

TOSHIBA CORPORATION

1-1, SHIBAURA 1-CHOME, MINATO-KU TOKYO 105-8001, JAPAN
PHONE: +81-3-3457-3734
FACSIMILE: +81-3-5444-9195

No. TOS-TR-GNL-2007-0006

November 16, 2007

Document Control Desk
United States Nuclear Regulatory Commission
Washington, DC 20555-0001

Subject: Toshiba Topical Report, NRW-FPGA-Based I&C System Design Process:
Submittal of Non-Proprietary Report Version with Corrected Marking

Reference: NRC Project Number 729; NRC Docket Number 00000729

Ladies and Gentlemen:

Toshiba is hereby submitting Revision 0 of the non-proprietary version of our Topical Report on our project to describe Toshiba's design, development, peer review, test, qualification, and manufacturing processes for NRW-FPGA-based I&C systems for US nuclear safety-related applications. Toshiba is submitting this topical report under the NRC licensing topical report program for review for referencing in licensing actions.

This transmittal forwards one (1) original of UTLR-0001-NP, "Topical Report of NRW-FPGA-Based I&C System Design Process" (NON-PROPRIETARY MARKUP VERSION) November 16, 2007. This submittal supersedes our November 3, 2007 submittal of this document which had incorrect marking on the cover page indicating that the report version was proprietary.

Should you have any questions regarding this request, please contact Ms. Rossnyev Alvarado at (703) 519-0200 or via e-mail at ralvarado@mpr.com, or Mr. Ryuji Iwasaki via e-mail at ryuji.iwasaki@toshiba.co.jp.

Sincerely,



Kiyoshi Okamura
Senior Manager
Plant Project Engineering Department
Nuclear Energy Systems & Services Division
POWER SYSTEMS COMPANY
TOSHIBA CORPORATION

cc: Ms. Stacey Rosenberg, Ms. Vanice Perin, USNRC (w/o enclosure)

Topical Report
NRW-FPGA-Based I&C System Design Process

M. Oda Nov. 16, 2007

Approved by
Monitoring System Engineering Group

Toshiba Corporation
Nuclear Energy Systems & Services Division

Table of Contents

Abstract	1
1. Introduction	6
1.1. Toshiba FPGA-based Systems	6
1.2. Purpose and Scope.....	8
2. Toshiba FPGA-Based I&C System Quality Assurance Process	10
2.1. Process and QA Overview.....	10
2.2. Quality Assurance Programs	13
2.2.1. PSNE Quality Assurance Program Description	14
2.2.2. Fuchu Complex QA Program.....	18
2.3. Vendor Evaluations.....	19
2.3.1. NED's Evaluation of Fuchu Complex	20
2.3.2. Audit of Actel.....	21
2.4. Critical Digital Review.....	22
2.4.1. Critical Digital Review of NICSD	23
2.4.2. Critical Digital Review of Actel.....	24
3. System Description.....	25
3.1. General Description of System Development Cycle.....	25
3.2. General Description of System Architecture.....	27
3.2.1. Units	29
3.2.2. Modules.....	29
3.2.3. FPGAs	29
3.2.4. Functional Elements.....	30
3.3. Establishing System Functional and Design Requirements	30
3.4. NRW-FPGA Features	33
4. FPGA Logic Development Lifecycle	34
4.1. Qualification Approach and Criteria	37
4.1.1. Standard Review Plan and Regulatory Guide.....	37
4.1.2. IEEE Standard 7-4.3.2.....	39
4.1.3. BTP 7-14 and BTP 7-18.....	39
4.1.4. EPRI TR-107330.....	40
4.1.5. IEEE Standard 1012	41
4.1.6. EPRI TR-106439.....	43
4.1.7. Cyber Security.....	48
4.2. Overview of FPGA Logic Lifecycle	51
4.3. System Design and Integration Process	56
4.3.1. Developing FPGAs	56
4.3.2. Integrating a Module.....	61
4.3.3. Integrating a Unit	62
4.3.4. Integrating a System.....	64
4.3.5. FPGA Design Principles	64
4.3.6. Developing and Using Functional Elements.....	72
4.3.7. Change Control	78

4.3.8. Maintenance	78
4.3.9. Software Tool Control and Maintenance	79
4.4. Verification and Validation Process.....	80
4.4.1. Design Verification.....	81
4.4.2. Validation Test.....	82
4.5. V&V Results	91
5. Hardware Qualification Process.....	92
5.1. Qualification Testing	92
5.2. Qualification Analysis	94
5.3. Hazard Analysis.....	95
6. Implementing Toshiba’s Generic Qualification Process for Application-Specific Equipment	96
6.1. Generating a Qualified System.....	97
6.2. Organization of an Application-Specific Topical Report	98
6.3. Modifying an Existing Application	100
7. References	101
Appendix A - Summary of Applicable NED and NICSD Instructions	107
Appendix B - Actel FPGA Features	111

List of Tables

Table 4-1. [[]]FPGA Processes.....	36
Table 4-2. Critical Characteristics for Digital Systems		44
Table 4-3. Errors Anticipated for Each Phase of the Development Process.....		90
Table 4-4. Countermeasures Against Errors Specific to FPGA-based Systems		91
Table A-1. NED Standards		107
Table A-2. ICDD Procedure		109
Table A-3. NICSD Procedural Standards		109
Table B-1. Software Vendors and Tools.....		115

Abstract

Toshiba currently markets digital control systems for service in Japanese commercial nuclear power applications, including safety and protection systems. Toshiba is currently developing Non-rewritable (NRW) Field Programmable Gate Array (FPGA)-based safety-related Instrumentation and Control (I&C) hardware for use in Japanese and US nuclear power plant safety-related applications.

The FPGA-based components in this hardware are composed of integrated circuits designed specifically by their commercial vendor to provide logic which can be physically embedded on FPGA chips using special tools. These circuits are designed to perform simple logic functions which can be combined and arranged in specific patterns to perform logical operations for signal processing.

Once the logic is embedded, the logic is hardwired and does not change. Consequently, the FPGA components are treated as hardware. The advantages of an FPGA platform are that the logic execution is completely defined, simple (compared to computer-based systems), and verifiable. FPGAs provide stable technology to minimize the risk of technology obsolescence. Since the FPGA performs processes using integrated circuits, the FPGA executes application logic without operating systems or application software, and thus has inherent advantages over other digital systems.

However, the logic for these FPGA-based components is designed and manufactured by a process which is similar to generating software. Specifically, Toshiba uses a hardware description language called Very High Speed Integrated Circuit (VHSIC) Hardware Definition Language (VHDL) to define the function of the circuits on the integrated circuit. To implement this process, Toshiba has developed a high quality design and manufacturing process for NRW-FPGA-based systems, with a lifecycle process suitable for the design and development of I&C systems for US nuclear safety-related applications.

This topical report is being submitted to the United States Nuclear Regulatory Commission (USNRC) for review and approval of the Toshiba NRW-FPGA-based system design and development processes for systems for use in safety-related applications in US nuclear power plants. The USNRC approval will be provided in a Safety Evaluation Report (SER). The FPGA-based I&C systems described in this topical report are designed as a replacement for the existing analog and CPU-based I&C systems in use in US nuclear applications.

This topical report describes Toshiba's design, development, peer review, test, qualification, and manufacturing processes for NRW-FPGA-based systems for US nuclear safety-related applications. The description includes: 1) quality assurance programs and activities, 2) lifecycle approach to FPGA logic development, including the validation and verification (V&V) and hazards analysis processes, 3) hardware qualification process, and 4) generic qualification process for specific safety-related systems. The qualification is based on the

Electric Power Research Institute (EPRI) Technical Report TR-107330 (Reference (20)). Toshiba will use these processes in conjunction with latest USNRC guidance for future qualification of specific NRW-FPGA-based systems. Qualification activities for these specific systems will be documented by Toshiba in separate topical reports as they are completed.

Acronyms

AFM	Actel Fuse Map
APRM	Average Power Range Monitor
AS	Toshiba Nuclear Energy Systems and Services Division Work Standard
ASIC	Application Specific Integrated Circuit
ASME	American Society of Mechanical Engineers
BTP	Branch Technical Position
BWR	Boiling Water Reactor
C-cells	Combinatorial cells
CDR	Critical Digital Review
CFR	Code of Federal Regulations
CG	Commercial Grade
CGD	Commercial Grade Dedication
CGI	Commercial Grade Item
CGS	Commercial Grade Service
CM	Configuration Management
CPU	Central Processing Unit
DIN	Deutsches Institut für Normung
DoD	United States Department of Defense
EDIF	Electronic Design Interchange Format
EEPROM	Electrically Erasable Programmable Read-Only Memory
EFT/B	Electrical Fast Transient / Burst
EMI/RFI	Electro Magnetic Interference/ Radio-Frequency Interference
EPRI	Electric Power Research Institute
ERS	Equipment Requirement Specification
ESFAS	Engineered Safety Features Actuation System
FE	Functional Element
FF	Flip-Flop
FIT	Failure In Time
FIR	Finite Impulse Response
FPGA	Field Programmable Gate Array
FMEA	Failure Mode and Effects Analysis
GPIB	General Purpose Interface Bus
G-TR	Generic Topical Report
HDL	Hardware Description Language
HMI	Human Machine Interface
I&C	Instrumentation and Control
IBD	Interlock Block Diagram
ICDD	Control and Electrical Systems Design and Engineering Department
IDE	Integrated Development Environment
IED	Instrumentation Electrical Diagram

IEEE	Institute of Electrical and Electronics Engineers
I/O	Input/Output
IPS	Industrial and Power Systems and Services Company
IPSNE	Industrial and Power Systems and Services Company Nuclear Energy
ISO	International Organization for Standardization
IV&V	Independent Verification and Validation
JTAG	Joint Test Action Group
LED	Light Emitting Diode
LPRM	Local Power Range Monitor
MHz	Mega Hertz
MPR	MPR Associates, Inc.
MSI	Medium-scale Integrated
MTP	Master Test Plan
NASA	United States National Aeronautics and Space Administration
NED	Nuclear Energy Systems and Services Division
NICSD	Nuclear Instrumentation and Control Systems Department
NNR	Nonconformance Notice Report
NQA	Nuclear Quality Assurance
NQAD	Quality Assurance Department, Nuclear Energy Systems and Services Division
NRW	Non Re-writable
NUREG	Nuclear Regulation
PC	Personal Computer
PHA	Preliminary Hazards Analysis
PPED	Plant Project Engineering Department
PQAM	Project Quality Assurance Manual
PQAP	Project Quality Assurance Plan
PRM	Power Range Monitor (or Power Range Neutron Monitor)
PRS	Problem Reporting Sheet
PS	Power Systems Company
PSNE	Power Systems Company, Nuclear Energy
PTER	Preliminary Technical Evaluation Report
PWR	Pressurized Water Reactor
QA	Quality Assurance
QAPD	Quality Assurance Program Description
QVL	Qualified Vendors List
R-cells	Register cells
RCV	Receive
RBM	Rod Block Monitor
RG	Regulatory Guide
RTM	Requirements Traceability Matrix
SIL	Software Integrity Level
SLCP	Software Lifecycle Process
SQAP	Software Quality Assurance Plan
SQR	Software Qualification Report

SRP	Standard Review Plan
SRS	Software Requirements Specification
TR	EPRI Technical Report
US	United States
USNRC	United States Nuclear Regulatory Commission
V&V	Verification and Validation
VHDL	Very High Speed Integrated Circuit Hardware Definition Language
VHSIC	Very High Speed Integrated Circuit
VME	VersaModule Eurocard bus
VVP	V&V Plan
VVR	V&V Report

1. Introduction

This topical report defines the process Toshiba uses to define, design, develop, review, test, and qualify Field Programmable Gate Array (FPGA)-based safety systems. This generic process is modeled on the IEEE Software Processes, and defines a methodology for generating FPGA-based systems which Toshiba concludes are suitable for safety-related use in US nuclear power plants. Toshiba intends to provide additional topical reports describing the application of this generic process to specific systems. Any changes or enhancements to the process defined in this generic report will be discussed with the USNRC and documented in either a revision to this topical report or in the system-specific topical report in which the process was applied. This topical report reflects a process that has been used to develop the first FPGA-based system intended for use in US nuclear power plant applications.

Toshiba designed this process based on the guidance provided in United States (US) Nuclear Regulatory Commission (NRC) Regulatory Guides (RGs) and the Institute of Electrical and Electronics Engineers (IEEE) standards applicable to nuclear power applications. These include RG 1.153 (Reference (9)) which endorses IEEE Standard 603-1991 (Reference (25)). Since these are digital devices, RG 1.152 (Reference (8)) and IEEE Standard 7-4.3.2-2003 (Reference (24a)) were also applied. Development of this process considered all the guidance provided in Regulatory Guides 1.168, 1.169, 1.170, 1.171, 1.172, and 1.173 (References (10) through (15)).

1.1. Toshiba FPGA-based Systems

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 (PRM) for individual plants, up to designing and manufacturing the world's first fully integrated CPU-based Boiling Water Reactor (BWR) digital system. This system was installed and is in use at Kashiwazaki-Kariwa Unit 6.

Toshiba has previously produced analog and central processing unit (CPU)-based (i.e., software-based) devices for systems such as neutron monitoring for Japanese utilities. However, there are limitations to analog and software-based systems:

- Analog systems are subject to signal drift and obsolescence. Signals may drift to the point where required safety actions may not occur when required, or occur spuriously when not required. Obsolescence requires design evaluation to find appropriate replacements for aging analog components, or at times complete redesign when appropriate replacement analog components cannot be found. Vendors find it difficult to commit to providing replacements for failed or degraded analog components for the life of the plants where they are installed.
- In conventional CPU-based systems, the digital circuits may be unavailable in a short

number of years, or even between the time the system is designed and when the system is installed in a plant. When the digital circuit become unavailable, design evaluations and redesign are required. For digital components, the design problem is even more difficult than for analog systems, since functionality of digital components is much more integrated, with very little chance of finding a replacement integrated circuit that will fit in the existing printed circuit board, or perform the same functions. As with analog systems, the vendor is faced with the same problem for long-term support, having to redesign printed circuit boards or buy and store large quantities of integrated circuits to reduce the number of design cycles through the life of the system in nuclear power plants.

Because of these limitations for both conventional analog systems and CPU-based systems, Toshiba has chosen to develop I&C technology based on non-rewritable (NRW) FPGAs. NRW-FPGA-based systems provided by Toshiba process signals primarily by digital circuits embedded on FPGA chips. The systems may have a few analog circuits that process detector signals as inputs. The analog signals are converted to digital signals, and then processed by FPGA circuits. FPGA-based I&C systems have the benefit of calibration drift reduction associated with CPU-based systems, without the need for CPUs, operating systems, or application software. Other advantages of an FPGA platform are that the logic design is rigorous, simple (compared to computer-based systems), deterministic, and verifiable. The FPGAs provide stable technology to minimize the risk of technological obsolescence. Additional discussion of the advantages of similar technology, specifically the Application Specific Integrated Circuit (ASIC), can be found in Nuclear Regulation/Contractor Report (NUREG/CR)-6812 (Reference (4)).

Toshiba has supplied FPGA-based I&C systems to Japanese Nuclear Power Plants for years. Note that Toshiba did not follow the process described in this topical report because the process requirements for Japanese plants are different. For example, Toshiba supplied FPGA-based non-safety and safety-related process radiation monitors to the following plants:

- Fukushima Daiichi-2,
- Fukushima Daini-1,
- Fukushima Daini-3,
- Kashiwazaki Kariwa-1, and
- Tsuruga-1.

In addition, Toshiba supplied the FPGA-based safety-related Power Range Monitor (PRM) system to Kashiwazaki Kariwa-2.

Signal processing functions embedded in an FPGA are composed of physical circuits. Toshiba uses a common development language, called Very-High-Speed Integrated Circuit (VHSIC) Hardware Description Language (VHDL), to develop the logic for the FPGA. VHDL is a development language which is similar to conventional programming languages. VHDL is used to code digital logic circuits and provide the mechanism for embedding logic into the

FPGA. In Toshiba's FPGA-based safety-related I&C systems, the logic is built from functional elements (FEs), which perform simple logic functions. These functional elements are designed and independently verified. Toshiba uses only these simple functional elements in combinations to develop the more complex system logic. Once the logic is embedded in an FPGA, it is hardwired and does not change; consequently the FPGA is treated as hardware.

Toshiba intends to supply NRW-FPGA-based products for use in United States (US) safety-related I&C systems. To supply hardware for these products, Toshiba will use its commercial manufacturing processes and commercial grade dedication. To design the logic for these products, Toshiba has developed an FPGA digital logic lifecycle process similar to that used for design and development of software. Toshiba uses this lifecycle process because the VHDL language used to embed the digital logic into FPGAs is similar to software code.

Toshiba has used this FPGA logic lifecycle process to design an NRW-FPGA-based Power Range Monitor (PRM) system. This system was used to test Toshiba's processes for designing, developing, and qualifying NRW-FPGA systems, and is currently being qualified for US applications.

Toshiba's qualification approach for NRW-FPGA-based I&C systems is based on the Electric Power Research Institute (EPRI) Technical Report (TR)-107330 (Reference (20)). The generic qualification approach described in EPRI TR-107330 includes both hardware and software qualification activities. Toshiba modified the software qualification approach described in EPRI TR-107330 to fit the NRW-FPGA technology.

Toshiba has extensive Quality Assurance (QA) experience in designing and supplying safety grade systems to Japanese nuclear power plants. Toshiba has previously produced analog and CPU-based devices for neutron monitoring in Japanese utilities. Toshiba makes extensive use of this experience in the design and manufacture of new FPGA-based safety-related I&C system products for the Japanese market, with the intent of eventually marketing this equipment to US nuclear plants. Toshiba established its FPGA logic lifecycle process in accordance with its Title 10 of the Code of Federal Regulations (CFR) Part 50, Appendix B Quality Assurance Program (Reference (1)).

1.2. Purpose and Scope

The purpose of this report is to describe Toshiba's lifecycle process for developing FPGA-based I&C systems, and to explain how this process is suitable for US nuclear safety-related applications. This report is being submitted to the United States Nuclear Regulatory Commission (USNRC) for review and approval.

This report includes the following information:

- Section 2 describes the quality assurance programs and activities used by Toshiba for design,

manufacturing and qualification of FPGA-based systems.

- Section 3 describes Toshiba's FPGA-based system architecture, and the system specifications and documentation that Toshiba uses to define a generic FPGA-based system.
- Section 4 describes Toshiba's lifecycle approach to FPGA logic development, including the validation and verification (V&V) processes used in this development.
- Section 5 describes the generic Toshiba hardware qualification process, which consists of qualification testing and analyses.
- Section 6 describes how Toshiba will implement this generic qualification process for qualification of specific safety-related systems.
- Section 7 lists reference documents.

This generic topical report (G-TR) is intended to define the basis for the development process applied to system-specific topical reports. Toshiba will follow the process defined in this topical report to design, manufacture, and qualify each FPGA-based system, and document the results of each qualification in a separate topical report. The system topical report will:

- Define Toshiba's application of the G-TR methodology in conjunction with USNRC guidance for qualification of specific NRW-FPGA-based systems.
- Document the system specification.
- Document the results of FPGA logic development and verification and validation activities.
- Document the results of hardware qualification activities.
- Document the EPRI TR-107330 Compliance and Traceability Matrix (CTM).
- Provide the application guide.

2. Toshiba FPGA-Based I&C System Quality Assurance Process

2.1. Process and QA Overview

Toshiba's FPGA-based systems are jointly developed by two Toshiba organizations: the Nuclear Energy Systems & Services Division (NED), and Fuchu Complex. NED is responsible for the overall development project, as well as system design and nuclear quality assurance. Fuchu Complex is responsible for component design, manufacturing, testing, and commercial quality assurance. [[]]

NED works under its Quality Assurance (QA) Program, which was established in accordance with 10 CFR 50 Appendix B (Reference (1)). Fuchu Complex works under [[]] QA Program. Toshiba's lifecycle process formalizes the interaction between the two organizations for FPGA-based systems by integrating these different QA programs.

The process for developing a safety-related product begins when NED receives an order for a product. NED provides nuclear power plant system-level engineering, and generates design requirements included in a technical specification sent to Fuchu Complex. Fuchu Complex design engineers decompose the required plant interface inputs and outputs into a modular set of components, based on NED's technical specification. FPGA-based components are designed, documented, reviewed, tested, and manufactured by Fuchu Complex. Both NED and Fuchu Complex have their own work instructions, which provide directions for performing their work in accordance with their own QA programs. Appendix A of this topical report contains a brief summary of NED AS standards and Fuchu Complex Nuclear Instrumentation and Control Systems Department (NICSD) procedural standards used for the FPGA-based systems and components.

This approach is applied to develop specific FPGA-based I&C system applications. Toshiba intends to qualify specific nuclear power plant systems, such as the Power Range Neutron Monitoring (PRM) System. Toshiba will use the process defined in this topical report to implement each application, qualifying each in accordance with Section 1.4.3 of EPRI TR-107330 (Reference (20)).

[[

]]

The V&V activities are performed by both NED and Fuchu Complex. Fuchu Complex's scope and responsibility for V&V activities are specified in the NED procurement documents. NED controls and accepts Fuchu Complex's activities and work products into the NED 10 CFR 50 Appendix B process, in accordance with NED's procedures for procurement and commercial grade dedication. NED procurement documents establish additional conditions on specific aspects of Fuchu Complex work, [[

]] NED can accept the product [[

]]

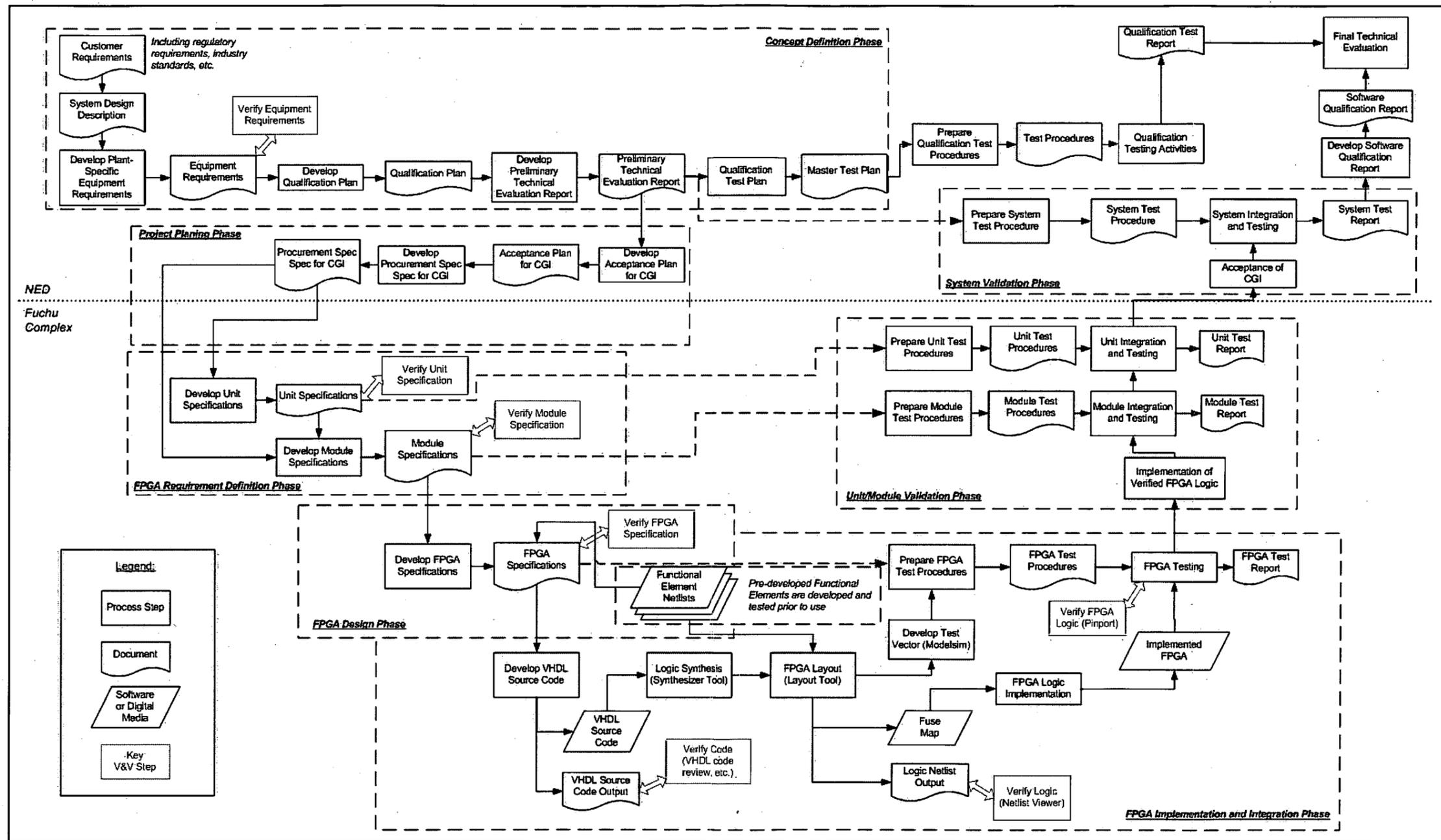


Figure 2-1. Toshiba FPGA-based System Development Process

2.2. Quality Assurance Programs

The Toshiba Power Systems Company has several established QA programs. These include ISO-9001 and 10 CFR 50 Appendix B. The 10 CFR 50, Appendix B QA program complies with American Society of Mechanical Engineers (ASME) Nuclear Quality Assurance (NQA)-1-1989 (Reference (3)) and USNRC Regulatory Guide 1.28-1985 (Reference (17)). The 10 CFR 50, Appendix B QA program also has a separate manual for work associated with the applicable sections of the ASME Boiler and Vessel Pressure Code.

Toshiba Corporation, Industrial and Power Systems & Services Company (IPS), IPS Nuclear Energy (IPSNE) Division established a QA Program complying with US nuclear safety regulations in October 2005. In April 2006, IPS was divided into three companies, one of which is Power Systems Company (PS). Toshiba PS is a manufacturer of heavy electrical apparatus. PS includes a nuclear business, known as the Power Systems Nuclear Energy (PSNE) division. After this reorganization, the IPSNE QA Program Description became the PSNE QA Program Description.

The work required to generate safety-related FPGA-based products for US nuclear power plants is performed by several organizations within Toshiba. These organizations are listed below and shown graphically in Figure 2-2.

- The nuclear portion of the Power Systems Company, which is referred to as PS Nuclear Energy (PSNE). PSNE has two units: the Nuclear Energy Systems and Services Division (NED) and the Nuclear Energy Equipment Manufacturing Department. NED is responsible for all PSNE activities except manufacturing. The Nuclear Energy Equipment Manufacturing Department is a manufacturer of nuclear reactor components.
- Fuchu Complex, which is one of Toshiba's factories, responsible for manufacturing electrical components. [[]]
- The Nuclear Instrumentation and Control Systems Department, which is a department of the Power Systems Products Segment of Fuchu Complex. NICSD designs, tests, and oversees manufacturing of components for safety-related systems for nuclear power plants. Other departments within the Power Systems Segment of Fuchu Complex perform the manufacturing.

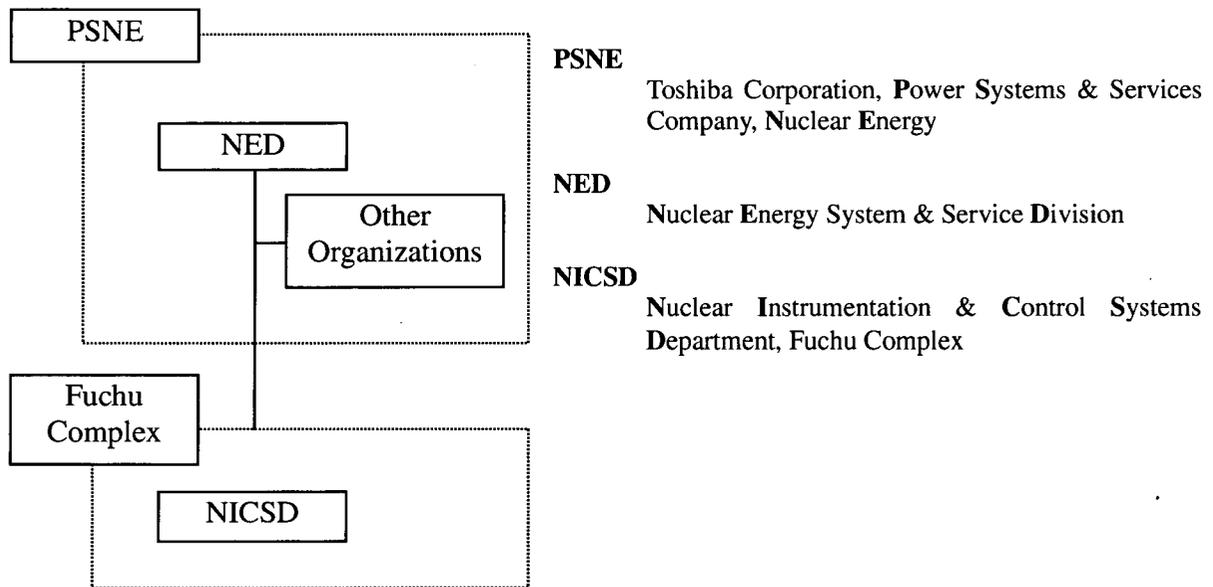


Figure 2-2. Toshiba Organizations for US Safety-Related FPGA-Based Products

The PSNE 10 CFR 50, Appendix B compliant QA Program Description establishes the control measures for performing activities affecting the safety-related functions of structures, systems, and components. The QA program description and PSNE regulations and procedures apply to all PSNE organizational units.

One of PSNE’s regulations and procedures is “Reporting Procedure for Defects and Noncompliance under USNRC 10 CFR 21.” This describes the procedure for ensuring compliance with the requirements of 10 CFR 21, “Reporting of Defects and Noncompliance” (Reference (2)).

Section 2.2.1 describes how the QA Program Description is in use at NED. Section 2.2.2 describes the major features of Fuchu Complex’s QA program related to this project. Section 2.3 of this topical report describes surveys and audits related to vendor procurements applicable to this topical report.

NED decided to use the Critical Digital Review (CDR) process to evaluate software processes used by NICSD and the key supplier for FPGA tools, Actel. Section 2.4 of this topical report describes the CDR process, and the results of CDRs performed at NICSD and Actel.

2.2.1. PSNE Quality Assurance Program Description

In October 2005, PSNE established its Nuclear Energy Quality Assurance Program Description (QAPD) (Reference (31)). The NED Quality Assurance Department, NQAD, is responsible for maintaining the PSNE QAPD.

The PSNE QAPD defines specific responsibilities and authority for control of design, documentation, procurement, processes, inspection, testing, nonconformance, corrective action, QA records, and audit. In addition, the PSNE QAPD defines requirements for inspection and audits.

The PSNE QAPD controls design and procurement. It also establishes the quality system document structure, which includes the following:

- NED standards, describing requirements for activities to be performed in accordance with the PSNE QAPD. These standards are identified as “AS” standards.
- Work Guides, which are established by each department within NED to implement the AS standards and PSNE QAPD requirements.

NED’s AS standards prescribe design control, procurement control, and test control measures, as well as the software design process and commercial grade dedication (CGD) process. Many of these AS standards are applied for the process documented in this topical report. Appendix A of this topical report includes a brief summary of AS standards used for the FPGA-based systems.

Of key importance, NED standard AS-200A001, “Engineering and Design Procedure” (Reference (33)), is used by NED engineers. This procedure defines the process for performing, and documenting design activities to be carried out to assure that applicable US regulatory requirements, design basis as defined in 10 CFR 50.2 and as specified in the license application, and ASME Code Section III requirements are correctly translated into the design output documents.

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

- The Plant Project Engineering Department (PPED), which is responsible for project management and document control for nuclear projects and related systems and components.
- The Sourcing Department, which is responsible for procurement of subcontracted services.
- The Control & Electrical Systems Design & Engineering Department (ICDD), which is responsible for system design and engineering of I&C products.

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

As mentioned in Section 2.1, NED and Fuchu Complex jointly develop FPGA-based I&C systems. Because they work under different QA programs, NED uses Fuchu Complex as the product manufacturer and controls Fuchu Complex work under the NED procurement control process. [[

]] The CGD process complies with EPRI NP-5652 (Reference (23)), which has been endorsed by the USNRC. [[

]]

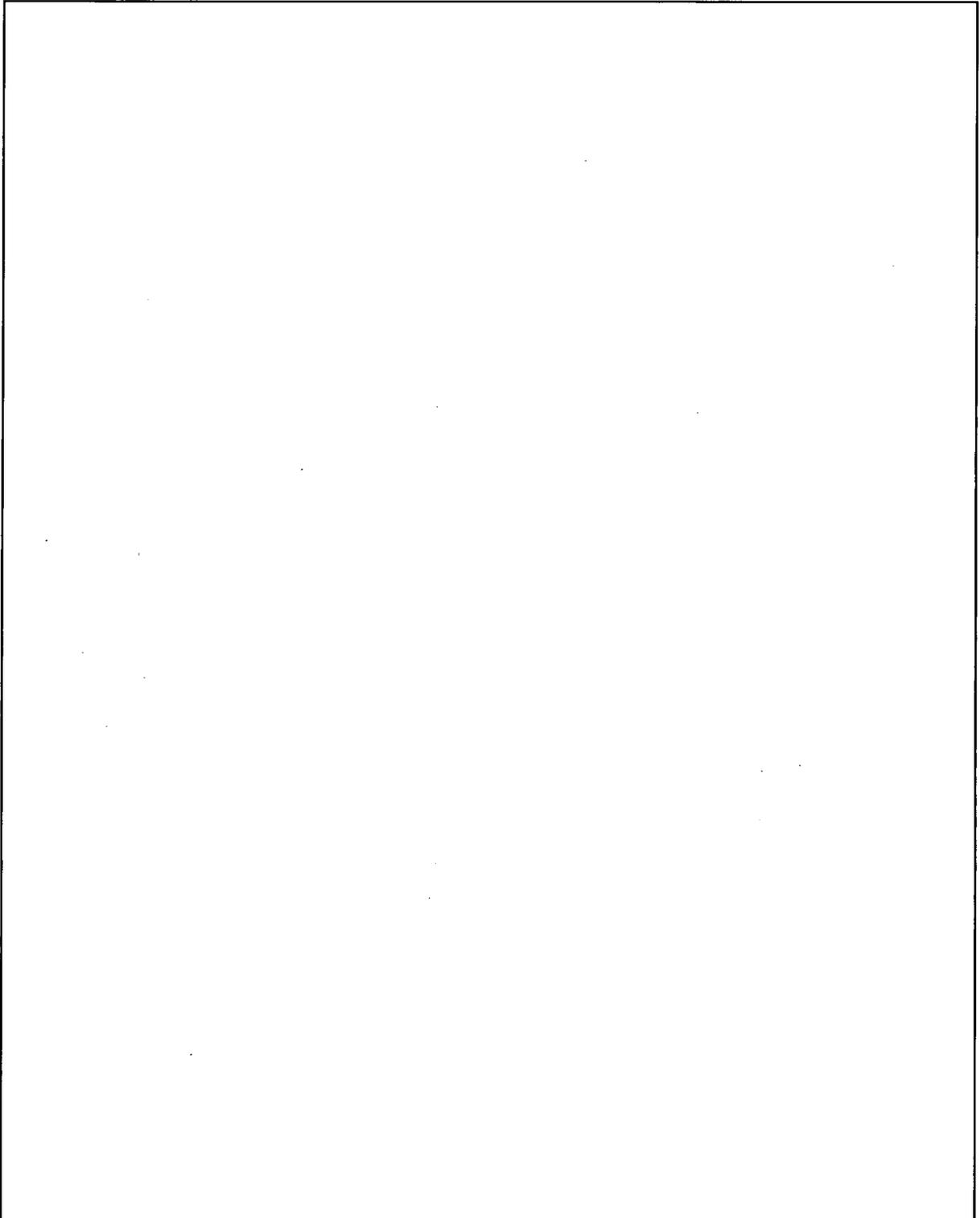


Figure 2-3. System Development Process

[[]] NED prepares an Equipment Requirement Specification (ERS) and a Qualification Plan. Following that, NED prepares a Preliminary Technical Evaluation Report to identify critical characteristics for the commercial grade items (CGI) and/or commercial grade services (CGS) to be procured. Then NED prepares an Acceptance Plan for the procurement, which identifies the critical characteristics, acceptance criteria, and methods of acceptance. Section 3.1 of this report provides a description of these documents. The acceptance methods identified in the Acceptance Plan are reflected in a Technical Specification and a QA Specification, which NED prepares as part of the Job Order to Fuchu Complex. The Technical Specification and the QA Specification identify extra requirements [[

]]

NED developed its commercial grade acceptance process based on the process described in EPRI TR-102260, Section 3, "Supplier Dedication Issues" (Reference (18)). NED Standard AS-200A110 (Reference (34)) defines NED's procedure for dedication of commercial grade items and services. This process includes the equipment qualification process.

The Toshiba FPGA-based I&C System Qualification Project follows the process outline for qualification defined in EPRI TR-107330, which requires the preparation of a Project Quality Assurance Plan (PQAP). NED refers to their PQAP as a Project Quality Assurance Manual (PQAM). NED creates a system-specific PQAM at the beginning of each system project. The PQAM defines the basic plan for implementing the QA requirements for qualification and product applications. The PQAM controls all project activities, including planning, designing, procurement, inspection, and testing performed by NED. NED has created a PQAM for the PRM qualification project, which will be used as a template for future projects.

2.2.2. Fuchu Complex QA Program

Fuchu Complex includes three segments. Each segment has its own quality assurance program. [[

]]

NICSD, Energy Control System Manufacturing Department, Power Systems Control Department, and Power Systems Quality Assurance Department belong to the Power Systems Segment of Fuchu Complex. These departments work under the QA program of the Power Systems Segment. The Fuchu Complex Procurement Department works for all segments at Fuchu Complex, using each segment's QA program; accordingly, for work done for the Power Systems Segment, the Procurement Department works under the Power Systems Segment QA program.

NICSD is the department at Fuchu Complex responsible for the design and implementation of

the FPGA logic and use of software tools for producing FPGAs.

The Power Systems Segment QA Manual is prepared and maintained by the Power Systems Segment Quality Assurance Department. The QA program defined by this manual includes various levels of standards, identified as A, B, C, and D standards. The A, B, and C numbered standards are common to the entire Power Systems Segment. Each department maintains its own set of D numbered standards for their own use to support its duties as required in the Power Systems Segment QA Manual.

NICSD has prepared several D numbered Procedural Standards to support the FPGA-based system design, development, and manufacturing. To satisfy all NED QA requirements for the FPGA-based systems, NICSD also revised several Procedural Standards. During each project, NED will verify that the NICSD procedural standards meet NED's QA requirements, and that the NICSD implementation of those standards satisfies the NED QA requirements. The NICSD procedural standards used for the FPGA-based systems and components are summarized in Appendix A.

2.3. Vendor Evaluations

Prospective vendors are surveyed and/or audited to ensure that the vendor will reliably provide products meeting Toshiba's requirements. This section describes the surveys and audits performed that are applicable to activities covered by this topical report.

Both NED and Fuchu Complex perform vendor qualification activities. NED's evaluations are performed in accordance with Chapter 8 of the PSNE QAPD and AS standard, "Procedure for Evaluation of Vendors," (AS-300A002) (Reference (43)), which covers planning, personnel qualification, survey team selection, implementation, maintenance of the qualification, and documentation of results. Key features of NED's vendor evaluation process include:

- Prospective vendors 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 auditors qualified in accordance with the AS standard "Auditor Qualification Procedure" (AS-300A013) (Reference (46)).
- A Survey Checklist is prepared and used.
- Survey results are documented in reports.
- Acceptable vendors are registered on NED's Qualified Vendors List (QVL).
- Qualified vendors are audited or evaluated annually, and surveyed every three years.

For commercial grade vendors, NED may perform a commercial grade survey where this acceptance method provides the means for NED to take credit for acceptable commercial controls that the vendor exercises on specific items/services. The commercial grade survey determines whether the critical characteristics that can be accepted by survey, as documented in

the commercial grade procurement acceptance plan, have been satisfied. Depending on the results of the commercial grade survey, NED may decide to place additional requirements for procurement in procurement documents when orders are placed with commercial vendors.

Fuchu Complex is the key vendor to NED for FPGA-based products. Actel is the supplier of FPGA chips and software tools for Fuchu Complex. The following subsections describe how NED and Fuchu Complex evaluate and control their vendors by survey and audit.

2.3.1. NED's Evaluation of Fuchu Complex

NED performed its first survey of Fuchu IP to evaluate the vendor's quality capability [[

]] the NED survey team recognized that the Fuchu IP documented quality system program is established and effectively implemented, except for some observations.

In addition, NED performed a survey of Fuchu IP on November 4, 2005 to cover critical characteristics [[]]. This survey identified an observation that NED determined would require placing additional requirements on Fuchu Complex for NED procurements. When preparing the technical specifications and the QA specifications for procurements from Fuchu Complex, NED adds these special requirements to the specifications.

After the survey was completed, reorganization within Toshiba merged Fuchu IP into Fuchu Complex. [[

]] NED performed a subsequent survey on Fuchu Complex following the reorganization. This subsequent survey, performed on May 10, 2006, confirmed that the reorganization did not have any adverse affect on quality of work at Fuchu Complex. [[

]]

Based on the results of these surveys, Fuchu Complex has been registered on NED's Qualified Vendor List (Reference (55)) since July 6, 2005 (at Rev.10) with nine conditions related to those observations.

[[

]] the NED QA Specification requires Fuchu Complex to provide measures for evaluation and selection of sub-tier suppliers, and document the results of these evaluations. The evaluations include providing and appropriately maintaining a list of approved sub-tier suppliers relevant to the FPGA-based systems. The current requirement is that components, equipment, material, modules, parts, subassemblies, or units of FPGA-based systems not be procured by Fuchu Complex from any sub-tier suppliers other than the listed sub-tier suppliers. NED confirms Fuchu Complex's vendor list and performance of the supplier during source verification.

By following this process, NED ensures that there is a reasonable assurance that sub-tier suppliers will be controlled effectively and appropriately by Fuchu Complex.

By procedure, NED will periodically review its qualified vendor list. As part of this procedure, NED will annually audit or evaluate Fuchu Complex, and perform a triennial survey.

2.3.2. Audit of Actel

At the time of the above survey, Actel was Toshiba's sole acceptable FPGA device and related tool supplier¹ for safety-related equipment. This status makes Actel a key supplier to Toshiba; hence, Fuchu Complex performed a QA audit of Actel, the supplier of the FPGA components, in accordance with the Fuchu Complex vendor audit process. This audit process will be used to support use of Actel equipment in future system implementations.

[[

¹ 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 vendors and select another FPGA vendor. While the process described in this topical report covers Actel parts and software tools, Toshiba expects to use this basic vendor 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 topical report, or at least a supplement to this topical report.

Toshiba also notes that process improvements may be made in the FPGA design and development process defined in this topical report, 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 topical report as a part of a utility submission of a safety system, as suggested by the USNRC.

]]

2.4. Critical Digital Review

A CDR is a technical review of a software development process. CDR is a tool that can be used in the vendor 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 uses this tool to control and enhance vendor processes related to FPGA logic development, therefore to ensure that the quality of FPGA logic meets a level sufficient for nuclear safety-related applications.

NED performs a CDR using the guidance provided by EPRI TR-107339 (Reference (21)) and EPRI TR-106439 (Reference (22)) for the qualification of specific applications. The USNRC has accepted EPRI TR-106439 as an acceptable means of assessing digital device quality for nuclear safety-related applications. The reviews performed used the process evaluation guidance in the USNRC Standard Review Plan, Chapter 7, Branch Technical Position (BTP) 7-14 (Reference (6)), and the sections on design integrity from the Institute of Electrical and Electronics Engineers (IEEE) Standard 7-4.3.2-1993 (Reference (24)), endorsed by RG 1.152 (Reference (8)). Future reviews will use the current IEEE standards and regulatory guides.

A CDR is performed by one or more qualified engineers. The member(s) are qualified by engineering experience and training recorded in their "Personnel Indoctrination, Training Plan and Evaluation Record," as defined in AS-100A008, "Procedure for Indoctrination and Training" (Reference (32)).

NED performs CDR to determine whether the processes at vendors or suppliers who provide software or software-like products are in accordance with the NED QA procedures. NED QA then periodically evaluates processes and procedures implemented by the vendor or supplier. If, during periodic evaluation, the NED QA personnel determine that changes have occurred at

the vendor that, based on the judgment of the NED auditors could create challenges to nuclear safety, then NED follows its normal QA practices for addressing concerns at the vendor. If resolving these concerns involves changes to software or processes, then the CDR report might be revised or a new CDR performed.

Since FPGA-based I&C systems are commercial products supplied by NICSD, NED used the CDR process to evaluate NICSD. [[

]] Accordingly, NED has also performed CDR of the supplier of these tools, the Actel Corporation.

The CDRs of NICSD and Actel focused on:

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

2.4.1. Critical Digital Review of NICSD

The scope of NED's CDR of NICSD included reviews of 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. The review consisted of interviews with key NICSD personnel representing the above disciplines, and technical reviews of design and development documentation, including internal design control procedures. This CDR addressed the issues relating to dependability, reliability, built-in quality, and design integrity of I&C products. The original CDR of NICSD focused on a specific system, PRM.

[[

]]

In general, the reviewers found the NICSD development process to be rigorous and robust, and the engineers to be of high caliber. The CDR reviewers concluded that the methods used for the FPGA-based PRM are suitable for use in producing safety-related devices for US nuclear utilities.

The CDR reviewers identified some issues or recommendations regarding the FPGA-based PRM system. Some issues were addressed during the CDR evaluation process at both NED and NICSD, by enhancing work instructions and by modifying the independence of staff performing review and test activities. NED addressed the remaining issues by adding additional requirements into each procurement specification for Fuchu Complex.

Other conclusions of the CDR of NICSD are as follows:

- The system architecture was designed for high reliability and dependability. The design includes features to detect and indicate plausible failure modes. Toshiba will use this design methodology for future products.
- The NICSD development process is rigorous and NICSD engineers implement the process properly. NED will evaluate any changes in the NICSD development process and staff to ensure that a process as good as that evaluated will continue.

- [[

]]

- [[

]]

2.4.2. Critical Digital Review of Actel

During the CDR at NICSD, the CDR reviewers 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 performed a CDR of the Actel toolset and Actel development practices, as well as the third-party tools provided with the toolset.

[[

]]

The CDR reviewers concluded that the programmed FPGAs generated by these tools are appropriate for safety-related use, provided that NED and Fuchu Complex continue to implement the processes evaluated in the earlier CDR of NICSD. The compensatory actions taken by NED provide an adequate level of assurance that the logic embedded in the FPGA performs the required functions, and that the processes minimize the possibility of design errors in the logic. Thus, the CDR reviewers concluded that the Actel tools, used with the Toshiba processes, are acceptable for use in transforming human-readable source code into digital logic

embedded into FPGAs.

[[

]]

3. System Description

3.1. General Description of System Development Cycle

Figure 2-1 shows the complete system development process. In addition, Figure 2-1 also shows the documentation to be prepared during the process described in this topical report. Section 2.1 of this topical report describes the process overview for the FPGA-based systems. Figure 2-3 shows the commercial grade acceptance process established by NED. This figure also identifies the documents to be prepared for this process.

As shown in Figure 2-1 and Figure 2-3, the following key documents are produced by NED during the system development cycle:

- Equipment Requirement Specification (ERS). The ERS represents the top-tier requirements document to specify the product. NED develops the ERS based on the system specification for an application for a type of nuclear power plant (e.g., BWR-5) and

the Vendor Package, which specifies the commercial product to be qualified for nuclear use. Section 3.3 of this topical report provides a detailed description of the ERS contents.

- Qualification Plan. The Qualification Plan describes the activities required for the dedication of the commercial grade item/service.
- Preliminary Technical Evaluation Report (PTER). The PTER is performed as an initial evaluation [[

]] The PTER also identifies additional requirements, qualification analyses, and testing. For FPGA-based systems, the PTER includes the requirements for the commercial grade procurement of the test system to be used by NED during qualification activities.

- Acceptance Plan. Based on the PTER, NED develops an acceptance plan [[

]]

- Technical Specification and QA Specification. Based on the PTER, NED develops a technical specification and a QA specification. The technical specification summarizes the applicable design requirements of the items/services included in the Job Order to Fuchu Complex. The QA specification identifies applicable quality assurance requirements [[
]] Therefore, these specifications describe all requirements to be met by the FPGA-based components provided by Fuchu Complex.
- Job Order. NED prepares a job order to procure items and services for FPGA-based systems from the Fuchu Complex. The procurement process requires NED to develop a technical specification and a QA specification. These specifications are prepared following the steps described in [[

]]

The technical specification included in the Job Order only includes the requirements that are imposed on Fuchu Complex. The process followed by Fuchu Complex and NED for the FPGA-based system design is described in Section 4.3 of this topical report. Section 3.3 of this topical report describes the documents NICS D prepares and uses during the process described in this topical report.

Based on the procurement documents, technical specification, and QA specification, Fuchu Complex designs, develops, tests, and manufactures the FPGA-based components. Then, NED accepts these items in accordance with [[

]]

[[

]]

3.2. General Description of System Architecture

The FPGA-based I&C systems described in this topical report are designed as replacements for the existing analog and CPU-based I&C systems in use in Japanese and US nuclear applications.

This section describes the system architecture for the FPGA-based systems, and the different components that constitute the system. Figure 3-1 shows the system architecture for the PRM system². This figure is used in this topical report to show an example of the different system components.

Figure 3-1 shows that Toshiba designs an FPGA-based system as a modular, rack-mounted system. FPGA-based systems are constituted of units, which are made from a combination of modules. A module, such as a Local Power Range Neutron Monitor (LPRM) module, is constructed of one or more printed circuit boards, which include the FPGAs. Finally, the FPGAs are built from logical blocks, which are referred to as Functional Elements (FEs). The following subsections describe in further detail the components in an FPGA-based system.

² The Power Range Neutron Monitoring System was built to demonstrate use of the process documented in this topical report. The FPGA-based PRM system uses the same detectors as the existing analog systems. The FPGA-based PRM system provides similar annunciators and trip outputs as the existing analog systems, with additional self-test and diagnostic capabilities also capable of driving annunciators. The FPGA-based PRM system provides the same 1E to non-1E isolation for the analog outputs to the recorders, indicators, and plant computer inputs that the existing analog systems provide.

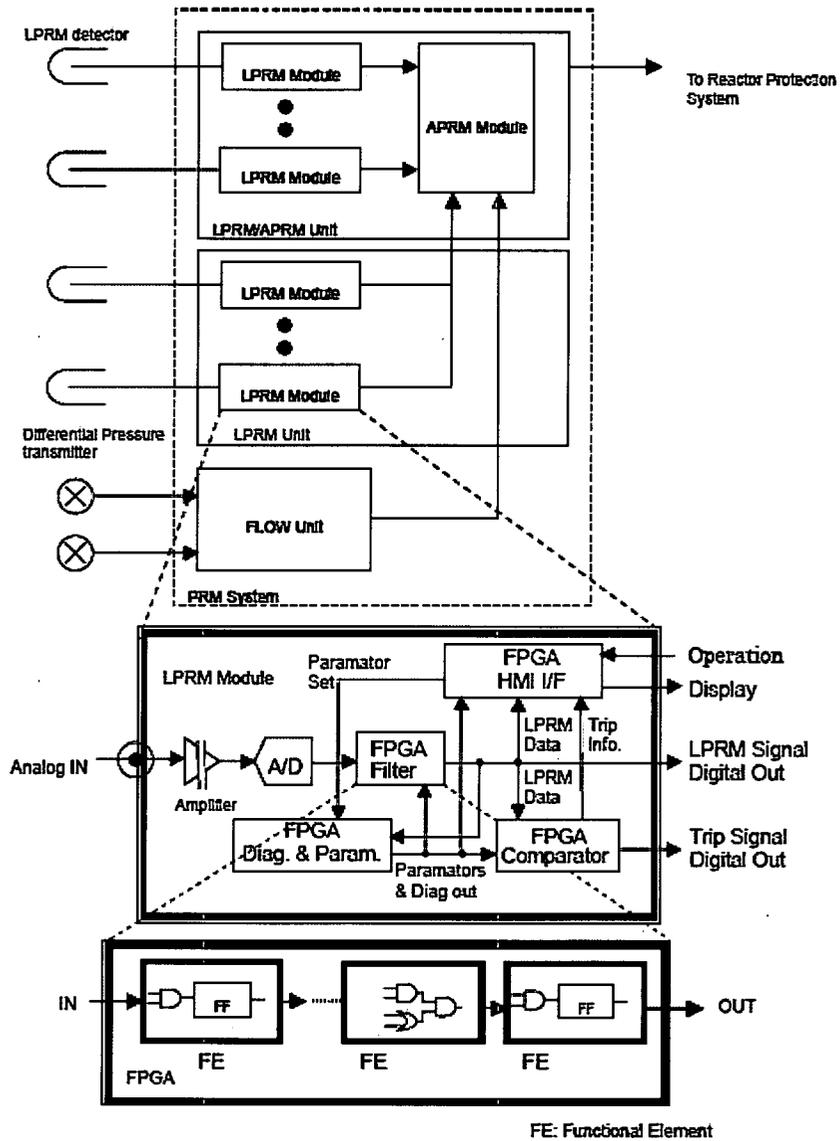


Figure 3-1. Architecture of the FPGA-based System (Example for PRM)

3.2.1. Units

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

3.2.2. Modules

Each module consists of one or more printed circuit boards and a front panel. Most modules require two printed circuit boards, including a small printed circuit board for the Human Machine Interface (HMI) on each module's front panel. The purpose of the front panel is to fix circuit boards to the unit and to provide mounting for the HMI. The front panel HMI provides a flat, front surface for discrete LEDs for status, numeric LEDs for values, and dedicated function pushbutton switches. The panel also provides captive screws, to ensure that the printed circuit boards remain in the unit and operable through seismic events. Analog and digital components, including the FPGA chips, are soldered to the printed circuit boards.

[[

]]

The module plugs into the unit backplane through connectors, using VersaModule Eurocard bus (VME) 96-pin Deutsches Institut für Normung (DIN) connectors. The printed circuit board runs through channels, guiding the assembly into a position where the connector will mate with the backplane.

Modules are considered the smallest replacement part level for a Toshiba system. There is no intent for an end user to replace anything at a level below the module level. Thus, FPGAs and other integrated circuits are soldered to the module's printed circuit boards.

3.2.3. FPGAs

An FPGA is a type of logic chip that can be programmed. The FPGA incorporates thousands of logic cells linked by one-time programmable connections that logically interconnect cells to meet different function requirements. In addition to logic cells, other programmable elements

of an FPGA are (1) I/O blocks, which serve as the interface between internal signal lines and the chip's external pins, and (2) interconnects, which route I/O signals to appropriate destinations. An FPGA can only implement digital logic.

Figure 3-1 illustrates how a module contains electronics and one or more FPGAs that implement logic elements. Discrete logic elements are captured in FEs, as shown at the bottom of Figure 3-1, which are analogous to reusable software function blocks. To create an FPGA circuit, NICSD uses combinations of verified FEs. The FEs are connected within the FPGA by logic paths, linked with antifuses.

3.2.4. Functional Elements

A Functional Element is defined as the minimum logical functional element in an FPGA.

[[

]]

3.3. Establishing System Functional and Design Requirements

Figure 2-1 in Section 2.1 of this topical report provides an overview of the process used to develop the system, and the relationship between the process steps and the documents they produce. Figure 3-2 shows the design specification document flow.

As described in Section 3.1, the top-tier requirements document is the Equipment Requirement Specification, which specifies the system based on the following sources:

- EPRI TR-107330 (Reference (20))
- System Specification
- Vendor Packages

For the PRM system, the system specification was created based on the system specification for Japanese plants, IEEE Standard 603-1991 (Reference (25)) and IEEE Standard 7-4.3.2-1993 (Reference (24)). Currently, the latest revision of IEEE Standard 7-4.3.2 is 2003. So, NED compared the 1993 and 2003 versions against the NED standards and concluded that the differences do not affect the NED software lifecycle. For future systems, Toshiba will use current RGs and endorsed IEEE standards.

The ERS specifies applicable regulations, codes and standards, and requirements for design, material, fabrication, inspection and test, packing, shipping, and transportation in accordance with AS standard AS-200A116, "Preparation Procedure for Equipment Requirement Specification" (Reference (37)).

The ERS also specifies the following design requirements:

- Functional requirements of the equipment to implement the system functions.
- Hardware requirements including unit I/O, module configuration of each unit and functional requirements for each module type.
- Software requirements (how software QA requirements are to be addressed for FPGA logic development).
- Setpoint accuracy.
- Availability/reliability requirements.
- Environmental condition to be withstood in accordance with EPRI TR-107330.

In addition to the technical information in the ERS, NED prepares an Instrumentation Electrical Diagram (IED) and an Interlock Block Diagram (IBD). The IED specifies the configuration of the control or instrumentation system and the function of the system. The IBD describes the control functions by representing electrical signal logic or control logic.

The ERS is sent to NICSD as an attachment to the Job Order. NICSD confirms that the ERS contains adequate definition of the functions, components and interfaces for the units, modules, and FPGAs. Then, NICSD develops unit design specifications that provide a description and define the requirements for the FPGA-based units in accordance with the ERS.

The unit design specification specifies the following:

- Unit functional requirements.
- Performance requirements (including response times).
- Power supply.
- Input/output signals.
- Interface/interaction with other units.
- Configuration of FPGA-based modules used in the unit.
- Sufficient criteria to support final acceptance testing of the unit.

The NICSD designer then determines module-level requirements and prepares module design specifications. Requirements and design activities for modules are primarily defined by the unit design specification. Module design specifications address the following:

- Module functional requirements.
- Module performance requirements (e.g., accuracy, response time, etc.).
- The purpose and application of the FPGA chips in the module and configuration of FPGAs within the module (i.e., internal logic).
- Power supply.
- Input and output signals and their characteristics.
- Internal device logic, including (as applicable) textual descriptions, truth tables, state tables, flow charts, pseudo code such as Hardware Description Language (HDL), VHDL (if it is appropriate and expedient) or any means suitable to specify the detailed requirements.
- Detailed timing requirements.
- External interfaces with hardware, other FPGA devices, and other software.
- Sufficient criteria to support testing of the module.

[[

]]

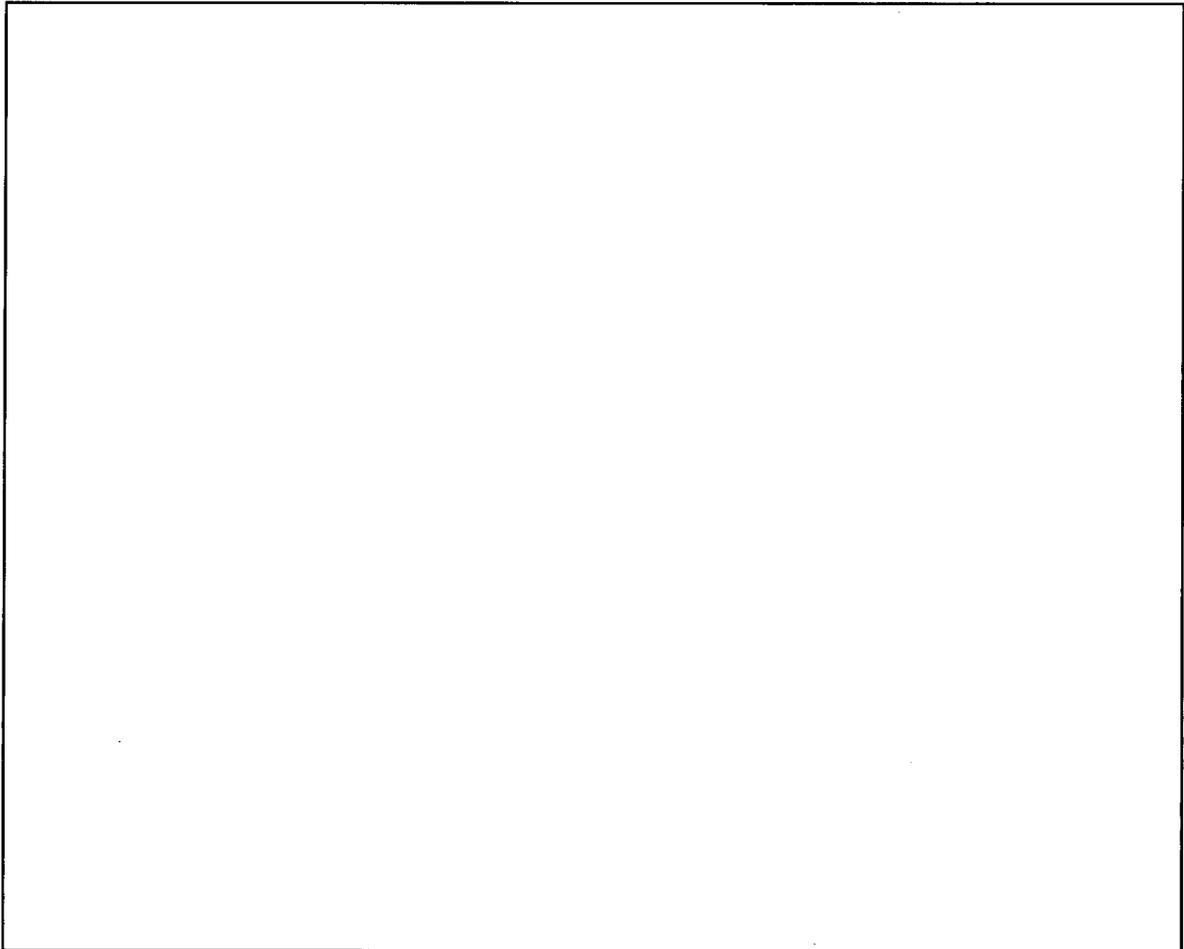


Figure 3-2. Design Specification Document Flow

3.4. NRW-FPGA Features

Toshiba has selected Actel FPGAs models A54SX72A and A54SX32A for use in its FPGA-based safety-related I&C systems. The FPGAs are one-time programmable devices with antifuse³ technology. The FPGA is designed to implement digital logic, absorbing many

³ In contrast to normal fuses in most integrated circuits which use programming power to break fusible links and create open circuits, antifuse technology uses programming power to break through an insulating layer and create a conductive via between two paths. A benefit of the Actel technology is that once programmed, the FPGA logic cannot be changed using standard programming equipment.

discrete integrated circuit packages into a single, complex device. These Actel FPGA models can only implement digital logic. Therefore, all analog processing and conversion between analog and digital representations occurs in devices attached to the FPGA.

The advantages of an FPGA platform are that the logic design is rigorous, simple (compared to computer-based systems), deterministic, and verifiable. FPGAs provide stable technology to minimize the risk of technological obsolescence. Toshiba engineers design FPGA-based I&C systems with the intent of creating an accurate, stable, safe, reliable, long-term maintainable system.

Design and programming FPGAs can be complex, requiring appropriate software tools. The design tools are specific for each FPGA vendor and each integrated circuit technology used in the FPGAs. Depending on the integrated FPGA and software tool vendor, software to program FPGAs varies in content and value-added features such as compilation and editing tools.

[[

]]

Appendix B of this topical report describes the Actel FPGA device, its architecture, and software tools used by Toshiba to program the FPGA logic. Additional information on the FPGA is contained in Actel's Data Sheet (Reference (60)).

4. FPGA Logic Development Lifecycle

[[

]]

Table 4-1. [[]]FPGA Processes

[[
]]

[[]]

[[

]]

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 others' 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. Without the documentation, Toshiba would not be able to remove design errors during the design process, and would have to postpone design error removal until system integration, when error removal would be much more costly.

4.1. Qualification Approach and Criteria

Ultimately, the basis for the qualification of Toshiba Corporation FPGA-based I&C systems is the USNRC Commission Standard Review Plan (SRP), provided in Nuclear Regulation (NUREG)-0800, Chapter 7, "Instrumentation and Controls" (Reference (6)). The approach used to demonstrate compliance with the requirements of the SRP is based on the guidance provided in EPRI TR-107330 (Reference (20)) and EPRI TR-106439 (Reference (22)).

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.

4.1.1. Standard Review Plan and Regulatory Guide

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 (6)), "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems."
- BTP 7-18, (Reference (7)), "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 (RG) 1.152 Rev. 2 (Reference (8)) endorsing IEEE Standard 7-4.3.2-2003 “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generation Stations,” (Reference (24a)).
- USNRC Regulatory Guide (RG) 1.153 Rev. 1 (Reference (9)) endorsing IEEE Standard 603-1991 “IEEE Standard for Safety Systems for Nuclear Power Generating Stations” (Reference (25)).

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

- Reg. Guide 1.168 “Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” (Reference (10)).
- Reg. Guide 1.169 “Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” (Reference (11)).
- Reg. Guide 1.170 “Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” (Reference (12)).
- Reg. Guide 1.171 “Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” (Reference (13)).
- Reg. Guide 1.172 “Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” (Reference (14)).
- Reg. Guide 1.173 “Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” (Reference (15)).
- Reg. Guide 1.180 “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety Related Instrumentation and Control Systems,” (Reference (16)).

Regulatory Guide 1.152 Rev. 2 states that conformance with the requirements of IEEE Standard 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 with respect to high functional reliability and design requirements for computers used in safety systems of nuclear power plants.

IEEE Standard 7-4.3.2-2003 requires the performance of Verification and Validation in accordance with IEEE Standard 1012-1998 (Reference (26)) for the highest software integrity level (level 4).

The requirements specified in Regulatory Guide 1.168 Revision 1 and IEEE Standard 1012-1998 provide an approach that is acceptable to the USNRC staff for meeting the requirements of 10 CFR 50 and the guidance given in Regulatory Guide 1.152, “Criteria for

Digital Computers in Safety Systems of Nuclear Power Plants.” USNRC Regulatory Guide 1.168 endorses and provides guidance for use of IEEE Standard 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.

NED Procedures AS-200A128 through AS-200A132 (References (38) through (42)) describe the specific tasks and responsibilities to be performed by NED for the typical software lifecycle in accordance with Regulatory Guide 1.152 , IEEE Standard 7-4.3.2, Regulatory Guide 1.168, and IEEE Standard 1012-1998 .

4.1.2. IEEE Standard 7-4.3.2

IEEE Standard 7-4.3.2-2003 (Reference (24a)) primarily concerns development of new computer systems and provides requirements for a complete system lifecycle. Section 5.4.2 of this standard recognizes the need to qualify existing commercial computers. This standard does not go into any detail on the acceptance of pre-developed software, although the standard states that, after acceptance, future changes shall follow the IEEE Standard 7-4.3.2-2003 requirements.

The principal thrust of IEEE Standard 7-4.3.2-2003 is to address requirements for sufficient design integrity. This is discussed in section 5.5 of the standard. The NRW-FPGA-based I&C products are evaluated to the design integrity requirements in this IEEE Standard.

The NED software lifecycle was first established to meet IEEE Standard 7-4.3.2-1993 (Reference (24)) requirements. The NED standards do not directly refer to the 1993 version. Currently the USNRC endorses the 2003 version through Regulatory Guide 1.152 Rev. 2, issued January 2006. NED compared the 1993 and 2003 versions against the NED standards and concluded that the differences do not affect the NED software lifecycle.

NED performed the CDRs of Actel and NICSD using the 1993 version of this IEEE Standard. NED concluded that the changes between the 1993 and 2003 versions have no significant impacts on the results of the CDRs that are not already incorporated into the digital logic lifecycle process and this topical report.

4.1.3. BTP 7-14 and BTP 7-18

The attributes provided in BTP 7-14 and BTP 7-18 are means of evaluating the concerns associated with digital I&C systems. As expressed in SRP Appendix 7.0A, the use of digital I&C systems presents the concern that minor errors in design and implementation can cause digital devices to exhibit unexpected behavior. To minimize this potential problem the design qualification for digital systems needs to focus on a high quality development process that incorporates disciplined specification and implementation of design requirements. Potential common-mode failures caused by software errors are also a concern. One of the protection

means against common-mode failures is also accomplished by an emphasis on the quality process.

Section 4.4 of this topical report describes the V&V process and software tools used by Toshiba to address the acceptance criteria of BTP 7-14.

The following section, 4.1.4, describes the qualification process used by Toshiba to address the qualification expectations of BTP 7-18.

4.1.4. EPRI TR-107330

The generic qualification program of FPGA-based systems will be performed using the guidance of EPRI TR-107330 "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants." Even though the Toshiba systems are not PLC-based, these safety-related systems are typically installed in the Main Control Room. Therefore, EPRI TR-107330 is considered as adequate to be applied for the general qualification program.

The generic qualification approach described in EPRI TR-107330 includes both hardware qualification and software qualification. The NRW-FPGA-based systems do not use application software. However, for FPGA-based systems, the software qualification is performed using a modified software process, including Verification and Validation for the FPGA logic. Section 5 of this topical report describes Toshiba's hardware qualification process and Section 4.2 describes FPGA logic lifecycle.

Toshiba will prepare a Requirements Traceability Matrix (RTM) to identify EPRI TR-107330 requirements, and disposition each of these requirements as being applicable or not applicable to the FPGA-based system qualification effort. In particular, a basis will be stated for any exceptions taken to the requirements of TR-107330.

In addition, EPRI TR-107330, section 8.7 lists the minimum set of documents that are needed to support software verification and validation and the related software quality processes. This list is based on NUREG/CR-6421 (Reference (5)), which BTP 7-18 describes as an acceptable process for qualifying existing software, and ASME NQA-1-1994. The minimum set of documents is:

[[

•

]]

4.1.5. IEEE Standard 1012

Toshiba uses the IEEE Standard 1012-1998 definition of independence from the Informative Annex C, "Definition of Independent Verification and Validation (IV&V)," to define and establish requirements for independence for the development of NRW-FPGA-based systems.

The IEEE Standard 1012-1998 definition notes that there are three parameters which define the level of independence. These parameters are technical, managerial, and financial independence.

Technical independence requires the IV&V effort to use engineers who are not involved in any development activities. Appendix B of the IEEE standard also further restricts independence by stating that engineers who set technical direction for the staff actually performing the design cannot be considered independent. The technically independent engineer must formulate his own understanding of the problem and how the proposed system attacks and resolves the problem.

Managerial independence requires that management responsibilities for the IV&V effort be separated from the management responsibilities for the design activities. The management of the IV&V effort is also independent in their evaluations of the system, using techniques, methods, resources, and schedules of their own devising. This eliminates possibilities of the design group failing to report unresolved issues and avoids undue direct or indirect pressure or influences on the IV&V staff by the design staff. This independence is not required in 10 CFR 50 Appendix B.

Financial independence requires that control of the IV&V budget be in an organization separated from the design organization, to ensure that overruns in design budgets do not result in diversion of funds from the IV&V budget. This independence is not required in 10 CFR 50 Appendix B.

Four commonly used levels of independence are defined in the IEEE standard. These four levels, listed in decreasing independence, are Classical, Modified, Internal, and Embedded. Toshiba concurs with the IEEE Standard 1012-1998 that neither Internal nor Embedded are appropriate for safety-critical systems.

The IEEE Standard 1012-1998 notes that Classical Independence requires an IV&V organization separate from the design organization. There is a requirement that the IV&V organization work tightly with the design organization, to ensure good communication of findings from the IV&V organization to the design organization and rapid resolution of those findings into design work products. Classical IV&V is typically performed by a separate vendor. The IEEE standard notes that this level of independence is appropriate for systems with significant safety consequences, leading to the loss of life, loss of mission, or significant

social or financial loss associated with Software Integrity Level (SIL) 4 systems. The USNRC has stated that they expect safety systems to be built to SIL 4 standards.

The IEEE Standard 1012-1998 notes that Modified Independence allows an organization to separate the IV&V from the design tasks within that organization. The IEEE standard notes that there is some degree of managerial independence that is lost by this arrangement. The standard notes that it is possible to retain financial and technical independence within this arrangement. The IEEE standard notes that this level of independence is appropriate for systems that serve an important mission and purpose, normally associated with SIL 3 criteria.

Toshiba notes that none of the active instrumentation and controls in a nuclear power plant performs functions that are SIL 3 or SIL 4. The fuel cladding, the reactor vessel, and the containment dome provide the primary protection against harm to the public. The safety-related instrumentation and controls protect those boundaries, with multiple lines of defense-in-depth to protect each boundary. Thus, the safety-related instrumentation and controls do not require processing to a high SIL rating. However, the regulator expects, and Toshiba concurs, that highly safe, reliable, and available equipment requires use of a process with sufficient independence to detect and cause the correction of any design errors in the instrumentation and controls. Toshiba believes that the level of independence provided, described below, is sufficient.

As was mentioned in Section 2.2 of this TR, two separate entities are involved in the design and development of the NRW-FPGA-based systems. NED, in the nuclear portion of the Power Systems Company, provides system engineering functions. NICSD, in the Power Systems Products Segment of Fuchu Complex, designs and implements the equipment that comprises the systems. NED and NICSD are as separated as individual vendors would be in smaller companies. NED writes job orders to NICSD to get work done. As parts of the Toshiba Corporation, each works well together, and both have worked on collaborative nuclear systems development for many decades.

Figure 2-1 shows the logic lifecycle process that is applied to developing NRW-FPGA-based products, and the documents, reviews, analyses, tests, code, and other work products that result. The design products and the reviewers for each level are discussed below.

NED Standard AS-200A130 (Reference (40)) describes the responsibility for NED's V&V team and design group for the FPGA logic lifecycle. AS-200A130 states that V&V documents are created by the NED design group and reviewed by the NED V&V team, which has financial, managerial, and technical independence from the design group. The NED V&V personnel are assigned by a different manager than the manager responsible for design activities. In addition, the approver of documents prepared for any V&V activities is in a managerial position independent from the NED design group.

NED produces the initial system requirements documents. These documents are reviewed internally in NED, under the PSNE 10 CFR 50 Appendix B QA program. As part of the

process, NICSD also reviews these documents and provides comments back to NED for resolution. [[

]] Toshiba

concludes that this process meets the regulatory expectations.

The Unit, Module, and FPGA design specifications and the test procedures are created by NICSD design engineers. These documents are prepared by NICSD engineers working for one manager. The documents are reviewed by an independent set of NICSD engineers working for a different manager, with a different budget. These documents are also supplied to NED for additional review and acceptance. While the NICSD review exhibits only Modified Independence, Toshiba considers that the NED review provides Classical Independence. [[

]]

The Preliminary Hazard Analysis (PHA) reports, the system validation test plan, and system validation test procedures are created by NED design engineers. These documents are reviewed by an independent reviewer from the NED V&V organization, which is from a different group outside of the NED Design Group, with separate cost, schedule, and resources.

4.1.6. EPRI TR-106439

Table 4-2 summarizes the critical characteristics applicable to the digital aspects of the FPGA-based systems and components being evaluated for safety-related applications. Table 4-2 in this report is based on Tables 4-1 and 4-2 of EPRI TR-106439 (Reference (22)). Table 4-2 in this report also describes the acceptance criteria and the methods used to verify compliance with the criteria considered for the digital aspects of the Toshiba FPGA-based systems and components. The criteria in Table 4-2 in this report were selected based on guidance from the USNRC Standard Review Plan, associated Branch Technical Positions, IEEE Standard 7-4.3.2-1993 (Reference (24)), EPRI TR-107339 (Reference (21)) on qualification of software for safety-related use, and USNRC NUREG/CR-6421 (Reference (5)). These critical characteristics are evaluated by several methods, including critical digital review, commercial grade survey, source verification, verification and validation, and testing.

Table 4-2. Critical Characteristics for Digital Systems

[[
	•	
]]

[[
]]

[[
]]

Specific critical characteristics relating to performance, hardware, and physical characteristics of FPGA-based systems and components are evaluated below.

Process Controls and Software Quality Assurance

- [[

-

]]

Configuration Control

- [[

]]

Problem Reporting

- [[

]]

Reliability and Dependability

- [[

-

]]

Quality of Design

[[

•

]]

Failure Management and Diagnostics

[[

•

]]

4.1.7. Cyber Security

[[

4.2. Overview of FPGA Logic Lifecycle

NED Procedures AS-200A128 through AS-200A132 (References (38) through (42)) describe the specific tasks and responsibilities to be performed by NED for the typical software lifecycle, as applied to FPGA-based products, in accordance with Reg. Guide 1.152 and IEEE Standard 1012-1998. Figure 2-1 shows the system development cycle for the FPGA-based systems. Control and Electrical Systems Design & Engineering Department (ICDD) Procedure P-101 (Reference (54)) provides more detailed description about the FPGA-based system lifecycle activities, and defines the division of responsibility between NED and NICSD.

The following lifecycle activities are necessary to implement the process described in this topical report. These processes run through the system development cycle, as shown in Figures 4-1 and 4-2. These six activities are as follows:

- System development. Design and development activities are performed by the NED Design Group and consist of identifying and specifying system and software (i.e., digital logic) requirements, creating and implementing the system which satisfies those requirements, and preparation of system test procedures to ensure that the system meets its requirements. NED procedure AS-200A129, "Digital System Development Procedure," is used in performing development tasks.
- Verification and Validation (V&V). Digital system verification and validation includes reviews performed on the results of each development phase to ensure that the phase was completed appropriately and correctly. Digital system verification and validation is performed on the final product of the code in the Implementation and Integration Phase. Validation is used to ensure that the final product satisfies user requirements. Verification and validation are performed as defined in test procedures, which include a description of how adherence to each requirement will be demonstrated. NED procedure AS-200A130, "Digital System Verification and Validation Procedure," (Reference (40)) is used to implement these V&V tasks. V&V reports (VVRs) are prepared for each phase; in addition, a project-specific V&V Plan (VVP) is established and implemented in accordance with the procedure. The V&V reports are used to prepare the Software Quality Assurance Report.
- Quality Assurance. As stated in P-101, for a specific FPGA-based I&C system or safety-related qualification activities for such system, NED develops a project specific Software Quality Assurance Plan (SQAP) in accordance with NED procedures AS-200A128, AS-200A129, AS-200A130, AS-200A131 and AS-200A132.
- Management. Normal management activities control schedule, budget, and resources. Because this is a nuclear safety-related process, quality concerns override schedule and budget considerations.

- Digital system configuration management (CM). Configuration management provides the capability of reproducing, to the extent necessary, the system environment and system design artifacts required for modification and further system development. NED procedure AS-200A131, "Digital System Configuration Management Procedure," is used to implement the digital system configuration management tasks.
- Digital system safety and hazards analysis. Safety and hazards analyses are used to determine if the digital system lifecycle activities are established in a manner that minimizes risk of faults, failures, and design errors. Hazard analyses are conducted during each phase of digital system development to ensure that potential failures are identified, evaluated, and resolved as the design evolves and that verification and validation activities are adequate and sufficient to ensure that the identified hazards are resolved or mitigated appropriately. Figure 4-1 shows the relationship between the lifecycle phases and the hazard analysis prepared for each phase. NED procedure AS-200A132, "Digital System Safety and Hazards Analysis Procedure," is to be used to implement the system hazard analyses. To reduce the risk of common mode failure, Toshiba has implemented a structured process that detects and eliminates errors. Toshiba performs hazards analysis of the system design, module design, and FPGA design at a sufficiently detailed level to find the errors that could result in common mode failures. In addition, the design itself is evaluated to ensure good engineering practices are incorporated and the design is complete, to further eliminate errors. The types of hazards considered include those common to software, as well as hardware issues such as signal propagation and timing.

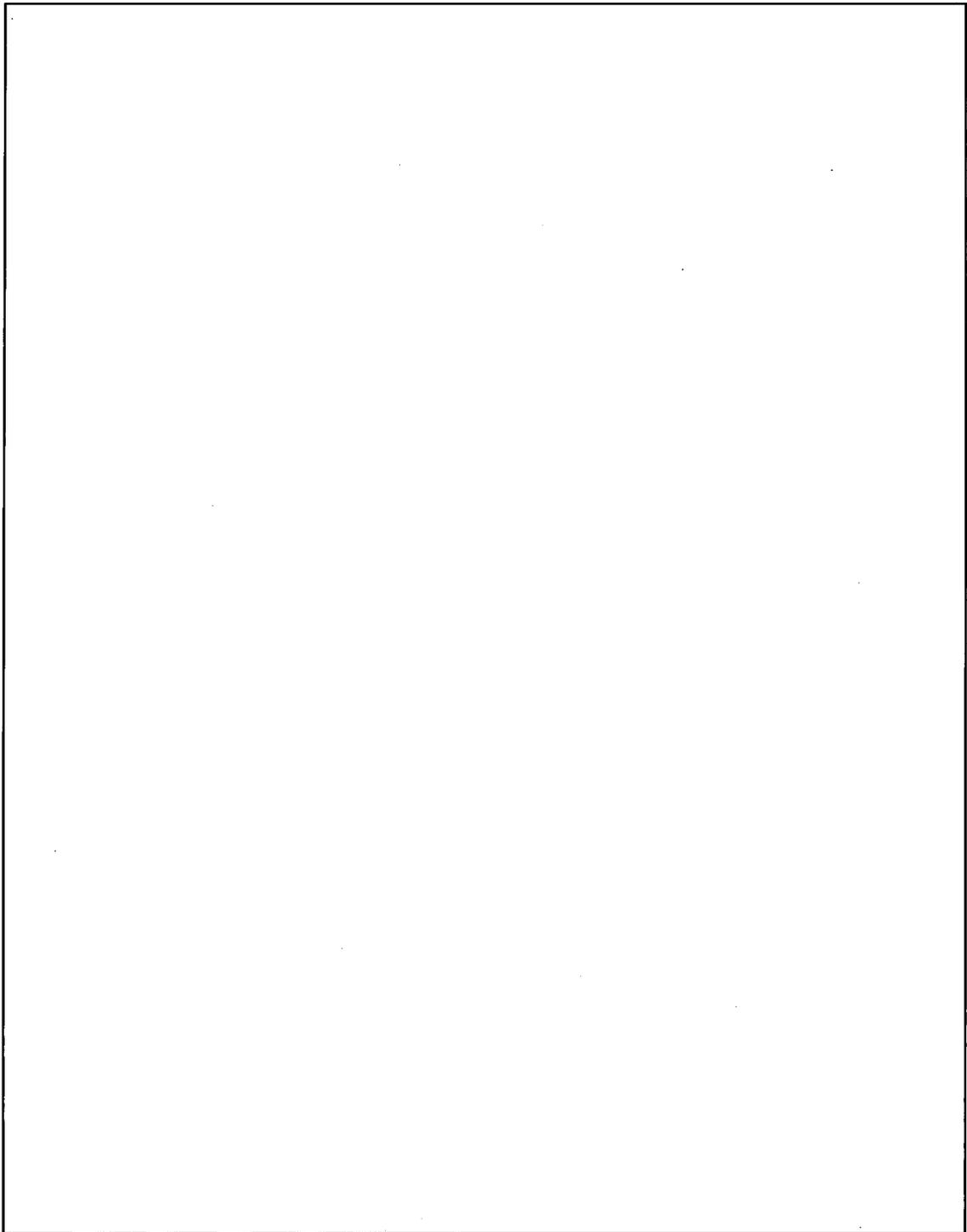


Figure 4-1. Software Qualification Activities

The activities above are mapped in to the lifecycle phases shown in Figure 4-2 and explained below. The lifecycle phases are defined in procedure P-101 and supported by AS standards. Figure 4-2 shows a simplified diagram of the process flow through the lifecycle phases.

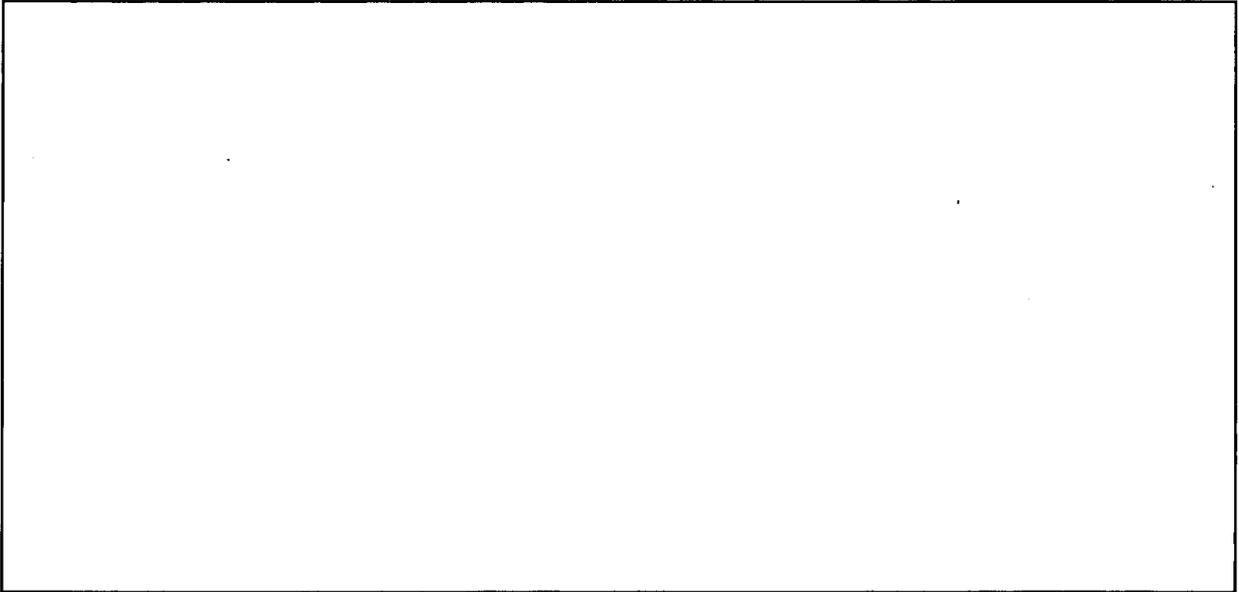


Figure 4-2. Lifecycle Process for Development and Procurement of FPGA-based Systems from NICSD

[[

]]

4.3. System Design and Integration Process

[[

]]

4.3.1. Developing FPGAs

[[

]]

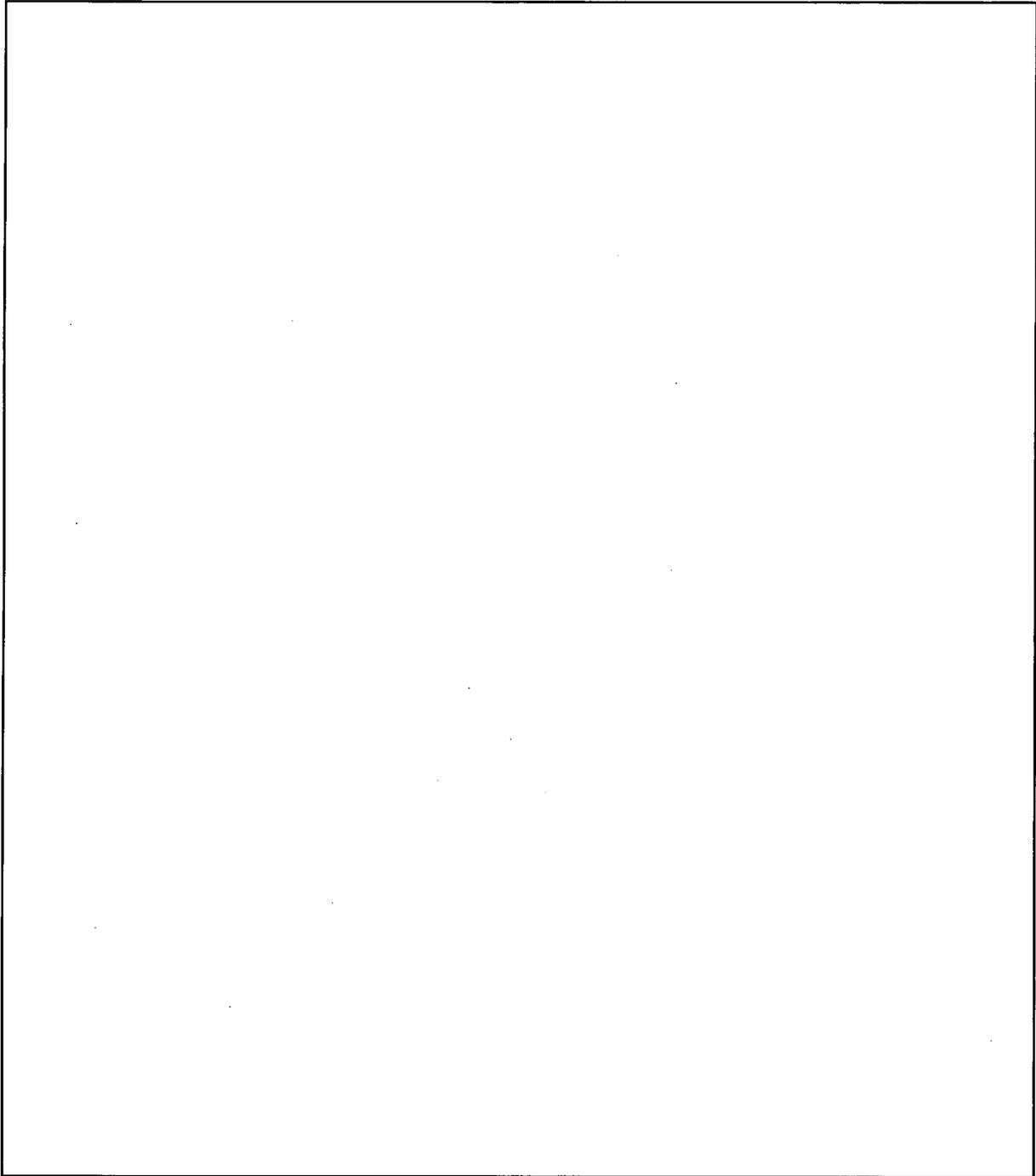


Figure 4-3. NICSD FPGA Implementation Process

[[

[[

]]

]]

4.3.2. Integrating a Module

[[

]]

4.3.3. Integrating a Unit

[[

]]

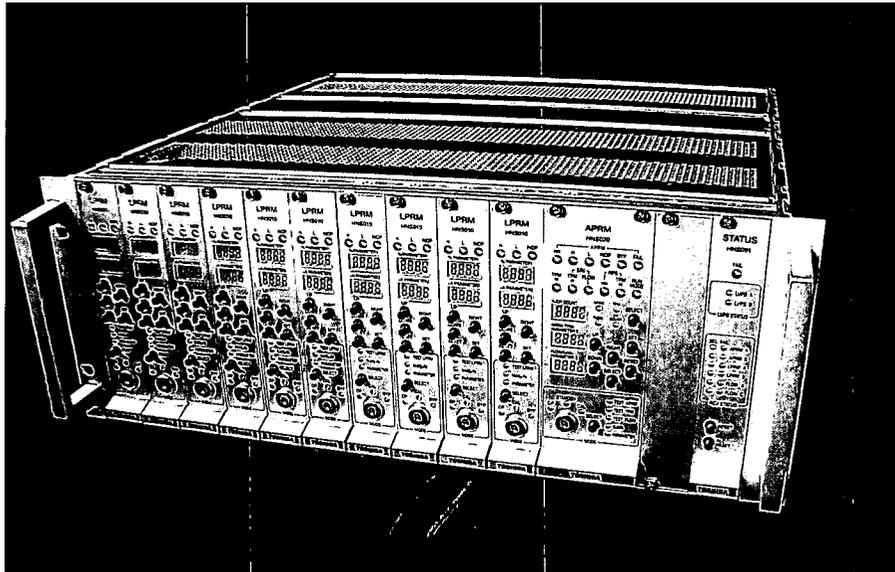


Figure 4-4. LPRM/APRM Unit

4.3.4. Integrating a System

[[

]]

4.3.5. FPGA Design Principles

[[

]]

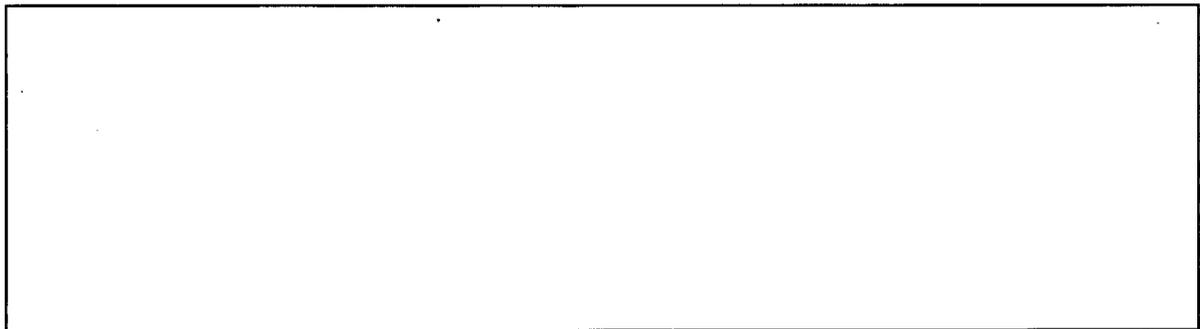


Figure 4-5a. Timing Delay

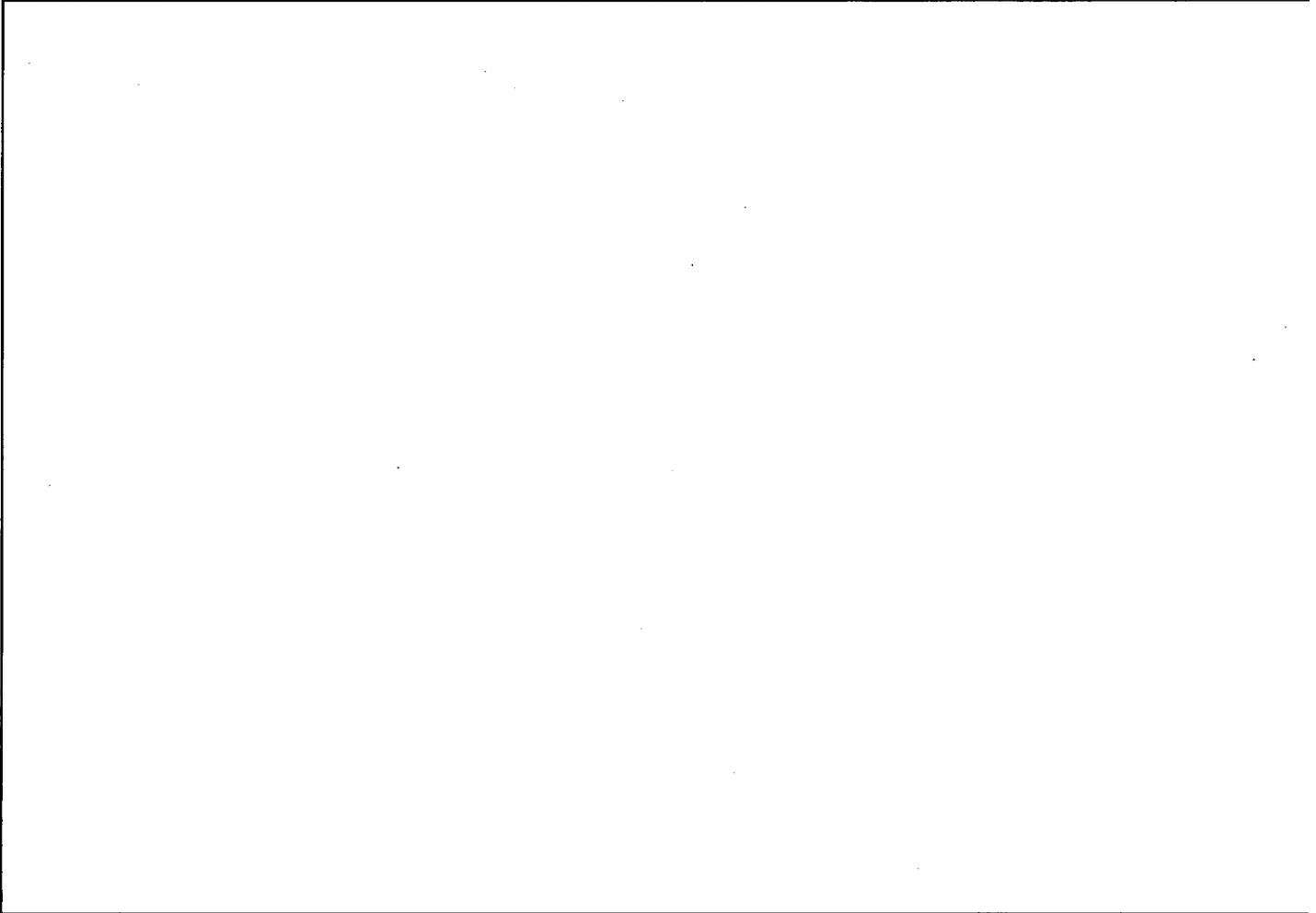


Figure 4-5b. Propagation Delay in NRW-FPGA

[[

]]

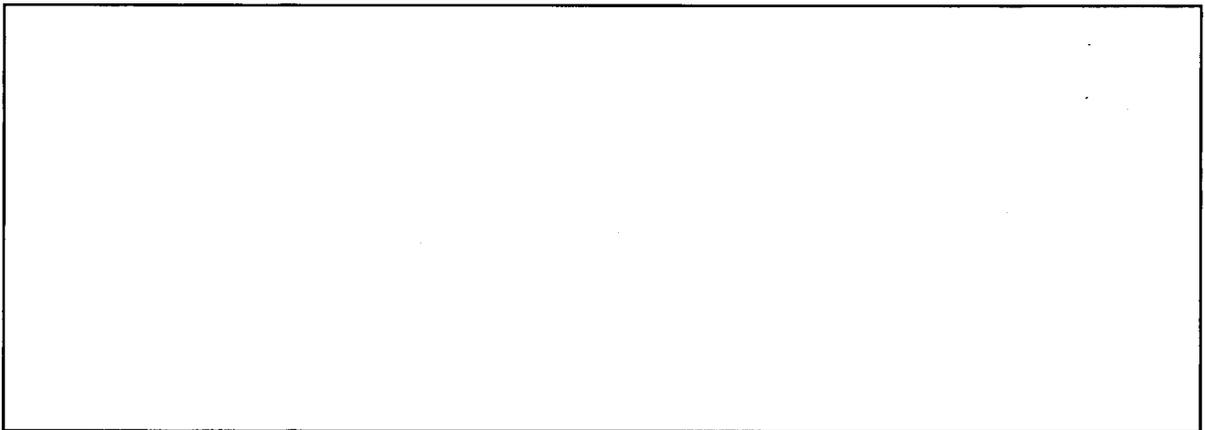


Figure 4-6. [[]]

[[

]]

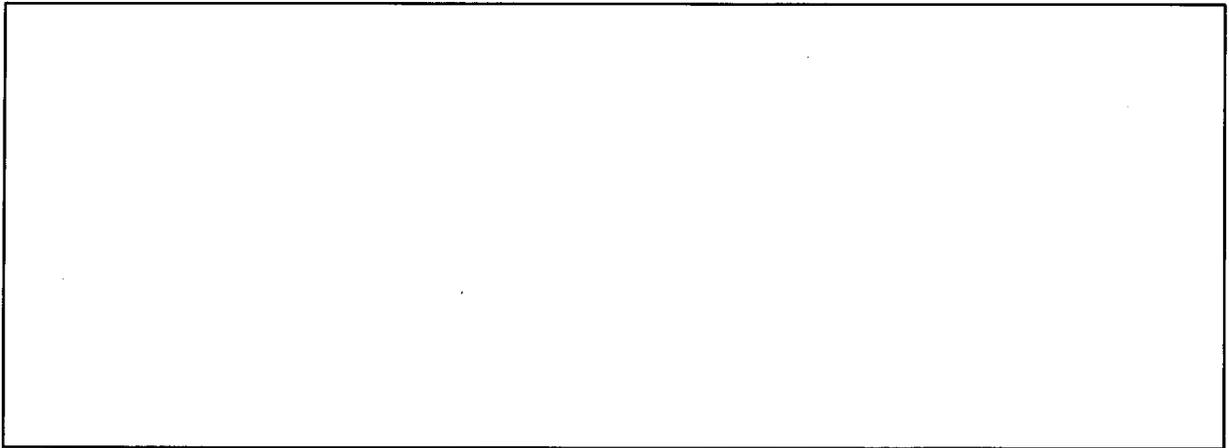


Figure 4-7. [[

]]

4.3.6. Developing and Using Functional Elements

[[

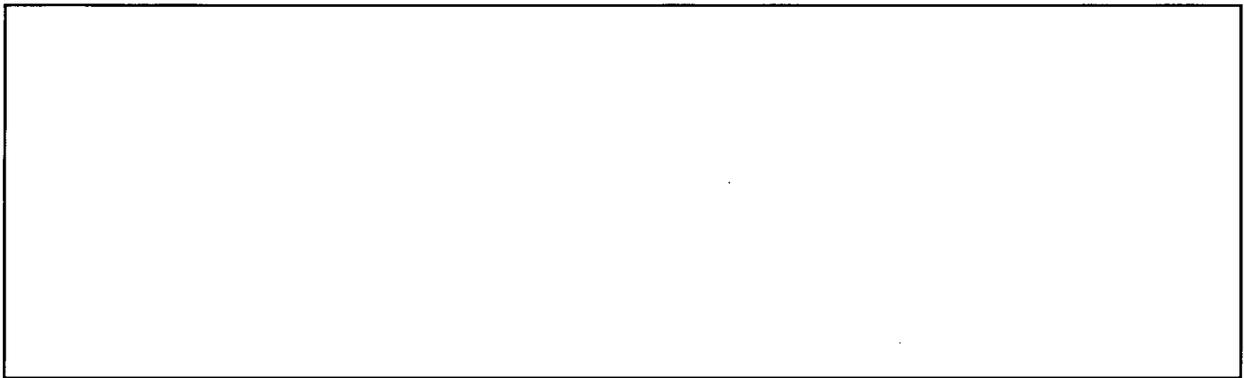


Figure 4-8.

[[

]]

II

4.3.7. Change Control

During the design process, NICSD follows NICSD procedure D-68019, which describes the configuration management process in accordance with NED procedure AS-200A131. When NICSD identifies any needed improvements or modifications to configuration items, NICSD will follow their process to modify or enhance the appropriate component and its documentation.

Change activity is controlled and documented on the Change Control Sheet. During development NICSD will resolve errors internally. Changes to resolve errors in shipped products will result in NED notification.

NICSD maintains a master configuration list that identifies the configuration items that comprise the software baseline of the FE. If an FE is modified, NICSD issues a revised master configuration list to NED for approval.

After the FPGA logic is developed, an FE might need to be modified or enhanced. In this case, the change to the FE is controlled under the above change process. Similarly, if an FPGA needs to be modified or enhanced, the change is controlled under the above process.

4.3.8. Maintenance

Actel FPGAs models A54SX72A and A54SX32A are one-time programmable devices. Therefore, after an FPGA-based product is completed, no changes to the system logic are possible without re-configuring the system. Any changes to the system must be made under strict change-control procedures, similar to those required in BTP 7-14. All changes must be thoroughly verified and validated, as well as audited and approved by the plant safety change control committee or group. 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 deciding when a design change is necessary. NICSD is responsible to provide 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. Changes to configuration items are explained in Section 4.3.7.

Modifications and/or enhancements to FEs and FPGAs require that the NICSD design group follow the lifecycle process described in this topical report to address those activities that focus on the design and development of the required or desired changes. NICSD's maintenance procedure for FEs is prescribed in NICSD D-68018 and NICSD's maintenance procedure for FPGAs is prescribed in D-68016. NICSD D-68019 also prescribes the procedure for configuration control activities relating to maintenance activities of FEs and FPGAs. After installation in a nuclear power plant, any modifications are tested at Toshiba and then installed and tested at the plant.

Maintenance activities are as follows:

- Identify software improvement needs.
- Implement problem reporting method.
- Reapply software lifecycle.
- Update the design baseline.

4.3.9. Software Tool Control and Maintenance

Software tools used by NICSD design groups for the design, development, verification, validation, and production of FPGAs are controlled in accordance with D-68020.

The following requirements are satisfied prior to approving software for use:

- Verify the functions of the software tool.
- Establish a process for verifying proper installation of the software on the computer platform to be used.
- Document the software tools used.

Software tools are approved for use by NICSD design teams. These tools go through a verification and validation process, which is described in D-68020. This procedure establishes how software tools are approved, validated, registered, and installed. When NICSD engineers use a software tool, they record the software tool information in Form 1 of D-68020. This software tool information sheet is stored within the software tool control file. All uses of a given tool version can thus be determined; and if significant errors are found in any tool version that affect the FPGA logic, the affected FPGA products can be tracked down.

Control sheets for FPGA products identify the software tools used, as well as the version and the identification number for the software tool information sheet. NICSD design engineers also file the name and version of the software tools used for FPGA implementation activities in the FPGA Implementation Record Sheet. The frozen software tool version used to build specific FEs and FPGAs is stored by NICSD.

When error notifications are distributed by the software tool vendors, NICSD evaluates the error notices to identify possible problems in using the software in the FPGA design. The NICSD engineer documents the results from this evaluation in an error notice evaluation sheet. If potential problems are identified for developed or manufactured FPGA products, NICSD engineers file a Change Control Sheet in accordance with NICSD procedure D-68020, and contact NED, who will initiate their Part 21 evaluation and notification process and also notify the FPGA product users appropriately.

4.4. Verification and Validation Process

[[

.]]

4.4.1. Design Verification

[[

]]

4.4.2. Validation Test

[[

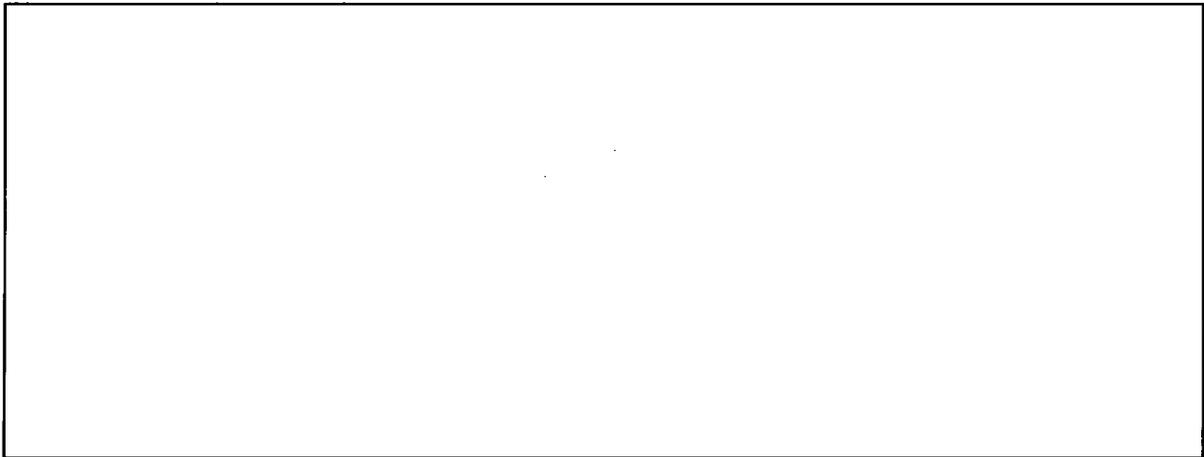


Figure 4-9. [[]]

[[

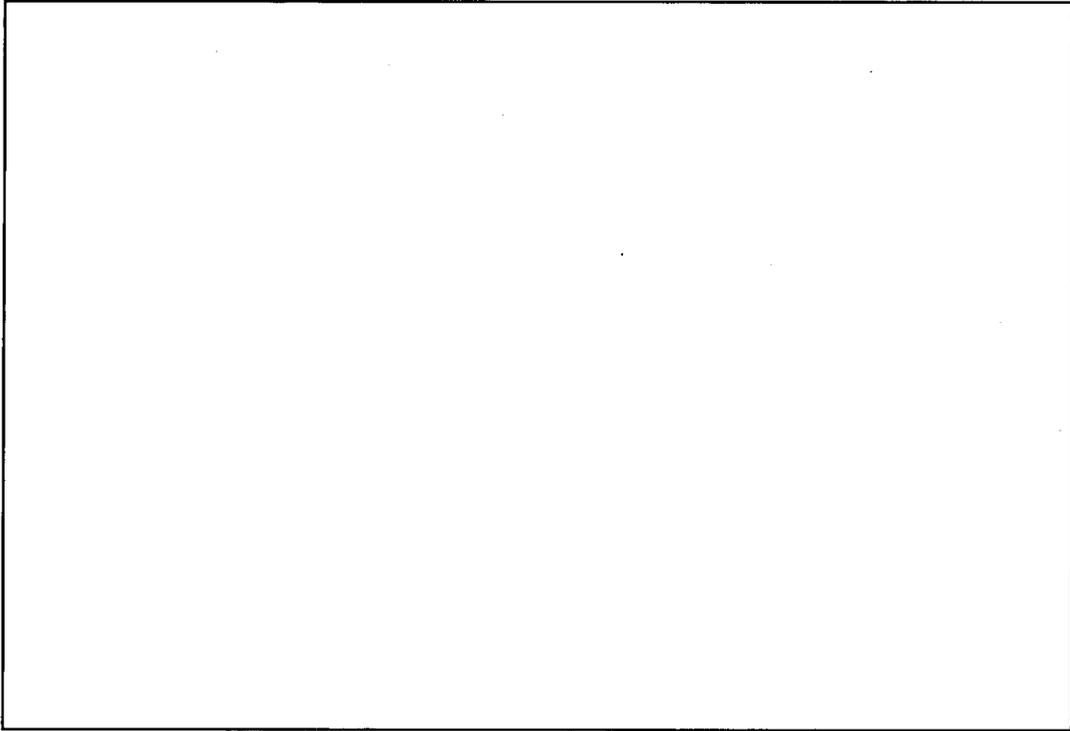


Figure 4-10. [[

]]

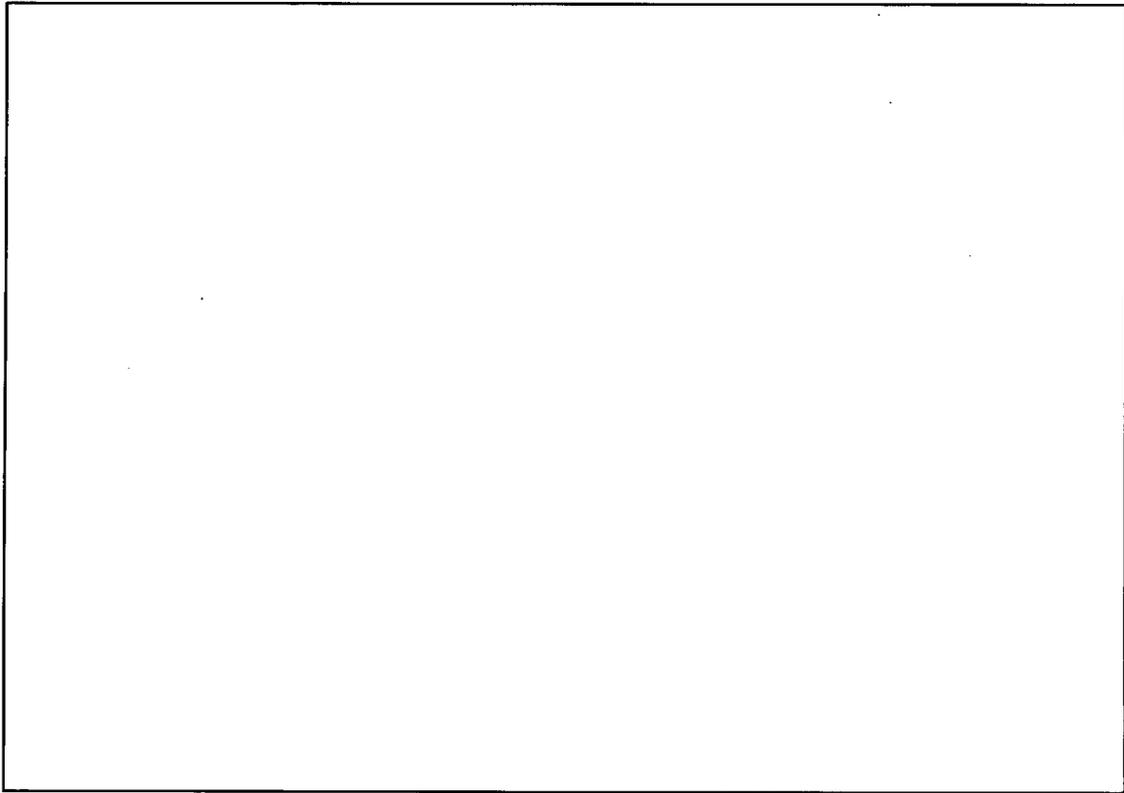


Figure 4-11. [[

]]

[[

]]

Table 4-3. Errors Anticipated for Each Phase of the Development Process

[[
[[
[[]]

[[

]]

Table 4-4. Countermeasures Against Errors Specific to FPGA-based Systems

[[
]]

4.5. V&V Results

For each phase, NED prepares a V&V report to document that phase’s V&V activities. The V&V report for the System Validation Testing Phase will summarize all V&V activities. Each V&V report contains the following information:

- Results of reviews of design, planning, review, and test documents.
- Results of RTM efforts.
- Results of reviews of hazard analyses.
- Summary of validation test results, as applicable.
- Problem reporting and corrective action, if any.

When all activities are completed, NED develops the Software Qualification Report to summarize all FPGA logic development activities, including V&V efforts. The Software Qualification Report (SQR) satisfies the documentation requirements provided in Section 8.7 of EPRI TR-107330.

If NED and NICSD find any problem in V&V activities, the problem is reported and corrective action is taken.

If NICSD finds any problem with the configuration items during FPGA validation testing, the problems are reported using Problem Reporting Sheets (PRS) in accordance with NICSD Procedure D-68016. If NICSD finds any problem in documents during Unit/Module validation testing, the problems are reported using PRS in accordance with NICSD Procedure D-68017.

Any problems that are not covered by the above cases are reported in the following manner:

- For problems caused by NED, the problem is reported and corrected in accordance with NED Procedure AS-300A008 (Reference (45)).

- For problems caused by NICSD, the problem is reported and corrected in accordance with NED Procedure AS-300A006 (Reference (44)).

After any identified problems are resolved, NED confirms that all requirements are met, all technical concerns are resolved, all corrective actions and non-conformances are disposed, and that NICSD and NED used the correct procedures appropriately in each activity. Then, NED finalizes the V&V summary report for the system. Finally, NED summarizes the results of the software activities in the SQR.

5. Hardware Qualification Process

The hardware qualification process is intended to demonstrate that the system meets those requirements that can be demonstrated by test and analysis. The requirements for acceptance and operability tests are specified in Section 5 of EPRI TR-107330 (Reference (20)) and requirements for qualification tests are specified in Section 6 of EPRI TR-107330. Qualification of the FPGA product is demonstrated primarily by conducting a series of qualification tests in accordance with EPRI TR-107330. The tests specified in the EPRI TR-107330 are required in order to comply with the applicable regulatory requirements and industry standards. In addition, recent regulatory guidance on qualification was considered, including Regulatory Guide 1.180 Revision 1.

Qualification analyses are also performed to demonstrate compliance with additional hardware and system requirements specified in EPRI TR-107330.

For specific applications, NED will confirm that the customer's requirements are bounded by the qualification envelope established by the qualification.

These qualification activities are performed under the NED QA Program.

5.1. Qualification Testing

EPRI TR-107330 describes the hardware qualification tests to demonstrate hardware acceptability for safety-related applications. As explained in Section 3.1, NED prepares the ERS based on the expectations provided in EPRI TR-107330. The ERS specifies the test requirements for pre-qualification test and qualification type test. NED performs qualification testing on a Test System which contains a Test Specimen and Test Equipment. The Preliminary Technical Evaluation Report documents which of the critical characteristics of the system are to be verified by the qualification testing, which defines the requirements for qualification testing system.

The test specimen is composed of all the units needed to recreate a typical FPGA-based system. For example, when qualifying a PRM system for a utility customer, NED will select the following units for the test specimen: an LPRM/APRM unit, an LPRM Unit, and one Flow Unit.

NED builds a test system to match one channel, division, or train of the final system to be provided to the customer. This provides an adequate and defensible type test of a shipped system, with all components, functions, and features operating. Since channels, divisions, and trains are physically and electrically separated, this provides a bounding case for all environmental qualification testing. Toshiba notes that some reactor units may not need the full complement of units and modules that were tested. Removing modules from the final configuration should not affect the results of testing, and the system will still be tested for operability by NED. Thus, based on the idea of a complete qualification providing the bounding case, it is acceptable to change the configuration that will be provided to the plant.

Test acceptance criteria are based on the expectations provided in EPRI TR-107330. These criteria are provided as acceptance criteria in the test procedures.

The test specimen requires stimulation and monitoring for the type tests. The test equipment is necessary to generate input signals and to monitor the output signals of the test specimen during the qualification type testing. The test equipment generally includes data recording equipment, power supply variation equipment, input simulators, etc. Based on the PTER, NED prepares the procurement specifications for the test equipment, including requirements for calibration and traceability to national standards. Fuchu Complex is responsible for supplying the test equipment.

The qualification tests are implemented in accordance with NED procedure AS-300A103, "Test Control Procedure" (Reference (47)).

For hardware qualification NED prepares a Master Test Plan (MTP). This document identifies the test activities and testing sequence. The MTP specifies the set of qualification tests to be performed on the test specimen, including defining a set of operability tests to be performed during qualification testing.

The following describes the hardware testing required by EPRI TR-107330 as it relates to the FPGA-based systems.

[[

]]

Detailed test processes and acceptance criteria are documented in the test procedures. Test results are documented in test reports.

5.2. Qualification Analysis

EPRI TR-107330 specifies qualification analysis requirements. These are identified in the ERS. The PTER specifies qualification analysis requirements. The qualification analyses are performed in accordance with the "Engineering and Design Procedure" (AS-200A001) (Reference (33)) by responsible NED system engineers. This procedure defines the process for performing and documenting design activities to be carried out to ensure that applicable design inputs are correctly translated into the design output documents.

The following analyses are performed:

[[

]]
Results of qualification analyses are documented in separate analysis reports.

5.3. Hazard Analysis

[[

]]

6. Implementing Toshiba's Generic Qualification Process for Application-Specific Equipment

Toshiba intends to provide NRW-FPGA-based I&C products for safety-related systems in US nuclear power plants. Toshiba will use the process specified in this topical report to develop and qualify products for new applications or for enhancements to existing products.

Once Toshiba has qualified a new or enhanced system in accordance with this topical report, Toshiba can provide the equipment to interested US utilities as follows:

- Upon receipt of a requirement specification from a US customer for a specific application, Toshiba's NED division first reviews the customer requirements and confirms consistency between the specification and the related ERS included in the topical report and Safety Evaluation Report for that equipment. This includes a determination as to whether the environmental conditions specified by the customer are bounded by the qualification envelope specified in Toshiba's Application Guide.
- Depending on the results of this review, Toshiba may need to make changes or modifications to the existing system. Then Toshiba decides whether the modified system requires additional qualification testing or analysis. Activities associated with this process are described in Section 6.3 of this topical report.
- In either case, Toshiba follows the procedure defined in this topical report to design and manufacture the system, and perform any needed qualification activities. Toshiba manufactures the equipment for sale to their customers using the same manufacturing, test, and integration methods documented in this topical report. As discussed in this report, Fuchu Complex manufactures the units and performs module and unit tests, and NED

integrates the units into a system and tests the deliverable system. If the system passes the NED and customer acceptance tests, the system is ready to be shipped.

As shown in this topical report, this system development process is performed in accordance with PSNE's 10 CFR 50 Appendix B QA program. PSNE's program provides the appropriate, expected processes for safety-related digital I&C equipment, including system development and testing; sub-tier supplier qualification; management controls; V&V; hardware qualification; planning; change control; configuration management; document generation and control; and other key processes. Toshiba maintains QA process documentation for the life time of each product installed in a US nuclear plant.

This section describes how NED applies this development process for implementing products, including qualification. This section does not describe the process of building equipment for sale to utilities.

6.1. Generating a Qualified System

When NED decides to use NRW-FPGA-based products for specific safety-related I&C systems (such as Power Range Neutron Monitor Systems, Start-up Range Neutron Monitor Systems, or Reactor Protection Systems) in US nuclear plants, NED follows the process defined in this topical report to develop and qualify the new system. The qualification of the new system application is documented in a separate topical report, which references the process defined in prior sections of this topical report.

For modifications to existing applications, Toshiba may either prepare a new topical report or revise an existing topical report.

If the qualification process includes any departures from the process documented in this topical report, the topical report for the new or modified application specifies the departures from the process documented in this topical report and demonstrates that the process and the system still meet regulatory expectations.

Toshiba's process for developing a new FPGA-based system is as follows:

1. Define the Application's Scope

Toshiba defines systems and the applicable types of reactors (e.g., Pressurized Water Reactors or BWRs) where the system can be used.

2. Define Equipment Requirements

Toshiba specifies the equipment requirements for the system, in accordance with Section 3.3 of this topical report. Toshiba will define any new hardware that must be developed for this system in this step.

3. Define the Application-Specific Software QA Plan
Toshiba defines the quality assurance plan for the FPGA logic in this step, including developing the SQAP, the system-specific V&V plan, and the application configuration management plan, as described in Section 4.2 of this topical report. This may require writing a new software QA plan, or taking an existing plan and modifying it to suit the needs of this application.
4. Design and Manufacture the FPGA-based Test Specimen
In this step, Toshiba designs and manufactures the units comprising the test specimens in accordance with the process defined in Sections 2, 3, and 4 of this topical report.
5. Unit Integration and System Integration Test
Toshiba integrates the units and tests the integrated units in accordance with Section 4.4.2 of this topical report.
6. Verification and Validation (V&V)
Toshiba performs V&V in accordance with Section 4.4 of this topical report. At the end of each V&V phase, Toshiba will prepare a V&V report.
7. Software Qualification Report (SQR)
Toshiba prepares an SQR to document the basis for qualification of the logic implemented in the FPGA-based system. The V&V reports are used to prepare the Software Quality Assurance Report.
8. Qualification Test
Toshiba prepares application-specific qualification test procedures and performs the testing in accordance with Section 5.1 of this topical report. For qualification testing, Toshiba will define and prepare a test specimen, composed of all the units needed to create a typical system.
9. Qualification Analysis
Toshiba performs the qualification analysis as described in Section 5.2 of this topical report.
10. Issuance of Topical Report to USNRC
All development and qualification activities are documented in reports. The activities are summarized in a topical report, to be provided to the USNRC. Section 6.2 of this topical report describes the required content of the application-specific topical report. The topical report may be submitted directly to the USNRC by Toshiba, or by the end user.

6.2. Organization of an Application-Specific Topical Report

Toshiba's application-specific topical report will be organized as follows:

Section 1, "Introduction," introduces the project to implement a specific system. This section contains:

- An introduction to the system-specific qualification project.
- An introduction to the I&C system to be qualified.
- A statement that the qualification project is performed as described in this generic topical report, or enhancements and modifications to the process may be provided for USNRC review and acceptance.

Section 2, "Design Process," introduces the applied design process for the applied I&C systems. The contents of this section are as follows:

- This section begins with a general statement indicating that the process used for qualification of the specific application is in accordance with the development process specified in this generic topical report.
- This section specifically identifies any departures from this generic process used for the specific application, and provides an analysis of the impact of each departure. This section also indicates whether the departures are permanent process improvements, or necessary only for this specific application.
- This section identifies the scope of the qualification.
- This section describes any changes to organizations since the last USNRC notification, and the status of all sub-tier suppliers during the project.

Section 3, "System Description," contains the following information:

- A description of the major features of the system.
- The requirements to be met by the qualified products.
- A description of the system configuration, including the system hardware configuration and the interfaces between the plant and the system.

Section 4, "FPGA Logic Qualification," provides the results of the FPGA logic implementation. This section contains the following information:

- A statement that the qualification is implemented in accordance with Section 4 of the generic topical report.
- A summary of the verification results, with the errors and their resolutions (with reference to the software verification information to be provided in Appendix C of the specific topical report).
- A summary of the validation test results.

Section 5, "Qualification Test," provides results of the qualification tests. The contents of this section are as follows:

- This section begins with a statement that the qualification testing is implemented in accordance with Section 5.1 of the generic topical report, or identifies any changes to the qualification process based on new guidance from the USNRC.
- This section contains results of pre-qualification and qualification tests, including any requirements or limitations on installation based on results of these tests.
- This section discusses any departures from related requirements of EPRI TR-107330, or new guidance, such as an USNRC Regulatory Guide on digital equipment qualification.
- This section contains the appropriate test documentation.

Section 6, "Qualification Analyses," summarizes results of the qualification analyses. The contents of this section are as follows:

- The section begins with a statement that the qualification analyses are implemented in accordance with Section 5.2 of the generic topical report, or identifies any departures from this approach.
- This section summarizes the results of the analyses.

Section 7, "References," will provide the reference document list for the project.

Appendix A, "EPRI TR-107330 Requirements Compliance and Traceability Matrix," provides a matrix demonstrating compliance with the requirements of EPRI TR-107330 for this qualification project. The matrix has Section, Summary of Requirements, Compliance, and Comment columns. These elements are evaluated and filled in as appropriate for the application-specific system.

Appendix B, "Application Guide," provides guidance for utilities when using this system, including:

- Specific guidance for the applicability of the specific system, such as system type and reactor types.
- Configuration information needed for applying the product to the safety-related system.
- A summary of the qualification envelope.

Appendix C, "Software Verification," provides software verification information.

6.3. Modifying an Existing Application

There are several reasons that Toshiba may have to modify an existing, qualified system. These include the following:

- An integrated circuit or other active device becomes obsolete.
- The customer requires a qualification envelope that exceeds the current envelope.
- A customer requires a slightly different configuration (e.g., the number of monitored points differs from the qualified system).
- An enhancement is required in the application logic or in the hardware capabilities.
- An error is found in the application logic.

Any of these changes requires Toshiba to perform some part, or all, of the process documented in this topical report. The evaluation of and justification for the scope of the project to change the application is documented, reviewed, approved, and retained in the document control system. The impact of the change determines how much of the process is required to qualify the new application.

It is possible that changing an integrated circuit or active device requires changing only the device itself, with no changes to the printed circuit board, module mass, electrical characteristics, or other qualified parameters. It is possible that the replacement part may require changes to the application logic, which may require performing additional qualification activities. It may be possible to analyze the impact, determine that no application logic changes are required, and that the replacement part is an exact form, fit, and function replacement through an equivalency evaluation, which would also determine any required qualification activities that need to be performed for this change. This evaluation is documented as a quality record, and no changes, other than the Bill of Materials, might be required.

If the qualification envelope has to be extended, Toshiba evaluates the new requirements, determines if any compensatory actions are required to meet the new requirements and whether those new requirements can be met, and then develops plans for new qualification activities. If design changes are required, Toshiba plans and performs those design activities. A test specimen incorporating any required design changes is produced, and then acceptance and qualification testing is performed on the test specimen. A new or revised topical report, or some other form of equivalent documentation, is produced for this activity to reflect the new qualification envelope. When testing is complete and the customer accepts the qualification and appropriate documentation, Toshiba can then manufacture new equipment for the customer.

Changing the number of field inputs is likely to affect the logic embedded in the FPGA. Certainly, enhancing the algorithms or repairing a design error in the logic affects the logic embedded in the FPGA. For these activities, the scope of the modification is determined, and appropriate portions of the process documented in this topical report are followed.

7. References

- (1) 10 CFR 50 Appendix B
"Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants."

- (2) 10 CFR 21
"Reporting of Defects and Noncompliance."
- (3) ASME NQA-1-1989
"Quality Assurance Program Requirements for Nuclear Facilities."
- (4) USNRC NUREG/CR-6812
"Emerging Technologies in Instrumentation and Control," March 2003.
- (5) USNRC NUREG/CR-6421
"Proposed Acceptance Process for Commercial Off-the-Shelf Software in Reactor Applications," March 1996.
- (6) USNRC Standard Review Plan, NUREG-0800, Chapter 7, Instrument and Controls Branch (HICB) Technical Position 7-14
"Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems," June 1997.
- (7) USNRC Standard Review Plan, NUREG-0800, Chapter 7, Instrument and Controls Branch (HICB) Technical Position 7-18
"Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems," June 1997.
- (8) RG 1.152
"Criteria for Programmable Digital Computer System Software in Safety Related Systems of Nuclear Power Plants," Rev. 2, January 1996.
- (9) RG 1.153
"Criteria for Safety Systems," Rev. 1, June 1996.
- (10) RG 1.168
"Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Rev. 1, February 2004.
- (11) RG 1.169
"Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," September 1997.
- (12) RG 1.170
"Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," September 1997.
- (13) RG 1.171

- “Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” September 1997.
- (14) RG 1.172
“Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” September 1997.
- (15) RG 1.173
“Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” September 1997.
- (16) RG 1.180
“Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety Related Instrumentation and Control Systems,” Rev 1, October 2003.
- (16a.) RG 1.209
“Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants,” March 2007.
- (17) RG 1.28
“Quality Assurance Program Requirements (Design and Construction)(Task RS 002-5),” Rev 3, August 1985.
- (18) EPRI TR-102260
“Supplement Guidance for the Application of EPRI Report NP-5652 on the Utilization of Commercial Grade Items,” March 1994.
- (19) EPRI-TR-102323
“Guidelines for Electromagnetic Interference Testing in Power Plant Equipment,” Rev. 2, November 2000.
- (20) EPRI TR-107330
“Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants,” December 1996.
- (21) EPRI TR-107339
“Evaluating Commercial Digital Equipment for High Integrity Applications,” December 1997.
- (22) EPRI TR-106439
“Guideline on Evaluation and Acceptance of Commercial Digital Equipment for Nuclear Safety Applications,” October 1996.
- (23) EPRI NP-5652

“Utilization of Commercial Grade Items in Nuclear Safety Related Applications,”
March 1988.

(24) IEEE Standard 7-4.3.2-1993

“IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power
Generating Stations,” September 1993.

(24a.) IEEE Standard 7-4.3.2-2003

“IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power
Generating Stations,” September 2003.

(25) IEEE Standard 603-1991

“IEEE Standard for Safety Systems for Nuclear Power Generating Stations.”

(26) IEEE Standard 1012-1998

“Standard for Software Verification and Validation Plans.”

(27) IEEE Standard 1076-2000

“IEEE Standard VHDL Language Reference Manual.”

(28) IEEE Standard 1164-1993

“IEEE Standard Multivalued Logic System for VHDL Model Interoperability.”

(29) IEEE Standard 384-1992

“IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits.”

(30) IEEE Standard 352-1987

“IEEE Guide to General Principles of Reliability Analysis of Nuclear Power Generating
Station Safety Systems.”

(31) Toshiba 4401-4

“Nuclear Energy QA Program Description.” Rev. 1.

(32) Toshiba NED AS-100A008 Rev. 9

“Procedure for Indoctrination and Training.”

(33) Toshiba NED AS-200A001 Rev. 8

“Engineering and Design Procedure.”

(34) Toshiba NED AS-200A110 Rev. 1

“Procedure for Commercial Grade Items and Services.”

(35) Toshiba NED AS-200A111 Rev. 1

“Acceptance Procedure for Commercial Grade Items.”

- (36) Toshiba NED AS-200A112 Rev. 1
“Acceptance Procedure for Commercial Grade Services.”
- (37) Toshiba NED AS-200A116 Rev. 1
“Preparation Procedure for Equipment Requirement Specification.”
- (38) Toshiba NED AS-200A128 Rev. 0
“Digital System Lifecycle Procedure.”
- (39) Toshiba NED AS-200A129 Rev. 0
“Digital System Development Procedure.”
- (40) Toshiba NED AS-200A130 Rev. 1
“Digital System V&V Procedure.”
- (41) Toshiba NED AS-200A131 Rev. 1
“Digital System Configuration Management Procedure.”
- (42) Toshiba NED AS-200A132 Rev. 0
“Digital System Safety and Hazard Analysis Procedure.”
- (43) Toshiba NED AS-300A002 Rev. 9
“Procedure for Evaluation of Vendors.”
- (44) Toshiba NED AS-300A006 Rev. 3
“Nonconformance Control Procedure for Procured Items and Services.”
- (45) Toshiba NED AS-300A008 Rev. 8
“Nonconformance Control and Corrective Action Procedure.”
- (46) Toshiba NED AS-300A013 Rev. 7
“Auditor Qualification Procedure.”
- (47) Toshiba NED AS-300A103 Rev. 3
“Test Control Procedure.”
- (48) Toshiba NICSD D-68016 Rev. 3
“NICSD Procedural Standard for FPGA Products Development.”
- (49) Toshiba NICSD D-68017 Rev. 3
“NICSD Procedural Standard for FPGA Device Development.”
- (50) Toshiba NICSD D-68018 Rev. 3

Appendix A - Summary of Applicable NED and NICSD Instructions

Table A-1. NED Standards

Document Number	Title	Description
AS-100A008	Procedure for Indoctrination and Training	[[
AS-200A001	Engineering and Design Procedure	
AS-200A110	Procedure for Commercial Grade Items and Services	
AS-200A111	Acceptance Procedure for Commercial Grade Items	
AS-200A112	Acceptance Procedure for Commercial Grade Services	
AS-200A116	Preparation Procedure for Equipment Requirement Specification	
AS-200A128	Digital System Lifecycle Procedure	
AS-200A129	Digital System Development Procedure	
AS-200A130	Digital System Verification & Validation Procedure]]

Document Number	Title	Description
AS-200A131	Digital System Configuration Management Procedure	[[
AS-200A132	Digital System Safety and Hazard Analysis Procedure	
AS-300A002	Procedure for Evaluation of Vendors	
AS-300A006	Nonconformance Control Procedure for Procured Items and Services	
AS-300A008	Nonconformance Control and Corrective Action Procedure	
AS-300A013	Auditor Qualification Procedure	
AS-300A103	Test Control Procedure]]

Document Number	Title	Description
D-68018	NICSD Procedural Standard for Functional Element Development	[[
D-68019	NICSD Procedural Standard for FPGA Configuration Management	
D-68020	NICSD Procedural Standard for Control of Software Tools for FPGA-based Systems]]

Appendix B - Actel FPGA Features

Toshiba selected Actel FPGA models A54SX72A and A54SX32A for use in its FPGA-based I&C system.

Models A54SX72A and A54SX32A are part of Actel's standard product line. Actel designed the FPGAs for use in high reliability applications, including military and space applications. For space applications, special highly radiation tolerant designs of the FPGAs are used. For US National Aeronautics and Space Administration (NASA) and US Department of Defense use, Actel has guaranteed to produce product that is form, fit, and function equivalent to these devices for about 30 years from their release. Reliability and availability result from the Actel design, which exhibits a failure in time (FIT) less than 100, which translates to less than 100 failures in one million hours.

These FPGAs are not custom parts, but are one-time configurable parts designed for low volume applications, where the cost of an Application Specific Integrated Circuit (ASIC) is not warranted. The FPGA is designed to implement digital logic, absorbing many discrete integrated circuit packages into a single, complex device. An FPGA can only implement digital logic. Therefore, all analog processing and conversion between analog and digital representations occur in devices attached to the FPGA. Standard parts are used for these functions, chosen by NICSD for reliability.

The Actel design can be thought of as a large number of high impedance, non-conducting antifuses, providing a sea of modular logic elements. When set into their low-impedance state, antifuses create circuit connections between logic elements. The routing capabilities are incorporated into the top two metallization layers, thus preserving the silicon base for logic elements. The design of the routing elements can be highly optimized for fast, complex circuits.

The Actel device also provides support for testing and inspection of its operation, using boundary scan techniques and industry-standard Joint Test Action Group (JTAG) ports. These capabilities exist in the FPGAs, and provision is made for JTAG ports on the printed circuit board. NICSD engineers will determine if such capabilities are necessary for each FPGA design. NICSD engineers use these capabilities in developing the FPGA design and coding, as well as in root cause evaluations of failed modules. To further enhance testability and reduce undesirable circuit behavior, the basic architecture of each module is a clocked sequential circuit, with periodic synchronizing registers.

In addition to highly flexible and powerful design routing capabilities, the FPGA design includes significant support for clock distribution and clocked sequencing of various areas of the FPGA. These clock networks can be used to further reduce the requirements for routing and delaying clock signals for the logic elements.

FPGA Architecture

The architecture of an Actel FPGA is very similar to that of a conventional gate array. The core of the device consists of simple logic cells used to implement the required logic gates and storage elements. The logic cells implement combinatorial and memory functions. The software tools connect the logic cells with segmented routing tracks. Unlike gate arrays, the segment lengths are predefined and can be connected with low-impedance switching elements to create the precise routing length required of the interconnect signal. Surrounding the logic core is the interface to the integrated circuit's input and output pins.

The major elements of the Actel FPGA architecture are the logic cells, the interconnect resources, I/O modules, and clocking resources, as described below.

- Logic cells

The Actel FPGA design can be thought of as an array of modular logic cells or elements, with programmable interconnects, partitioned by a large number of high impedance, non-conducting antifuses. When set into their low-impedance state, antifuses create circuit connections between logic cells.

Figure B-1 shows the typical FPGA configuration. Logic cells on the FPGA are of two types: register cells (R-cells) and combinatorial cells (C-cells). An R-cell provides a single flip-flop for data storage. The C-cell implements a complex range of combinatorial functions. Up to five inputs may be selected when the FPGA is designed, supporting up to 4,000 different combinatorial functions. There are no other software elements that define logic involving multiple C- or R-cells in the Toshiba FPGA-based I&C system. There are software elements that define single C- or R-cell functions that the Actel software tools use to define simple logic functions.

[[

]]

The C-cells and R-cells are grouped into horizontal banks on the chip, called Clusters, which are further grouped into SuperClusters. The Clusters and SuperClusters are designed with local, internal routing capabilities. Within these groups of cells, FastConnect and DirectConnect routing resources provide fast, predictable connections, minimizing the use of antifuses necessary to generate a function. These local resources have lower capacitance and lower resistance than the global routing elements, which decreases propagation delays through the logic.

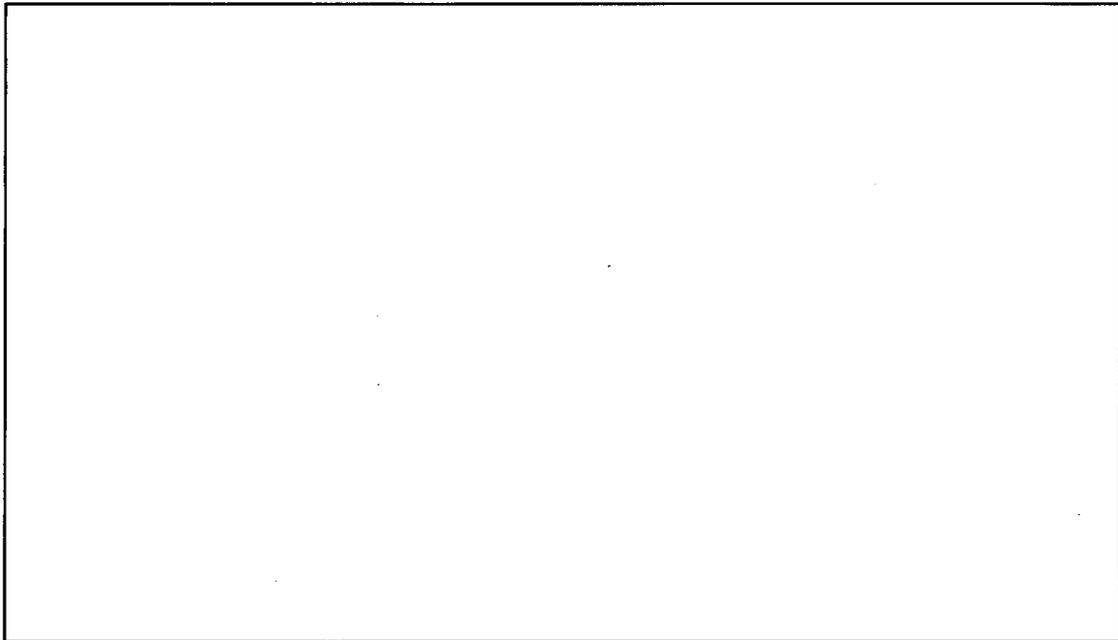


Figure B-1. Typical FPGA Configuration

- Interconnect Resources

Actel FPGAs are an array of logic modules that the user can interconnect by configurable routing. The routing determines both the interconnections of the modules as well as each module's logical function. Logic modules are organized in rows and columns across the chip. Adjacent to each row of logic modules are routing channels. These are used to configure the logic module, by connecting the inputs and outputs of logic modules to implement the design and Input/Output (I/O) modules to connect the FPGA and its design to the remainder of the system.

Within the routing channels are programmable antifuse elements. The antifuse is normally in the high impedance, or open, state. Programming forms a low impedance electrical connection between routing elements. The size of this interconnection is extremely small, providing abundant routing resources. The routing resources permit the designer to maximize use of the FPGA by providing selectable horizontal and vertical routing between modules.

- Input/Output (I/O) Modules

The I/O modules surround the array of logic modules and routing channels. The I/O modules translate and interconnect the logic signals from the core of the device to the FPGA integrated circuit input and output pads. The I/O modules use the interconnect resources to connect to the logic modules.

- Clocking Resources

In addition to highly flexible and powerful design routing capabilities, the FPGA design includes significant support for clock distribution and clocked sequencing of the modules within the FPGA. These clock networks are used to further reduce the requirements for routing and delaying clock signals for the logic elements.

Actel's routing structure provides the following clock networks:

- HCLK, which is hardwired into the circuit.
- CLKA and CLKB, which are global clocks.

The HCLK is used as the system clock, and CLKA and/or CLKB are used to distribute the reset signal. CLKA and CLKB provide identical functions in the FPGA. In the PRM system design, only the CLKB was used, but either or both CLKA and CLKB can be used in future designs.

- Security Fuses

The Actel FPGAs have a special security fuse that prevents any internal probing and overwriting of the logic provided. [[
]] If the security feature is engaged, it is not possible to access the internal logic or state of the device. [[

]]

The basic Actel FPGA device design makes reading back antifuse states impossible. For commercial products, this is a concern for reverse engineering and functionality copying. Actel implements this functionality with a set of internal security features throughout the fabric of the device. These devices are designed to make reading the design back or probing the design impossible. However, probing logic states through the built-in test access ports is still possible, providing the capability to evaluate failures in FPGAs.

- Power Requirements

An antifuse is programmed by applying a sufficiently high voltage across it to break down an oxide barrier and generate a short between two traces within the FPGA, which Actel calls an antifuse. Once an FPGA has been programmed, power consumption is extremely low, because the distances traveled by the signals are very short. Antifuses pose a low resistance path, and the interconnects are all low capacitance.

FPGA Programming and Software Tools

The most common development language used with FPGA is VHDL. Although this development language looks similar to conventional programming languages, there are some important differences. A VHDL is inherently parallel; i.e., commands, which correspond to logic gates, are executed (computed) in parallel, as soon as a new input arrives. A HDL program mimics the behavior of a physical, usually digital, system. It also allows incorporation of timing specifications (gate delays).

NICSD uses the Actel Libero® integrated development environment (IDE) software tool to represent the logic circuit of the FPGA. The Actel Libero® IDE provides the software tools necessary to support design, verification, and validation of logic to be embedded in the A54SX32A and A54SX72A FPGAs used by Toshiba. Table B-1 below lists the tools that are used in this process, [[
]]

Table B-1. Software Vendors and Tools

Vendor	Software Tool
Actel	Libero®* Integrated Design Environment (IDE)
Synplicity®	Synplify®** Actel Edition (AE)
Actel	Designer
Actel	SmartTime and Timer
Actel	SmartPower
Actel	NetList Viewer
Actel	Silicon Sculptor II (with BP Microsystems)
Actel	Silicon Explorer
Exsent	PinPort

* Libero® is trademark of Actel.

** Synplify® is trademark of Synplicity®

*** ModelSim® is trademark of Mentor Graphics®

The Libero® environment coordinates supplying the VHDL file created by the NICSD engineer to the logic synthesis tool, Synplicity® Synplify®. The Synplify® tool transforms the VHDL text into logical gates, based on the capability of the FPGA selected by the NICSD engineer. The output from the tool is a netlist of gates and connections, in an industrial standard format called Electronic Design Interchange Format (EDIF). The Actel Libero® IDE provides a design management environment that seamlessly integrates multiple design tools, hiding the

details of the interactions between tools. Section 4.3.1 provides detailed information on the system development process followed by Toshiba using the Actel software tools.