&V of Design Phase by IV&V Teams	NICSD VVR NED VVR	NICSD IV&V Team ICDD IV&V Team	V&V of Design Phase	VVR	NED V&V team	
	Update of NICSD MCL	NICSD MCL (Updated)	NICSD SD Team	Update of MCL	MCL (Updated)	NICSD	
	Baseline review	BRR	NICSD IV&V Team	(document review is included in V&V activities)	(included in VVR)	NED V&V team	

Life Cycle Phases	Current Process			Original Process			Notes
	Activity	Deliverables	Responsible organization	Activity	Deliverables	Responsible organization	
Implementation and Integration Phase	Generation of VHDL source code	Source Code	The module supplier	Generation of VHDL source code	Source Code	NICSD	
	VHDL source code review	Source Code Review Sheet	NICSD IV&V Team	VHDL source code review	(Code review result is included in Implementation and Integration Phase VVR)	NED V&V team	
	Preparation of FPGA Test Procedure	FPGA Test Procedure	The module supplier	Preparation of FPGA Test Procedure	FPGA Test Procedure	NICSD	
	Preparation of FPGA Test Report	FPGA Test Report	The module supplier	Preparation of FPGA Test Report	FPGA Test Report	NICSD	
	Generation of Module Master Configuration List (MCL)	Module MCL (including FPGA Control Sheet, VHDL source code, Fusemap)	The module supplier	(included in MCL)	(included in MCL)	NICSD	
	FPGA Logic Implementation Request	FPGA Logic Implementation Request/Record Sheet	NICSD SD Team	FPGA Logic Implementation Request	FPGA Logic Implementation Request/Record Sheet	NICSD	
	Preparation of Module Test Procedure	Module Test Procedure	The module supplier	Preparation of Module Test Procedure	Module Test Procedure	NICSD	
	Safety analysis for Implementation and Integration Phase by NICSD	NICSD SSAR NED SSAR	NICSD Software Safety Team ICDD	Hazard analysis for Implementation and Integration phase	PHAR	ICDD	

Life Cycle Phases	Current Process			Original Process			Notes
	Activity	Deliverables	Responsible organization	Activity	Deliverables	Responsible organization	
Implementation and Integration Phase	V&V of Implementation and Integration Phase by IV&V Teams	NICSD VVR NED VVR	NICSD IV&V Team ICDD IV&V Team	V&V of Implementation and Integration Phase	VVR (including verification of NICSD VVR)	NED V&V team	
	Update of NICSD MCL	NICSD MCL (Updated)	NICSD SD Team	Update of MCL	MCL (Updated)	NICSD	
	Baseline review	BRR	NICSD IV&V Team	(document review and software baseline review is included in V&V activities)	(included in VVR)	NED V&V team	
Module Validation Testing Phase	Module Validation Testing	Module Test Report	The module supplier	Module Validation Testing	Module Test Report	NICSD	
	---	---	---	Unit Validation Testing	Unit Test Report	NICSD	In Current Process, unit testing is included in System Validation Testing Phase
	Update of Module MCL	Module MCL (updated)	The module supplier	(included in MCL)	(included in MCL)	NICSD	
	Preparation of System Operations and Maintenance (O&M) Manual	System O&M Manual	NICSD SD Team	Preparation of System Operations and Maintenance (O&M) Manual	Unit User's Manual	NICSD	User's Manual for the EQ testing was issued in the Original Process.

Life Cycle Phases	Current Process			Original Process			Notes
	Activity	Deliverables	Responsible organization	Activity	Deliverables	Responsible organization	
Module Validation Testing Phase	---	---	--	Preparation of System Validation Testing Plan	System Validation Testing Plan	ICDD	In Current Process, preparation of a SVTP is initiated in Design Phase, and the SVTP is approved in Module Validation Testing Phase prior to System Validation Testing
	Safety analysis for Module Validation Testing Phase	NICSD SSAR NED SSAR	NICSD Software Safety Team ICDD	Hazard analysis for Unit/Module Validation Testing phase	PHAR	ICDD	
	V&V of the NICSD Module Validation Testing Phase by IV&V Teams	NICSD VVR NED VVR	NICSD IV&V Team ICDD IV&V Team	V&V of Unit/Module Validation Testing Phase	VVR (including verification of NICSD VVR)	NED V&V team	
	Update of NICSD MCL	NICSD MCL (Updated)	NICSD SD Team	Update of MCL	MCL (Updated)	NICSD	
	Baseline review	BRR	NICSD IV&V Team	(document review is included in V&V activities)	(included in VVR)	NED V&V team	
System Validation Testing Phase	Software Validation Testing	Software Validation Test Report (SVTR)	NICSD IV&V Team	System Validation Testing	System Validation Test Record	NQAD	
	Safety analysis for System Validation Testing Phase	Final NICSD SSAR Final NED SSAR	NICSD Software Safety Team ICDD	Hazard analysis for System Validation Testing phase	HAR	ICDD	

Life Cycle Phases	Current Process			Original Process			Notes
	Activity	Deliverables	Responsible organization	Activity	Deliverables	Responsible organization	
System Validation Testing Phase	V&V of System Validation Testing Phase by IV&V Teams	NICSD VVR NED VVR	NICSD IV&V Team ICDD IV&V Team	V&V of System Validation Testing Phase	Final VVR	NED V&V team	
	Update of NICSD MCL	NICSD MCL (Updated)	NICSD SD Team	Update of MCL	MCL (Updated)	ICDD	
	Baseline review	Baseline Review Reports (BRRs)	NICSD IV&V Team ICDD IV&V Team	(document review is included in V&V activities)	(included in VVR)	NED V&V team	
Operations and Maintenance Phase	Change control	Necessary configuration items will be revised due to change control process	ICDD, NICSD	Change control	Necessary configuration items will be revised due to change control process	ICDD, NICSD	

Table I-A-3 Changes of Division of Responsibilities for CGD Activities

Dedication Steps	Current Process			Original Process		
	Activities	Deliverables	Responsible Organization	Activities	Deliverables	Responsible Organization
Technical evaluation and dedication planning	Safety classification of system	System Design Description (SDD)	ICDD	Safety classification of system	Equipment Requirement Specification (ERS)	ICDD
	Identifying equipment safety function	Equipment Design Specification (EDS)	NICSD SD Team	Identifying equipment safety function	(included in ERS)	ICDD
	Dedication planning	CGD Plan	NICSD SD Team	Dedication planning	Qualification Plan	ICDD
	Preliminary technical evaluation for commercial grade item identifying system and component level critical characteristics	Preliminary Technical Evaluation Report (PTER)	NICSD SD Team	Preliminary technical evaluation for commercial grade item identifying system and component level critical characteristics	Preliminary Technical Evaluation Report (PTER)	ICDD
	Procurement planning	Procurement Planning Sheets (PPS)	NICSD SD Team	Procurement planning	Procurement Planning Sheets (PPS)	ICDD
	Identifying Unit safety function and module requirement function	Unit Detail Design Specifications	NICSD SD Team	Identifying Unit safety function	(included in ERS)	ICDD
	Identifying critical characteristics and defining acceptance planning for each item	Commercial Dedication Instruction (CDI)	NICSD SD Team	Acceptance planning for project	Acceptance Plan for CGI/CGS	ICDD
	Preparation of procurement document including technical and QA requirements	Procurement Document to the module supplier and commercial suppliers	NICSD SD Team (reviewed by NICS-QC)	Preparation of technical specification	Procurement Specification to NICSD	ICDD
				Preparation QA specification	QA Specification to NICSD	NQAD

Dedication Steps	Current Process			Original Process		
	Activities	Deliverables	Responsible Organization	Activities	Deliverables	Responsible Organization
Acceptance activities	Issuance of Job Order to the module supplier	Job Order	NICSD SD Team	Issuance of Job Order to NICSD	Job Order	ICDD/Sourcing Dept.
	Vendor evaluation (Commercial Grade Survey as required)	CG Survey Report	NICS-QA	Vendor evaluation (Commercial Grade Survey as required)	CG Survey Report	ICDD
	Critical Digital Review as required	CDR Report	NICSD, ICDD	Critical Digital Review as required	CDR Report	ICDD
	Qualified vendor registration	Qualified Vendor List (QVL)	NICS-QA	Qualified vendor registration	Qualified Vendor List (QVL)	NQAD
	Supplier design and testing documents review	Design Verification Reports (DVRs) and V&V reports	NICSD IV&V Team	Supplier design and testing documents review	Design Verification Reports (DVRs) and V&V reports	NED IV&V Team
	Source verification activities as required	Source Verification Reports	NICS-QC	Source verification activities as required	Source Verification Reports	NQAD
	Special testing and inspection as required	Test reports, Inspection reports	NICS-QC	Special testing and inspection as required	Test reports, Inspection reports	NQAD
	Receiving inspection	Receiving Inspection Report	NICS-QC	Preparation of acceptance records of CGI/CGS	Acceptance Records of CGI/CGS	NQAD
	Reporting CGD activities for each items	CGD Report	NICSD SD Team	Reporting CGD activities for project incorporating supplemental vendor evaluation	Final Technical Evaluation Report (FTER)	ICDD
	Reporting CGD activities for project incorporating supplemental vendor evaluation result and CGD reports	Final Technical Evaluation Report (FTER)	NICSD SD Team			ICDD
	Packaging CGD documents	CGD Package	NICSD SD Team	Packaging CGD documents	CGD Package	ICDD

Table I-A-4 Changes in Referenced Codes and Standards

Reference No. in Acronym and Reference Part	Current Process	Original Process	Notes
(a1)	10 CFR 21 "Reporting of Defects and Noncompliance"	No change	
(a2)	10 CFR 50 Appendix B "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants"	No change	
(a3)	ASME NQA-1-1994, and NQA-1-2008 and the NQA-1a-2009 Addenda "Quality Assurance Program Requirements for Nuclear Facilities"	ASME NQA-1-1989 "Quality Assurance Program Requirements for Nuclear Facilities"	Internal gap analysis shows no practical impact on the PRM qualification.
(a4)	USNRC Standard Review Plan (SRP), NUREG-0800 Section 7, 2010	No change	
(a5)	USNRC Standard Review Plan (SRP), NUREG-0800, Branch Technical Position 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems," Rev.5, March 2007	No change	
(a6)	USNRC Standard Review Plan (SRP), NUREG-0800, Branch Technical Position 7-17, "Guidance on Self-Test and Surveillance Test Provisions", Rev.5, March 2007	No change	

Reference No. in Acronym and Reference Part	Current Process	Original Process	Notes
(a7)	USNRC Standard Review Plan (SRP), NUREG-0800, Branch Technical Position 7-18, "Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems," Rev.5, March 2007	No change	
(a8)	USNRC, Regulatory Guide 1.28 "Quality Assurance Program Requirements (Design and Construction)(Task RS 002-5)," Rev. 3, August 1985	No change	
(a9)	USNRC, Regulatory Guide 1.75 "Physical Independence of Electric Systems," Rev.3, February 2005	USNRC, Regulatory Guide 1.75 "Physical Independence of Electric Systems," Rev.2, February 5	Internal gap analysis shows no practical impact on the PRM qualification.
(a10)	USNRC Regulatory Guide 1.105 "Setpoints for Safety-Related Instrumentation," Rev.3, December 1999	No change	
(a11)	USNRC Draft Regulatory Guide Regulatory Guide 1.152 "Criteria for Use of Computers in Safety Systems of Nuclear," Rev.3 July 2011	USNRC Regulatory Guide 1.152 , Rev 2, "Criteria for Programmable Digital Computer System Software in Safety Related Systems of Nuclear Power Plants," January 2006.	Internal gap analysis shows no practical impact on the PRM qualification. Toshiba complies with the new guidance on a Secure Development and Operational Environment. Toshiba concludes that the equipment supplied, if properly installed, would comply with the guidance in RG 5.71 on cyber security.
(a12)	USNRC Regulatory Guide 1.153 "Criteria for Safety Systems, " Rev.1, June 1996	No change	

Reference No. in Acronym and Reference Part	Current Process	Original Process	Notes
(a13)	USNRC Regulatory Guide 1.168 "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Rev. 1, February 2004	No change	
(a14)	USNRC Regulatory Guide 1.169 "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," September 1997	No change	
(a15)	USNRC Regulatory Guide 1.170 "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," September 1997	No change	
(a16)	USNRC Regulatory Guide 1.171 "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," September 1997	No change	
(a17)	USNRC Regulatory Guide 1.172 "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," September 1997	No change	
(a18)	USNRC Regulatory Guide 1.173 "Developing Software Lifecycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," September 1997	No change	

Reference No. in Acronym and Reference Part	Current Process	Original Process	Notes
(a19)	USNRC Regulatory Guide 1.180 "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," Rev. 1, October 2003	No change	
(a20)	USNRC Regulatory Guide 1.209 "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants," March 2007	No change	
(a24)	MIL-HDBK-217F "Reliability Prediction of Electronic Equipment"	No change	
(a25)	MIL-STD 461E "Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment"	No change	
(a26)	IEC 61000-4-2-1995 "Electromagnetic compatibility (EMC) - Part 4-2: Testing and measurement techniques - Electrostatic discharge immunity test"	No change	
(a27)	IEC 61000-4-4-1995 "Electromagnetic compatibility (EMC) - Part 4-4: Testing and measurement techniques - Electrical fast transient/burst immunity test"	No change	

Reference No. in Acronym and Reference Part	Current Process	Original Process	Notes
(a28)	IEC 61000-4-5-1995 "Electromagnetic compatibility (EMC) - Part 4-5: Testing and measurement techniques - Surge immunity test"	No change	
(a29)	IEC 61000-4-12-1995 "Electromagnetic compatibility (EMC) - Part 4-12: Testing and measurement techniques - Ring wave immunity test"	No change	
(a30)	IEEE Std 7-4.3.2-2003 "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generation Stations"	IEEE Std 7-4.3.2-1993, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generation Stations" and IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generation Stations"	Internal gap analysis shows no practical impact on the PRM qualification.
(a31)	IEEE Std 323-1983 "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations"	No change	
(a32)	IEEE Std 344-1987 "IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations"	No change	
(a33)	IEEE Std 352-1987 "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems"	No change	
(a34)	IEEE Std 384-1992 "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits"	No change	

Reference No. in Acronym and Reference Part	Current Process	Original Process	Notes
(a35)	IEEE Std 730-2002 "IEEE Standard for Software Quality Assurance Plans"	No change	
(a36)	IEEE Std 603-1991 "IEEE Standard for Safety Systems for Nuclear Power Generating Stations"	No change	
(a37)	IEEE Std 828-1990 "IEEE Standard for Software Configuration Management Plans"	No change	
(a38)	IEEE Std 1012-1998 "IEEE Standard for Software Verification and Validation"	No change	
(a39)	IEEE Std 1028-1997 "IEEE Standard for Software Reviews"	USNRC, Regulatory Guide 1.168, which refers to IEEE1028-1998.	Internal gap analysis shows no practical impact on the PRM qualification.
(a40)	IEEE Std 1076-2000 "IEEE Standard VHDL Language Reference Manual"	No change	
(a41)	IEEE Std 1164-1993 "IEEE Standard Multivalue Logic System for VHDL Model Interoperability"	No change	
(a42)	EPRI NP-5652 "Utilization of Commercial Grade Items in Nuclear Safety Related Applications," March 1988	No change	
(a43)	EPRI TR-102260 "Supplement Guidance for the Application of EPRI Report NP-5652 on the Utilization of Commercial Grade Items," March 1994	No change	
(a44)	EPRI TR-102323 "Guidelines for Electromagnetic Interference Testing of Power Plant Equipment," November 2000, Rev. 2	No change	

Reference No. in Acronym and Reference Part	Current Process	Original Process	Notes
(a45)	EPRI TR-106439 "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," October 1996	No change	
(a46)	EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," December 1996	No change	
(a47)	EPRI TR-107339 "Evaluating Commercial Digital Equipment for High Integrity Applications," December 1997	No change	
(a48)	Electric Power Research Institute (EPRI) Technical Report 1011710 "Handbook for Evaluating Critical Digital Equipment and Systems," November 2005	Not referenced	In the original process, the document was not freely open to the public. However Internal gap analysis shows equivalent methodologies were taken in the original process. Author of EPRI report consulted with Toshiba on CDR The contractor assisting with the CDR is one of two co-authors of the EPRI report, which updates the methodology in EPRI TR-107339. The updated methodology was applied to this CDR.