Class 2

Document No	IM-2003-171-NP Revision 0
Date	December 2, 2003

Topical Report of Generic Qualification Program for FPGA-Based Safety-Related I&C Systems

NON-PROPRIETARY MARKUP VERSION

改訂番号 Rev No	年 月 日 Date	改訂来歴 History	頁 Page	承 認 Approved	調 査 Reviewed	担 当 Prepared

年月日 Date	発 行 Section	承 認 Approved	調 査 Reviewed	担 当 Prepared	図書保管番号 Document filing No
'03.12.2	Control & Electrical Engineering Dept.	M. Oda	A. Tanaka	S. Odanaka	RS-5114516

株式会社 東芝 原子力事業部
TOSHIBA Corp. Nuclear Energy Division

Table of Contents

1. INTRODUCTION 4
   1.1. Objective 4
   1.2. Abbreviations 5
2. TOSHIBA FPGA-BASED I&C SYSTEM PROJECT 6
   2.1. Project Qualification Plan 6
   2.2. Scope of the Project 7
3. SYSTEM DESCRIPTION 9
   3.1. General Description 9
   3.2. System Specification 10
   3.3. Characteristics of NRW-FPGA 20
4. VERIFICATION AND VALIDATION 23
   4.1. Assuring Quality of FPGA 23
   4.2. Design and Manufacturing Process 26
   4.3. Verification 29
   4.4. Validation Test 38
   4.5. V&V Results 38
5. Qualification Process 39
   5.1. PRE-QUALIFICATION TESTS 39
6. QUALIFICATION TEST 43
   6.1. ENVIRONMENTAL TEST 43
   6.2. EMI/RFI TEST 44
   6.3. SURGE TEST 45
   6.4. CLASS 1E/Non-1E ISOLATION TEST 45
   6.5. ELECTROSTATIC DISCHARGE (ESD) TEST 46
   6.6. SEISMIC TEST 46
   6.7. PERFORMANCE PROOF TEST 47
   6.8. POST-QUALIFICATION TESTS 48
7. SAFETY ANALYSIS ..... 49 PROPRIETARY

[redacted]

8. REFERENCES 52

APPENDIX A: EPRI TR-107330 REQUIREMENTS COMPLIANCE AND TRACEABILITY MATRIX

APPENDIX B: APPLICATION GUIDE
APPENDIX C: SUPPLEMENTAL MATERIAL

1. INTRODUCTION

1.1. Objective

Toshiba is performing generic qualification of Non Re-writable (NRW) Field Programmable Gate Array (FPGA)-based safety related Instrumentation and Control (I&C) systems. These systems mainly operate based on specified digital circuits and have neither central processing units (CPUs) nor operating systems (OSs). Therefore these systems have advantages compared with generic CPU-based systems, such as high testability and long life supply. Toshiba is qualifying NRW-FPGA-based I&C systems to provide these advantages for nuclear safety-related systems at U.S. Nuclear Power Plants.

Selected applications of NRW-FPGA-based I&C systems are as the following systems.

- Power Range Monitor (PRM) of Boiling Water Reactor
- Trip Module (TM)

The PRM system monitors reactor power by measuring neutron flux level and issues a trip signal when the power exceeds specified setpoints. TM measures plant conditions by processing sensor signals and issues a trip signal when the measured value exceeds specified setpoints. Both PRM and TM can be used in safety-related (class 1E) systems.

Signal processing functions embedded in an FPGA are composed of physical circuits. In the FPGA-based safety-related I&C systems, the logic is built from simple, functional elements. These functional elements are independently verified. Only these simple. functional elements can be used to develop the more complex system logic. These circuits are similar to analog circuits. To implement this process, Toshiba has developed a qualified manufacturing process for FPGA-based control systems.

Toshiba's NRW-FPGA-based safety-related I&C system processes signals primarily by digital circuits embedded on FPGAs. The system has a few analog circuits that process detector signals as inputs. The analog signals are converted to digital signals, and processed by FPGA circuits.

The qualification of NRW-FPGA-based systems is based on EPRI TR-107330. The generic qualification approach described in EPRI TR-107330 includes both hardware qualification and software qualification. The NRW-FPGA system does not use application software. However, a hardware description language called VHDL is used for designing and manufacturing FPGA circuits. For NRW-FPGA software qualification is performed using Verification and Validation (V&V) for the VHDL.

The objective of this report is to document the results of generic qualification of NRW-FPGA-based systems.

1.2. Abbreviations

FPGA: Field Programmable Gate Array

An FPGA is an integrated circuit that can be logic-implemented.

NRW-FPGA: Non-Rewritable FPGA

A type of FPGA that can not be rewritten once implemented.

VHDL: Very High Speed Integrated Circuit Hardware Definition Language

A hardware description language which defines FPGA circuit.

This section will be completed later

2. TOSHIBA FPGA-BASED I&C SYSTEM PROJECT

2.1. Project Qualification Plan

This project is performed in accordance with the project qualification plan described in the Attachment.

PROPRIETARY

2.2. Scope of the Project

The scope of the generic qualification program includes the following safety systems.

- Power Range Monitor (PRM)
- Trip Module (TM)

The generic qualification program 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 project includes the scope of design, manufacturing and test as follow:

- Design of FPGA-based safety-related I&C system
  (PRM and TM)
- Manufacturing a set of one division of FPGA-based equipment
- Testing:
  - Test requirements for a channel
  - Detector signals will be simulated by a signal generator

The scope of this report and the scope of manufacturing and tests is shown in Fig. 2-1.

This project does not include design, manufacturing or testing of detectors, because they will not be modified from the conventional system.

The standard design for a BWR-5 neutron monitoring system is being applied as the reference design for NRW-FRGA system. A general description of the design is given in Section 3.2.1.

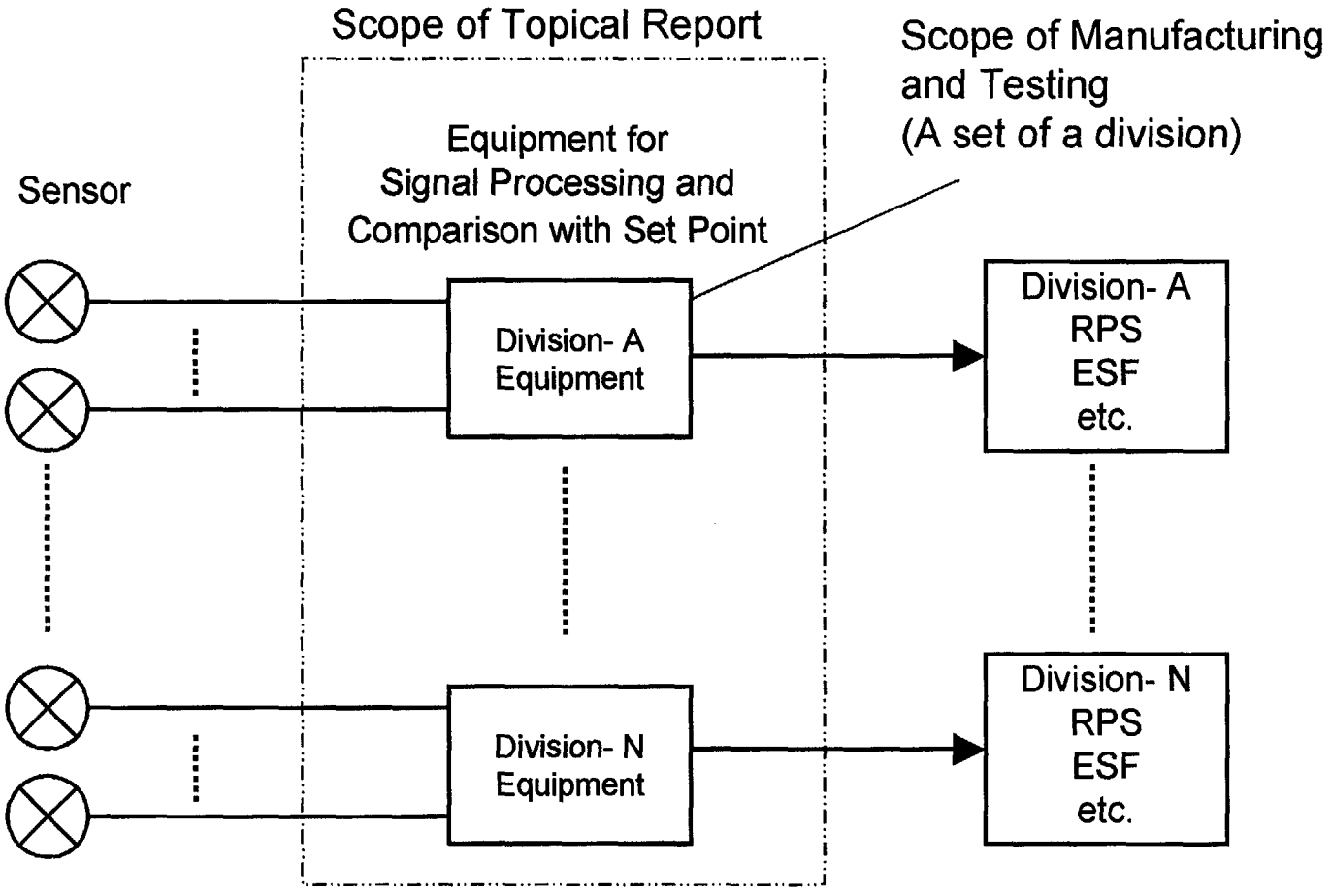


Fig. 2-1 : Scope of Design, Manufacturing and Tests

3. SYSTEM DESCRIPTION

3.1. General Description

3.1.1. Background

Toshiba has extensive experience in supplying nuclear safety-grade I&C systems in Japan, including Power Range Monitors (PRM) and Trip Modules (TM). Also, Toshiba developed safety-related digital I&C systems and supplied these systems to operating plants as upgrades. Based on the above technology, Toshiba designed and manufactured the world's first fully integrated microprocessor-based BWR digital safety system. This system has been used at Kashiwazaki-Kariwa Unit 6.

Toshiba has extensive software QA experience in designing and supplying safety systems. Toshiba makes extensive use of this experience in the design and manufacture of the FPGA-based Safety Related I&C System products.

Toshiba provides NRW-FPGA-based systems to address known issues with CPU based systems, while maintaining the benefits of digital systems, i.e. calibration drift reduction and simplified operation.

To resolve the issues existing both in conventional analog systems and in CPU-based system, Toshiba defines system requirements and designs logic to be implemented by FPGA-based circuits. Toshiba FPGA-based circuits process signals by hardware only. Therefore:

- No CPUs are used
- No OS and application software are used

Additional discussion of the advantages of ASIC (quite similar with FPGA) based systems can be found in NUREG/CR-6812.

3.2. System Specification

3.2.1. Power Range Monitor (PRM)

This Section describes a typical design specification of the Power Range Monitor (PRM) for BWR-5 neutron monitoring system. A system configuration and an equipment configuration are shown in Fig. 3-1 and Fig. 3-2 respectively. As mentioned in Section 2, the requirements of nuclear plants are not changed in this project

The PRM provides neutron flux information for monitoring power level of the reactor core. The PRM consists of the following subcomponents:

a. Local Power Range Monitor (LPRM)
b. Average Power Range Monitor (APRM)
c. Recirculation Flow Measurement
d. Rod Block Monitor (RBM)

The LPRM, APRM, Recirculation Flow Measurement and RBM unit have NRW-FPGA-based modules.

The LPRM continuously monitors the local neutron flux distribution in the core. It provides indication and reading of this information to other systems for operation and control. It also provides alarms when preset levels are reached. Fig. 3-3 shows the block diagram for LPRM Module.

The APRM averages the output signals from selected LPRM signal conditioners. It consists of six channels. LPRM signals are divided and assigned to APRM channels. The APRM issues trip signals for generating reactor trip and alarm functions. The setpoints of certain trips are dependent on the Recirculation flow rate. Fig. 3-4 shows the block diagram for APRM Module.

The Recirculation Flow Measurement function consists of four channels. Signals from a pair of differential pressure transmitters from each recirculation loop, are input to an associated Flow Measurement Module, where they are added and processed to determine the Flow data signal. Fig. 3-5 shows the block diagram for the Recirculation Flow Measurement Module.

The RBM is a system to stop withdrawing of the control rods to prevent fuel damage when the rods are continuously withdrawn due to malfunction or operator error. The RBM averages the LPRM signals surrounding each control rod being withdrawn, and use the averaged signals to detect local power change during the rod withdrawal. If the averaged LPRM signal exceeds a preset rod block setpoint, a control rod block demand will be issued to the Reactor Manual Control System. The RBM is a dual channel, highly reliable system, but not classified as a safety system (i.e. non-Class 1E).

Monitoring ranges of PRM are as follows:

LPRM: 1.2×10^{12} - 2.8×10^{14} neutrons/cm^2-sec

APRM: 0 - 125 % (Power)

Recirculation Flow Rate: 0 - 1.2×10^4 m^3/h

RBM: 0 - 125 % (Power)

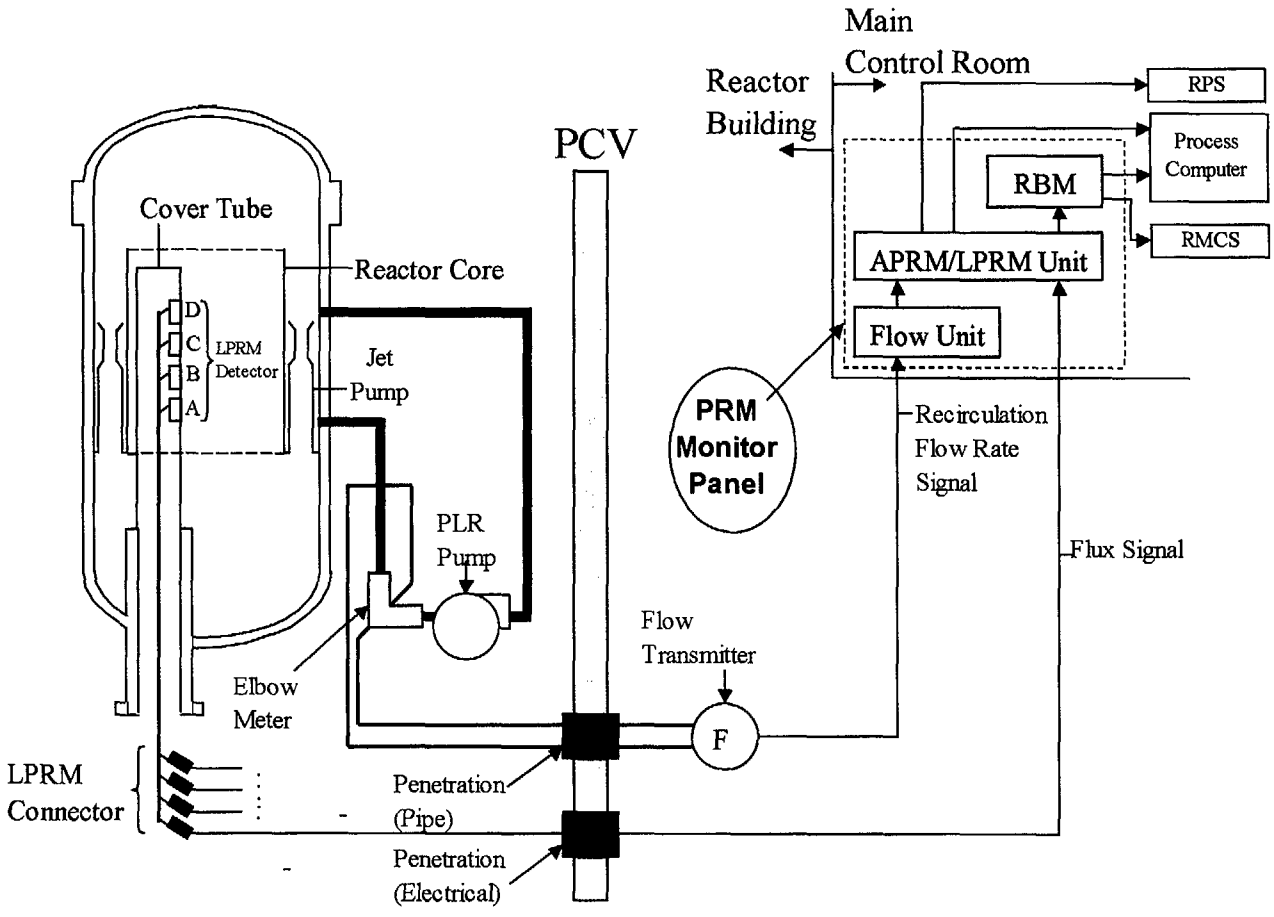
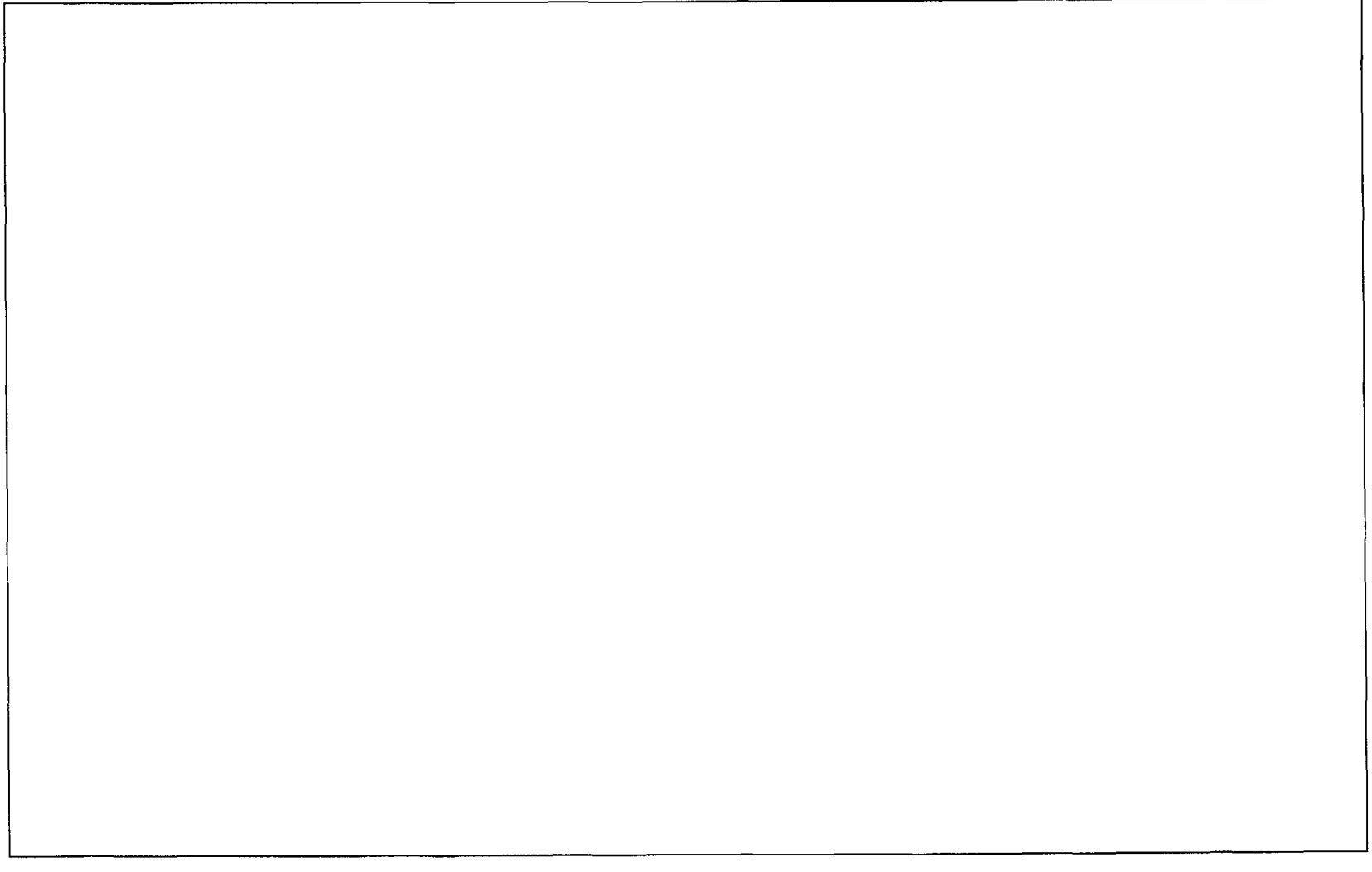
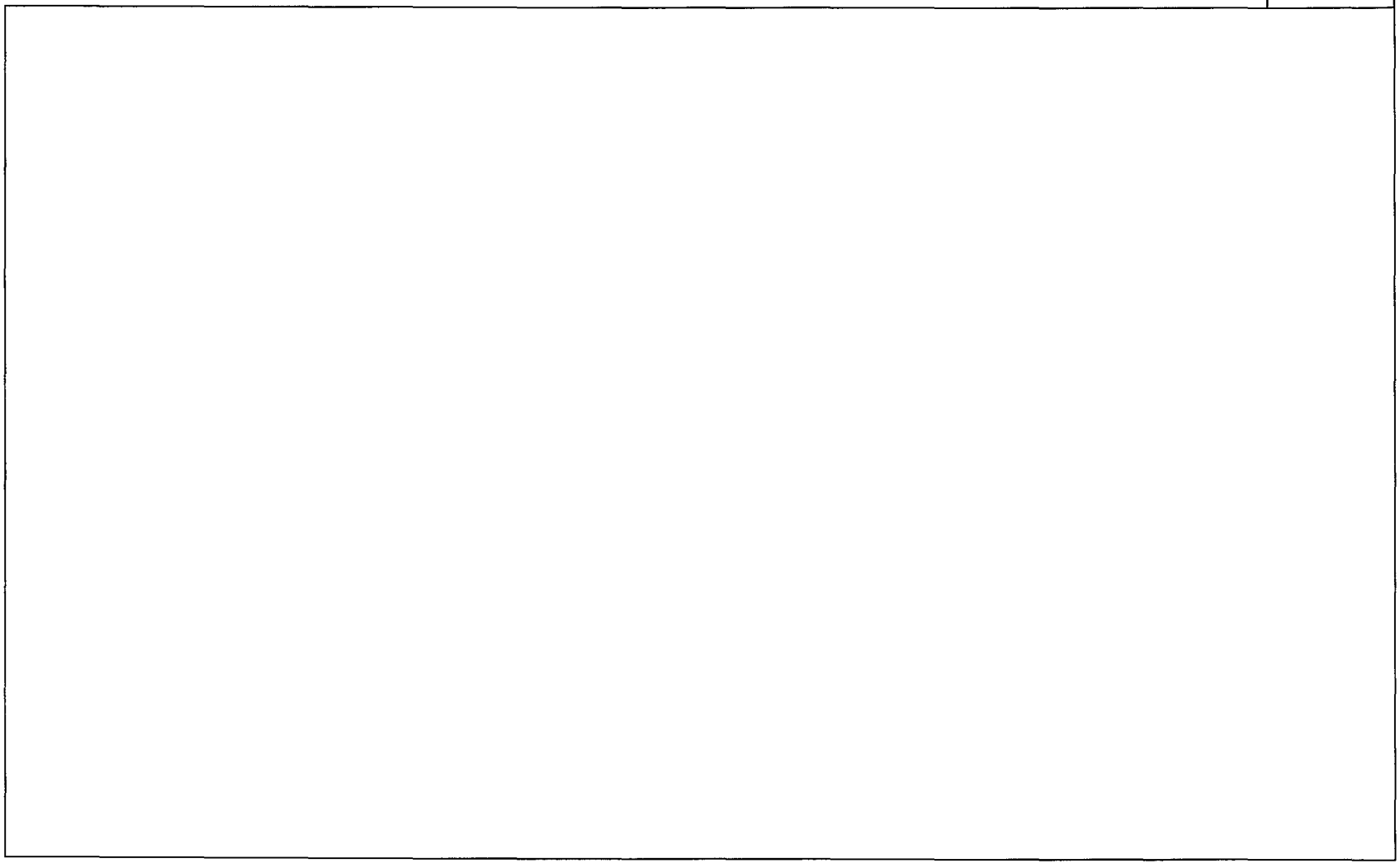


Fig. 3-1 : Power Range Monitor System Configuration

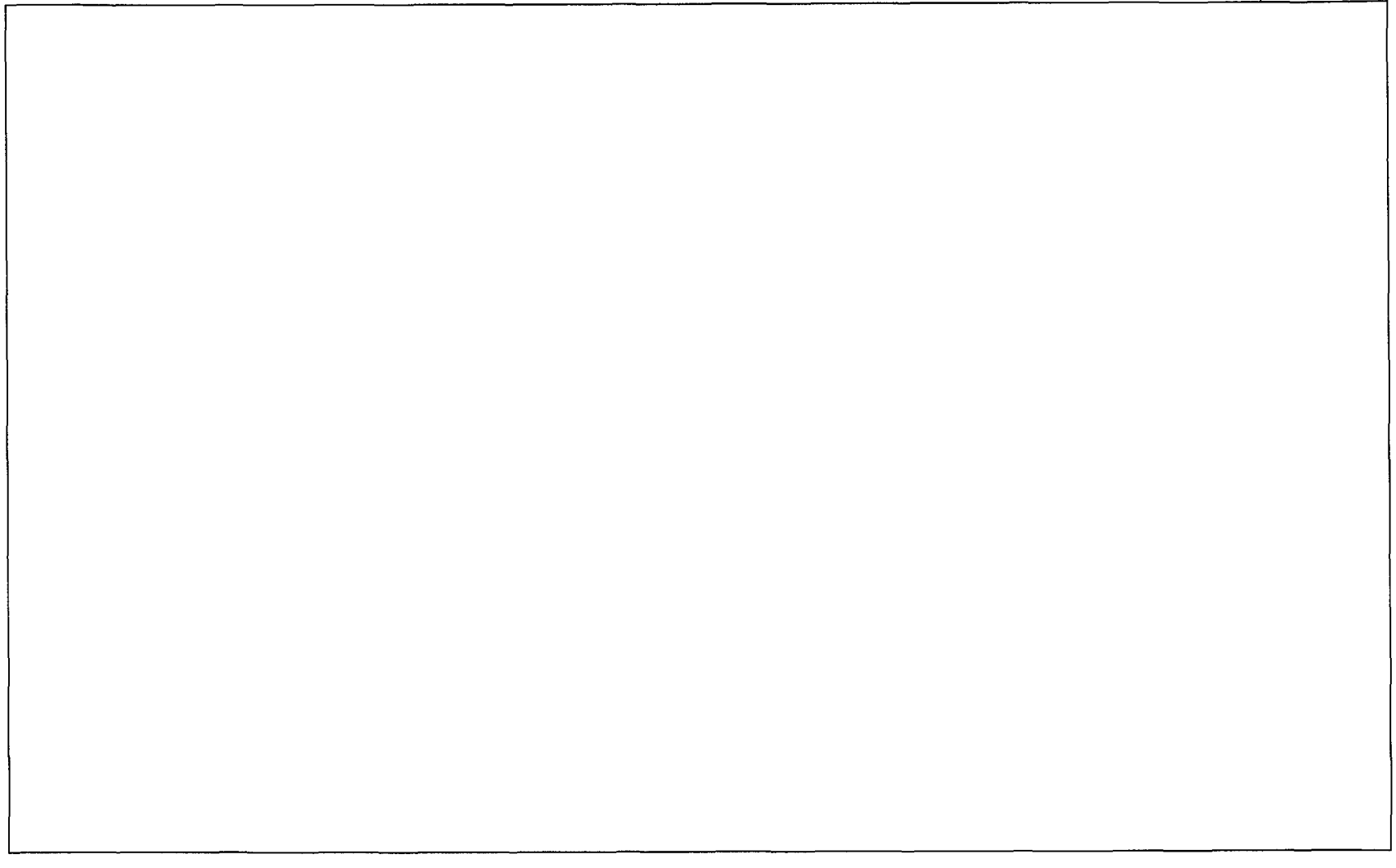
PROPRIETARY



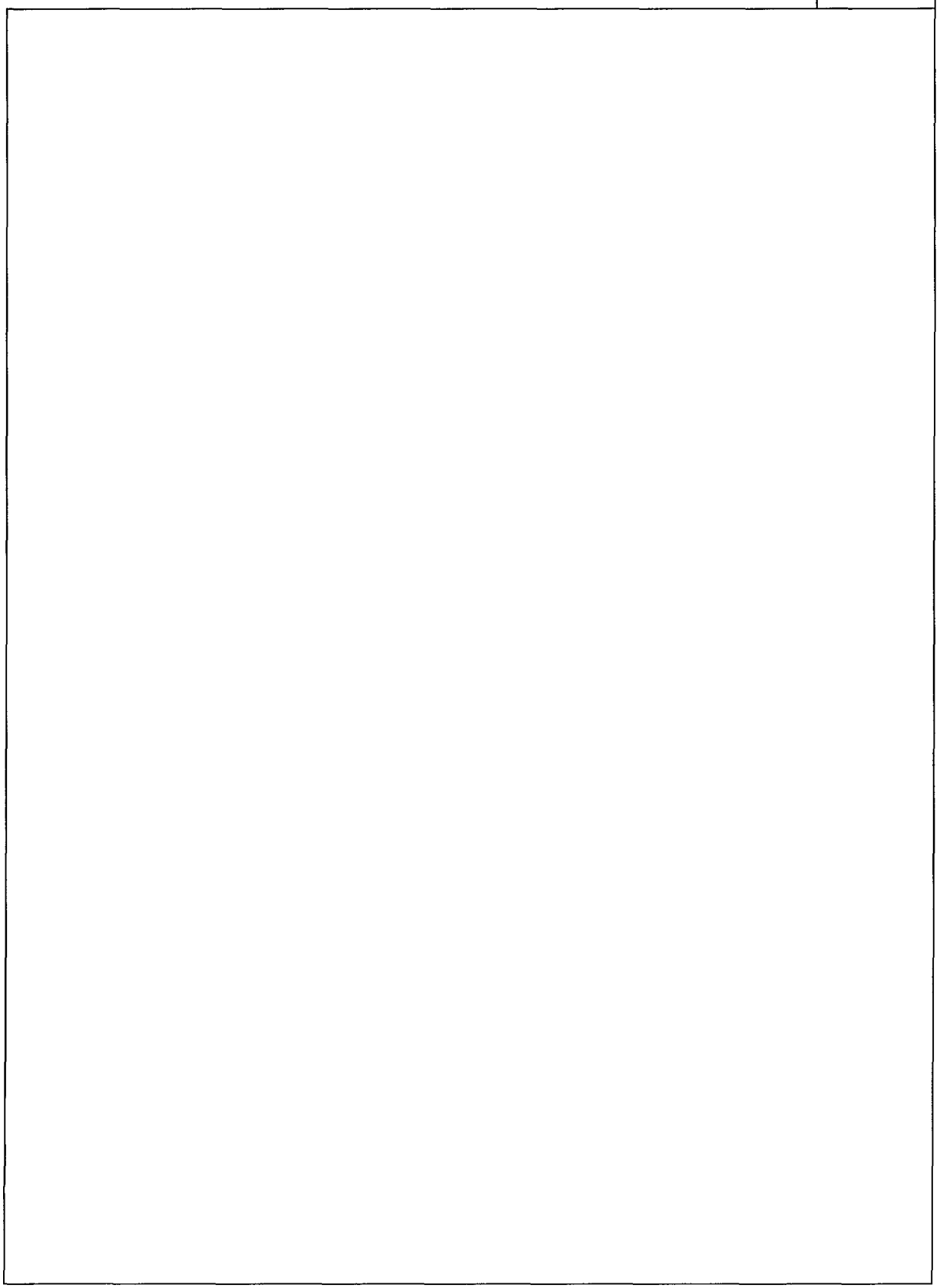
PROPRIETARY



PROPRIETARY



PROPRIETARY

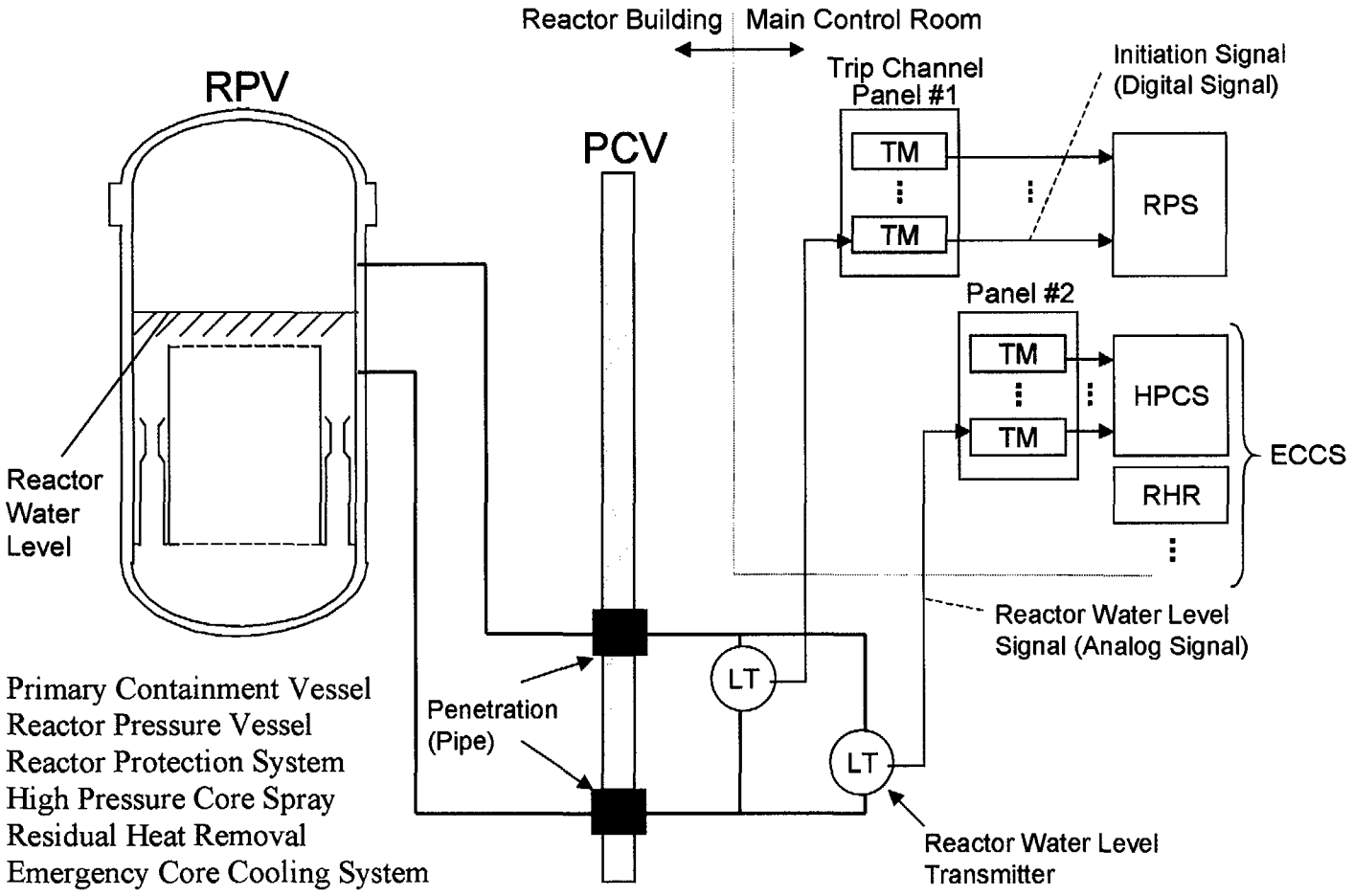


3.2.2. Trip Module

Trip Module (TM) measures plant conditions by processing sensor signals and issues a trip signal when the measured value exceeds specified setpoints. Each TM receives an analog signal from a sensor which monitors a plant variable. The TM compares the monitored variable value with a trip setpoint value. The TM issues a separate, discrete (trip/no trip) output signal to trip logics, such as RPS and ECCS. The TM has capability for testing and calibration during power operation.

Fig. 3-6 shows the system configuration, and Fig. 3-7 shows the block diagram of a typical NRW-FPGA-based module.

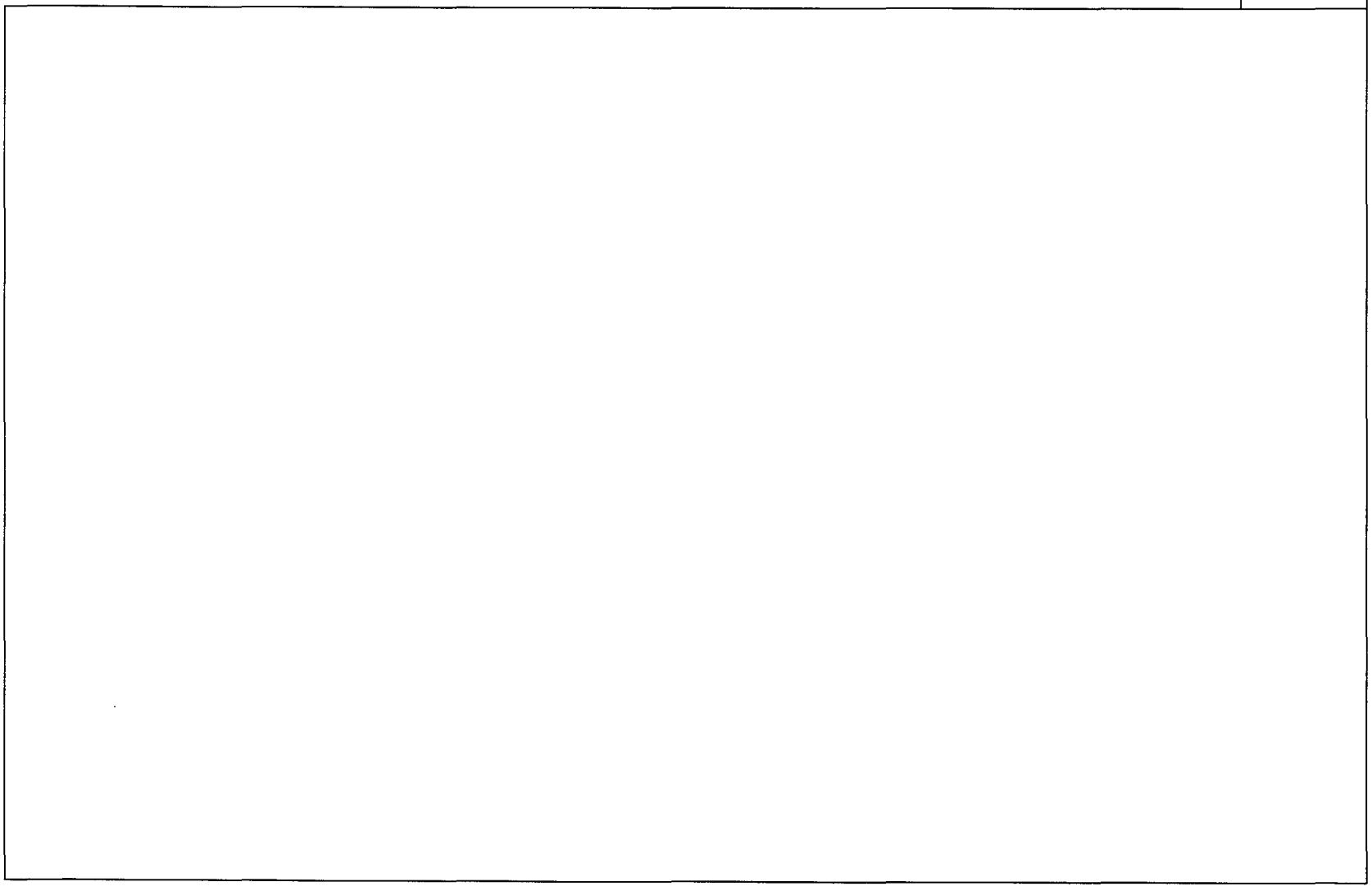
TM is also used with other reactor protection and ESFAS signals, such as Reactor Pressure, Drywell Pressure, and Suppression Pool Water Level.



PCV : Primary Containment Vessel
RPV : Reactor Pressure Vessel
RPS : Reactor Protection System
HPCS : High Pressure Core Spray
RHR : Residual Heat Removal
ECCS : Emergency Core Cooling System

Fig. 3-6 : Trip Module System Configuration

PROPRIETARY



3.3. Characteristics of NRW-FPGA

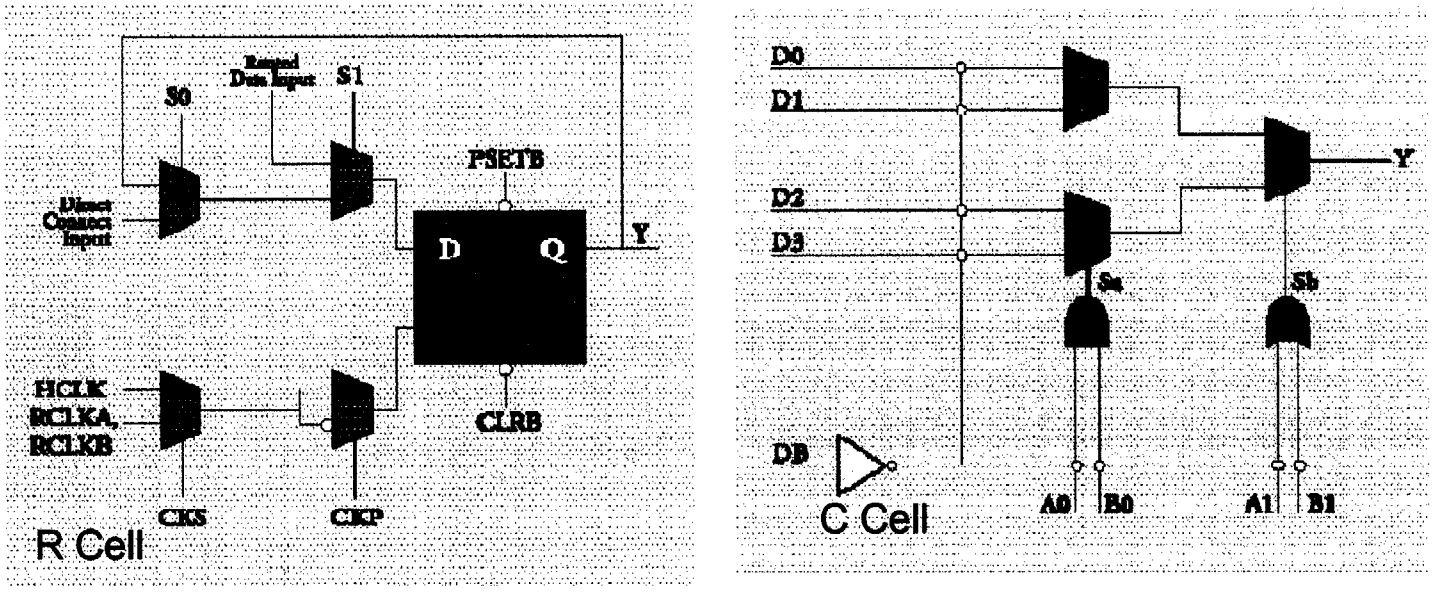
An FPGA consists of logic cells. Application logic will be formed by combining these cells via antifuse. Fig. 3-8 and Fig. 3-9 show the configuration of an FPGA.

However, the procedure for forming required circuits on an FPGA is similar to coding application software. Application logic is developed using a hardware description language (VHDL). The VHDL is converted to an FPGA fuse-map which defines the combination of FPGA cells that optimizes the logic. Application logic is embedded in the FPGA by applying voltages to various combinations of the FPGA connections per the fuse-map. These applied voltages form semiconductor logic cells.

The antifuse type FPGA has the following features:

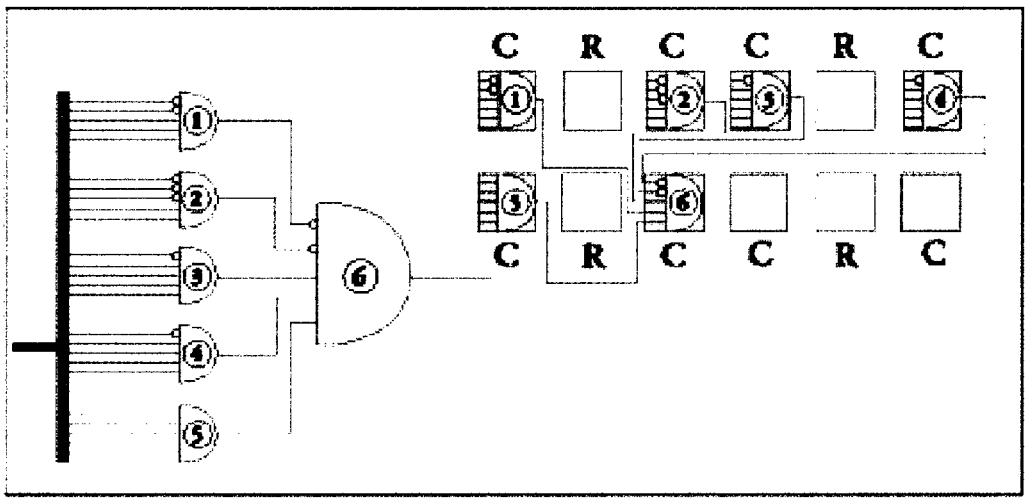
- Non-volatile
- Non-rewritable
- High-speed operation
- Radiation hardened
- Highly reliable
- Current applications include satellites, military, aerospace, aircraft, etc.

Since the FPGA performs processes on digital circuits, the FPGA executes application logic without invoking an operating system or application software. To clarify the above features (especially, non-volatile and non-rewritable), Toshiba has named the FPGA as Non-Rewritable (NRW) FPGA.

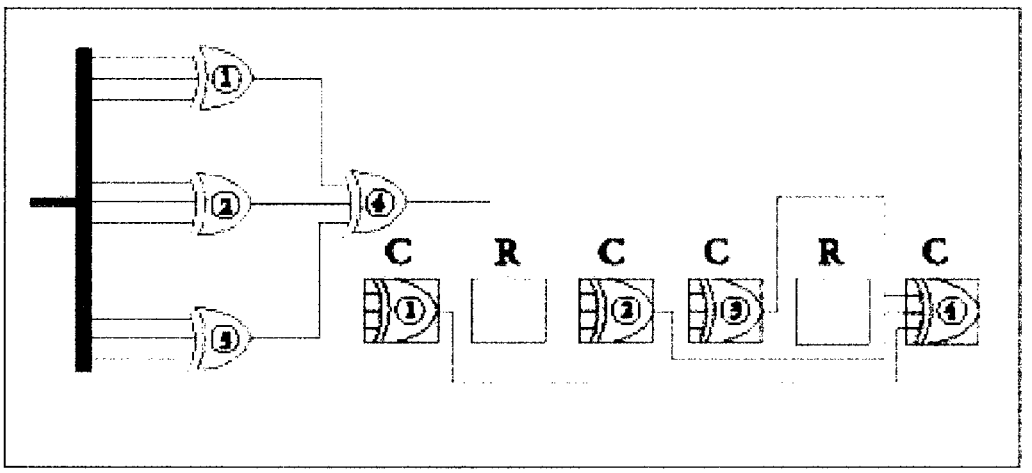


The typical antifuse FPGA consists of logic cells (R cell and C cell). Logic is formed by connecting these cells via an antifuse.

Fig. 3-8 : Typical FPGA Configuration (Reference 13)



24-Bit Address Decoder Example.



9-Bit Parity Generator Example.

Fig. 3-9 : Typical FPGA Configuration (Reference 13)

4. VERIFICATION AND VALIDATION

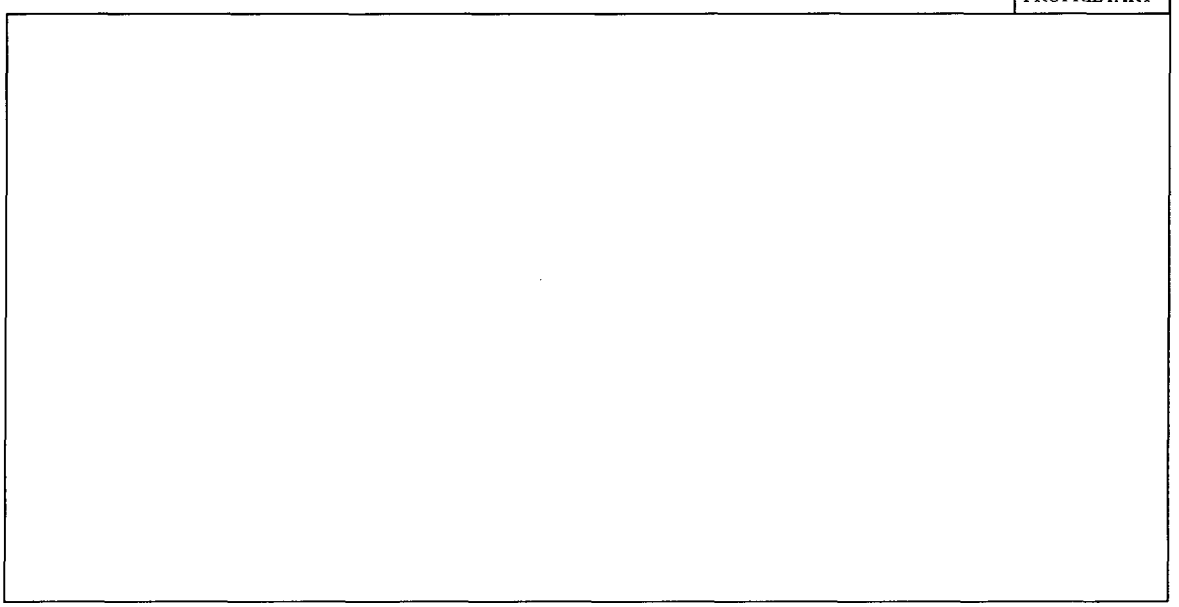
4.1. Assuring Quality of FPGA

4.1.1. Overall Approach

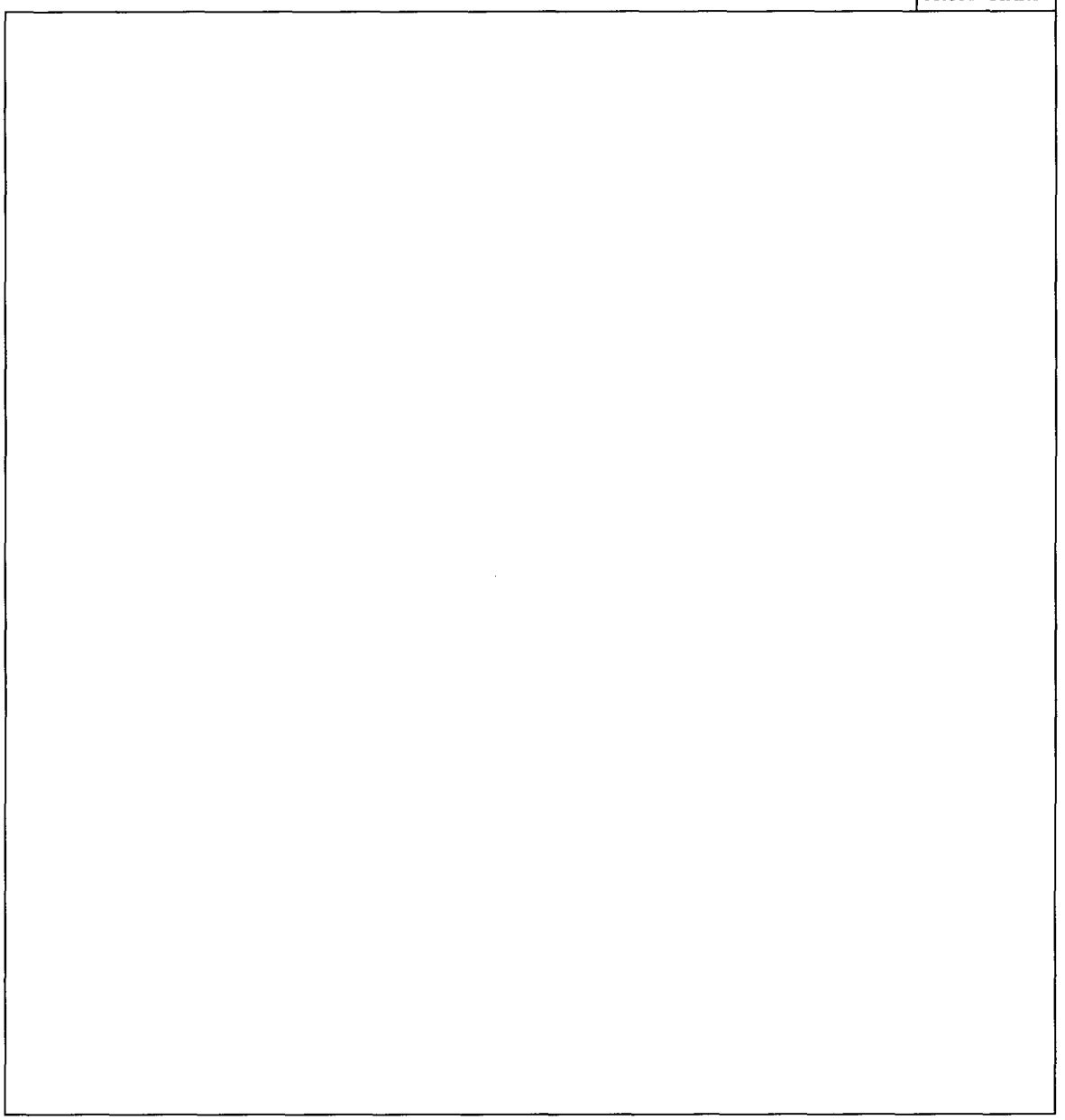
As mentioned in Section 3.3, NRW-FPGA consists of logic cells that are combined to form a digital circuit (hardware). Unlike microprocessor-based systems, neither an operating system nor an application program is used. Therefore, quality assurance of design and manufacture is simpler, since software V&V is only required for developing the logic in VHDL.

The key to software quality assurance is V&V of application logic as it is processed by the design and manufacturing tools. Toshiba will perform V&V of the design and manufacturing processes in a manner equivalent to IEEE 7-4.3.2.

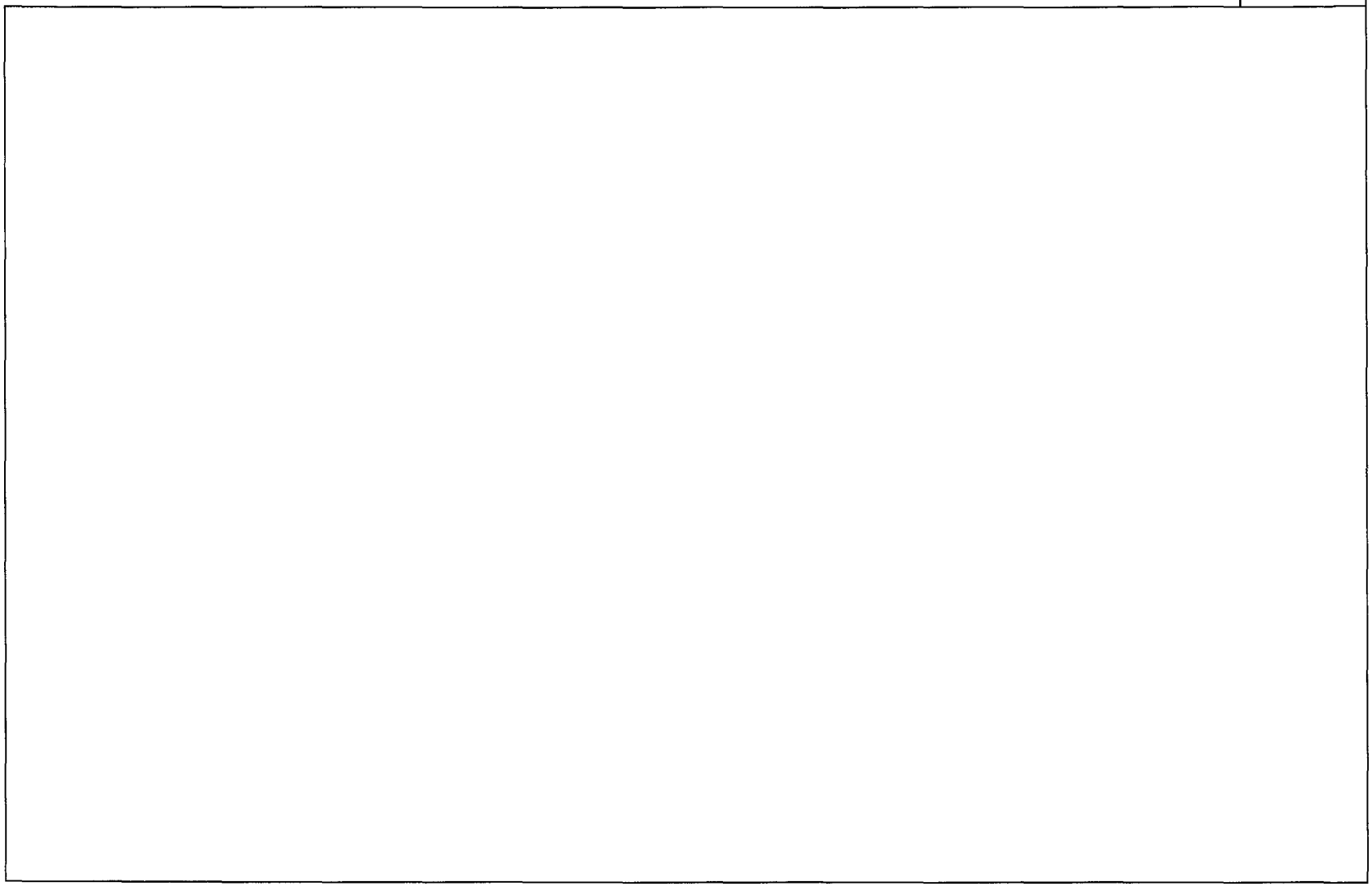
NRW-FPGAs are qualified by V&V and hardware qualification tests described in Section 4, 5 and 6. The qualified modules including NRW-FPGAs are managed by Master Configuration List. In the case that only functions (i.e. VHDL) of NRW-FPGAs are changed, only V&V will be conducted.



PROPRIETARY

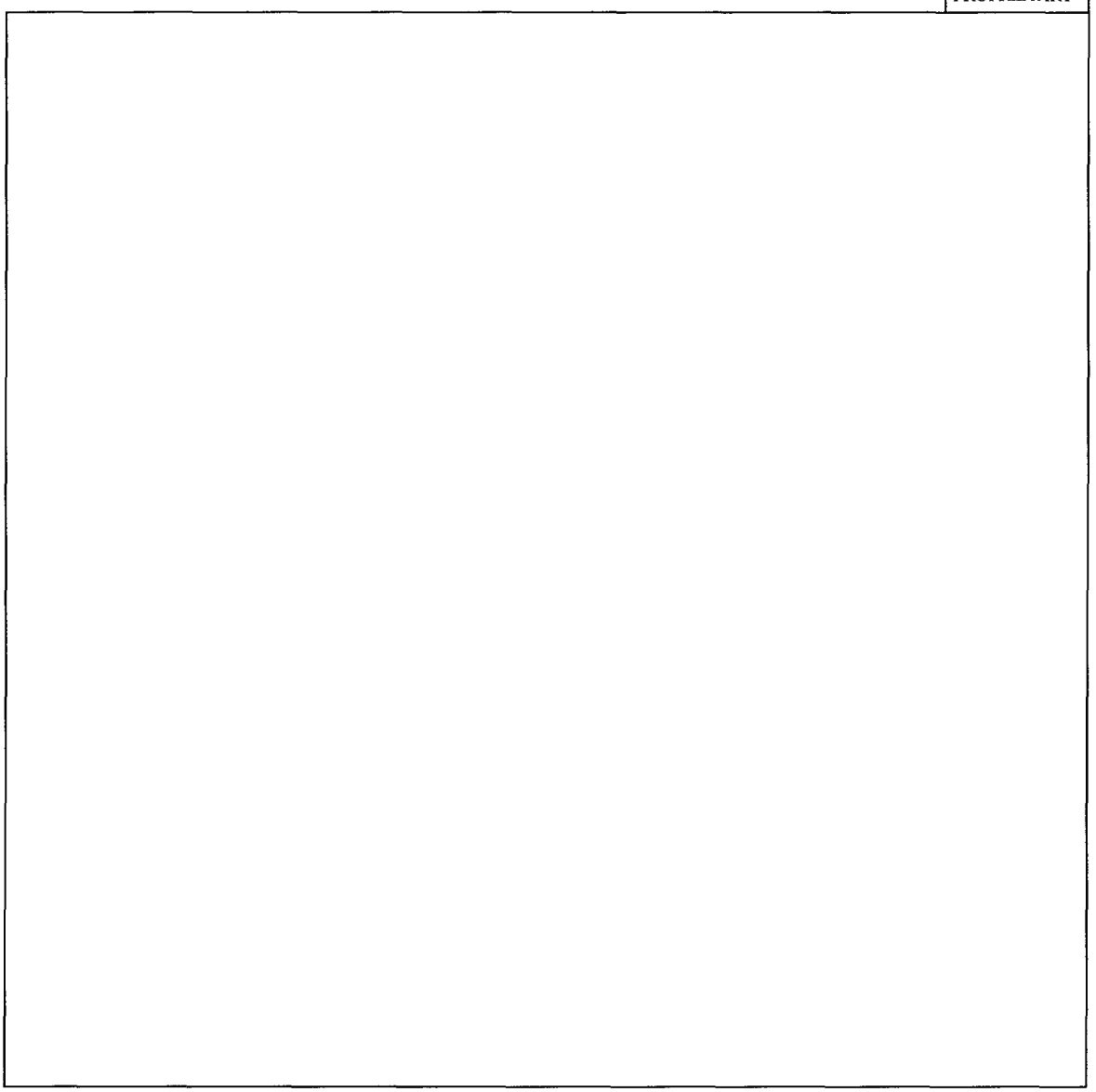


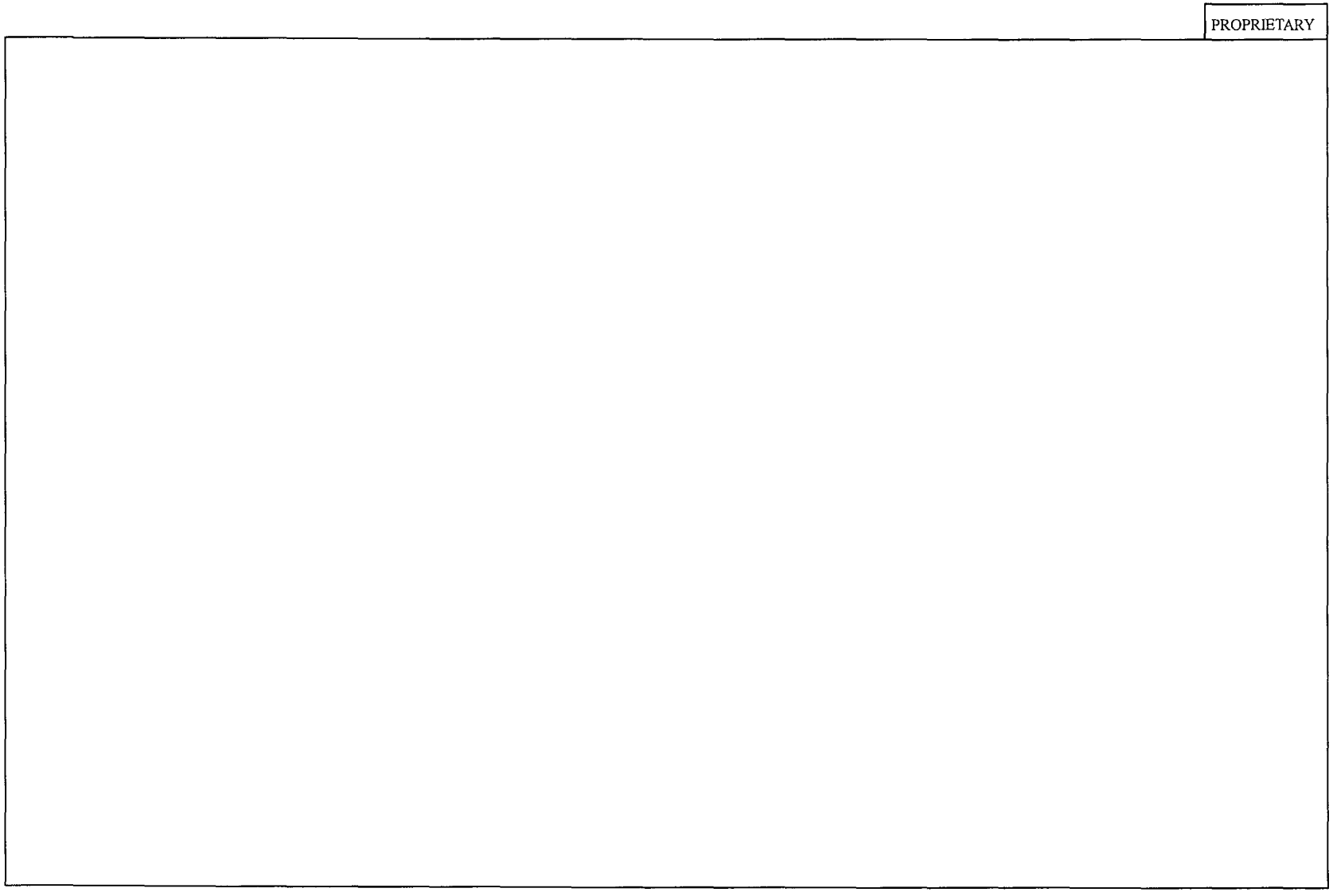
PROPRIETARY



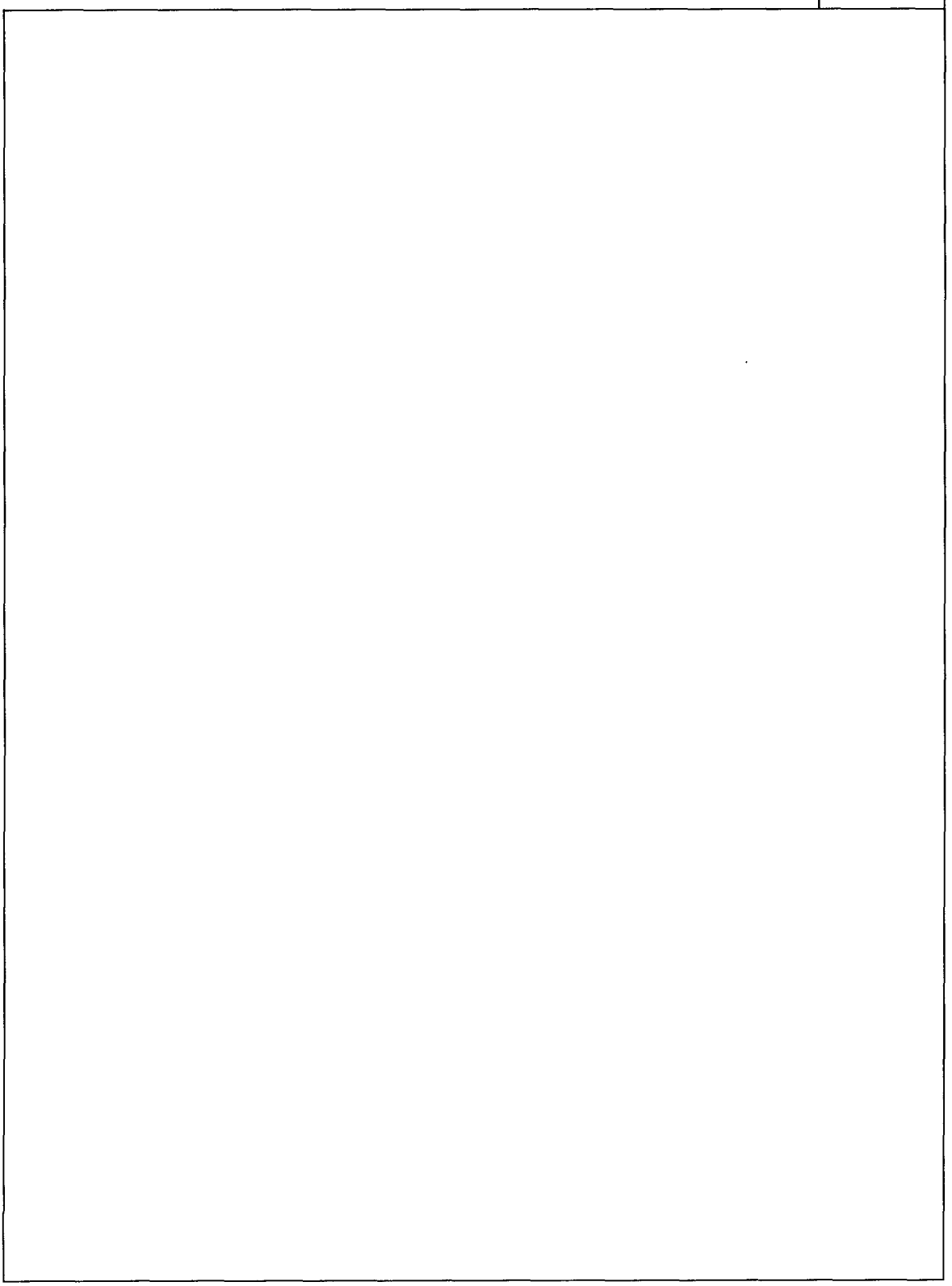
4.2. Design and Manufacturing Process

PROPRIETARY




PROPRIETARY

PROPRIETARY

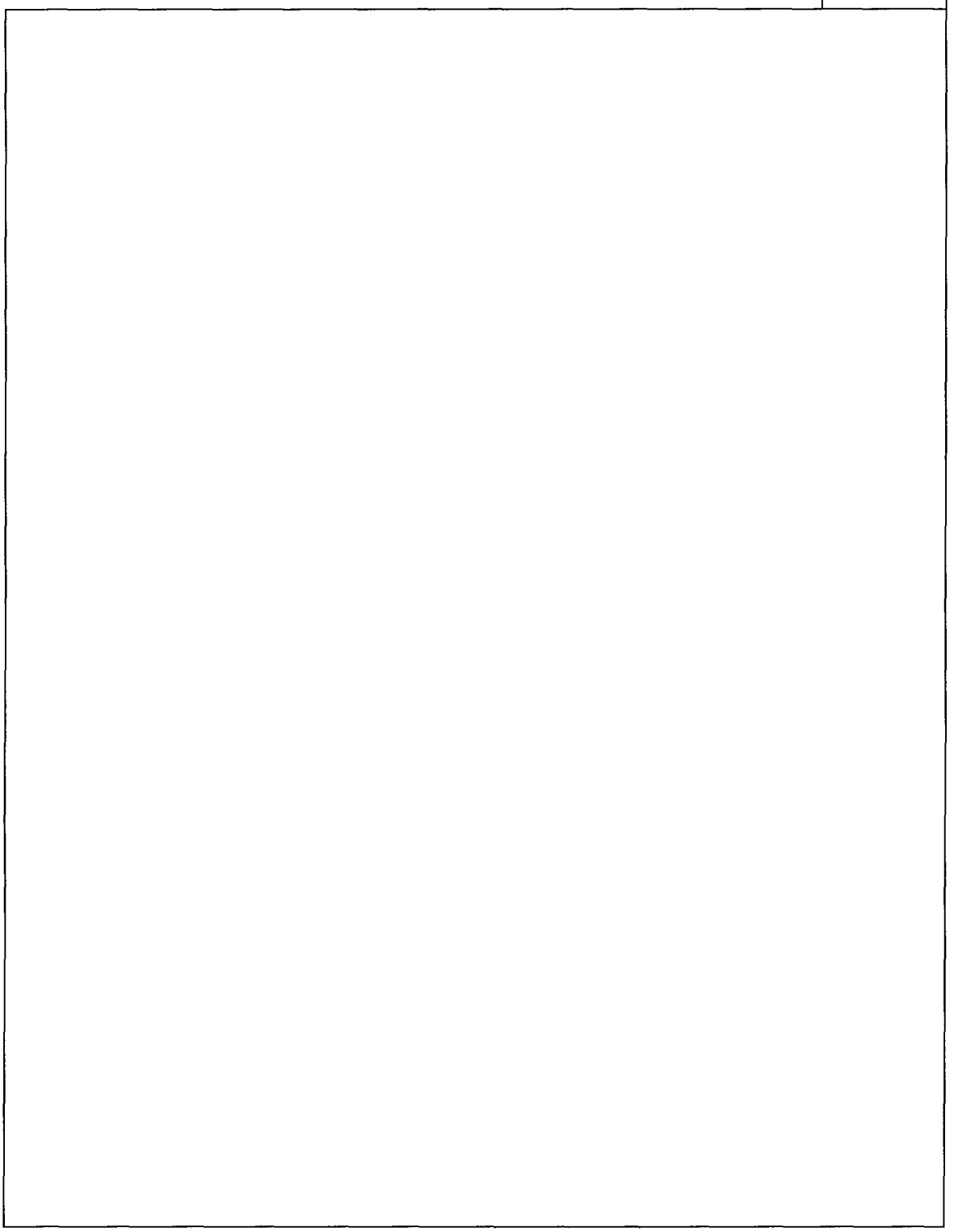


PROPRIETARY

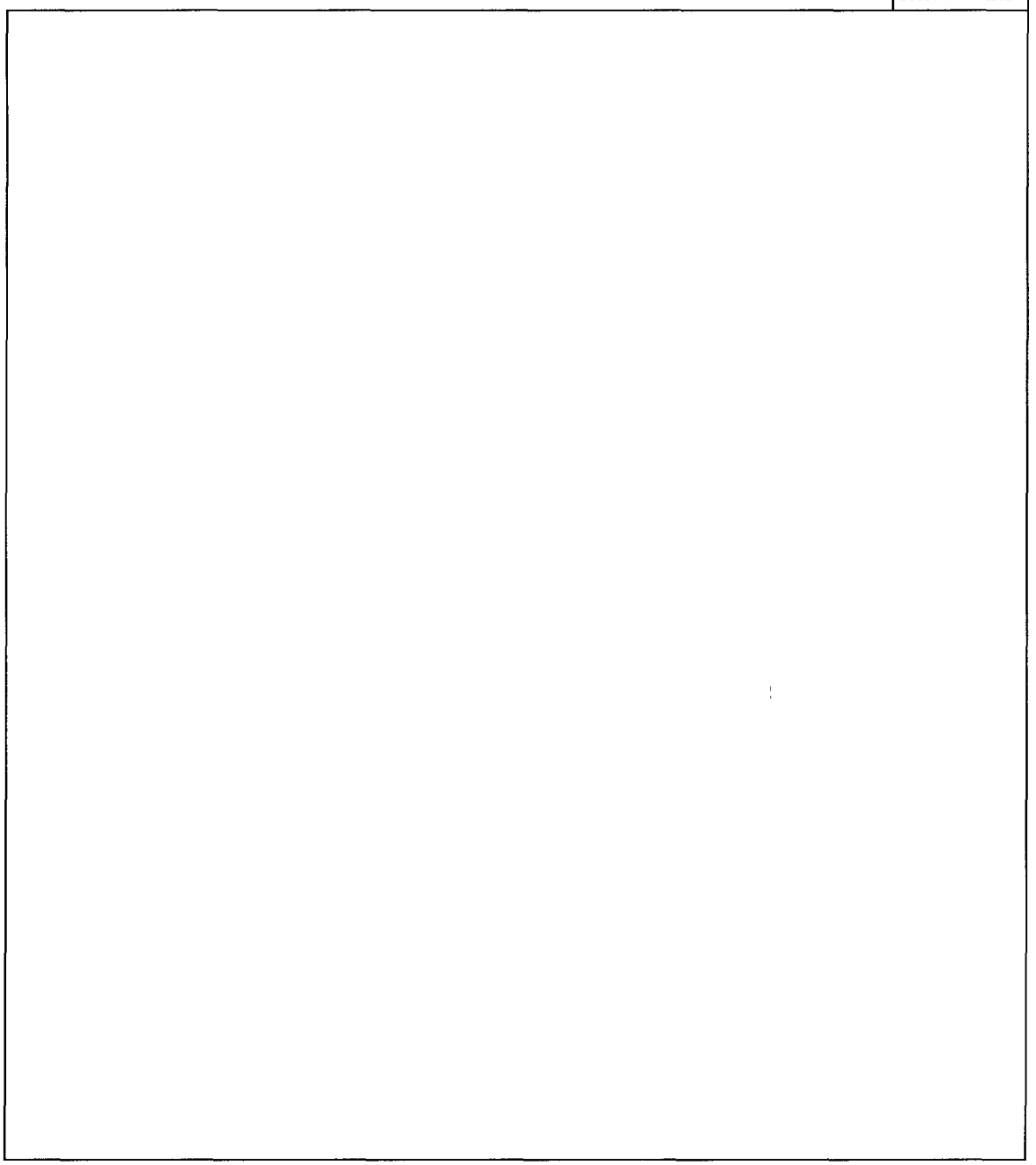
4.3. Verification

PROPRIETARY

PROPRIETARY



PROPRIETARY



4.3.3. Verification of coded VHDL and manufactured FPGA

4.3.3.1. Activities Outline

Fig. 4-4 is the V&V process given in of the publication of IEEE7-4.3.2 Annex E, with abbreviated names for each step.

PROPRIETARY

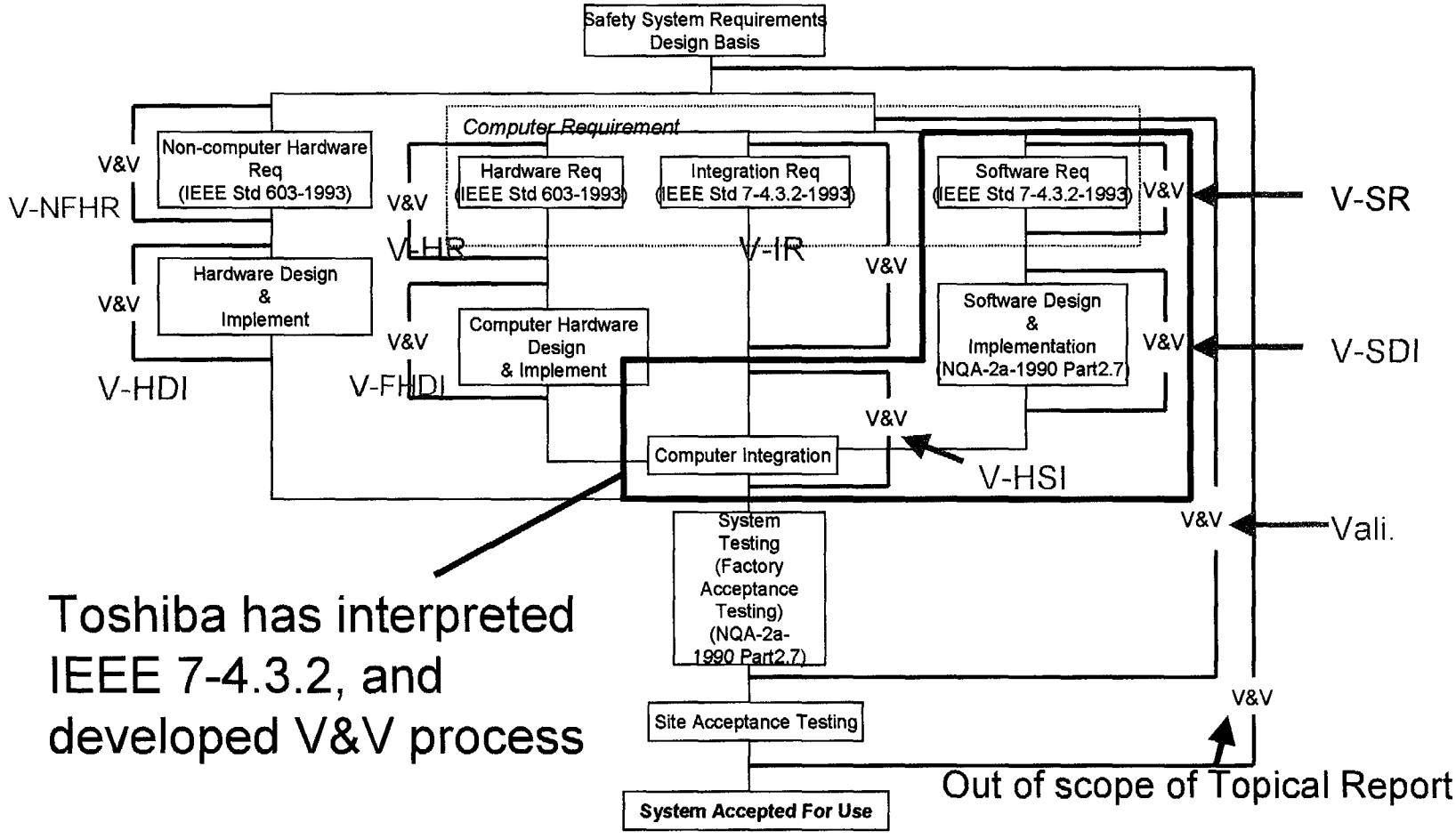
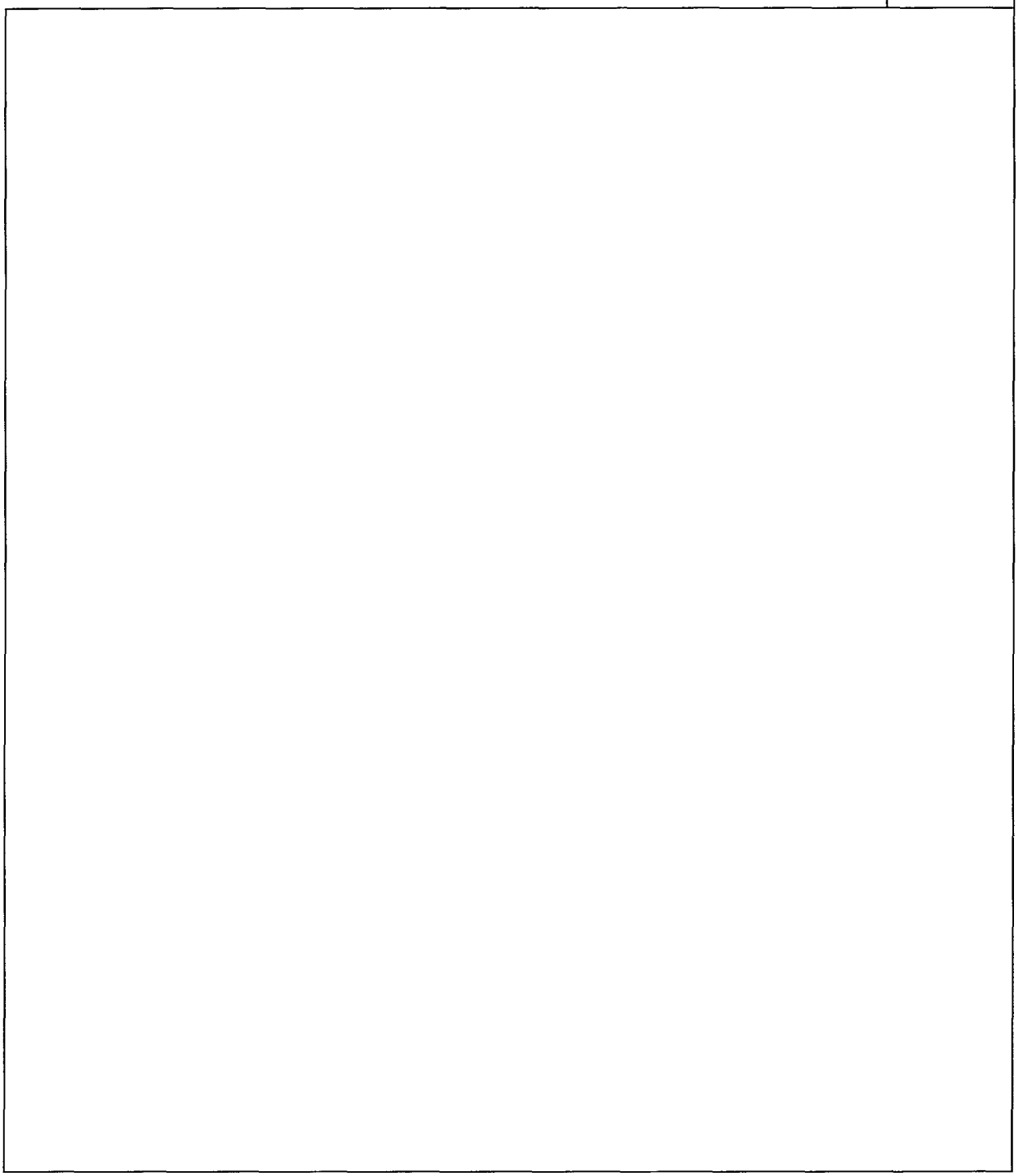
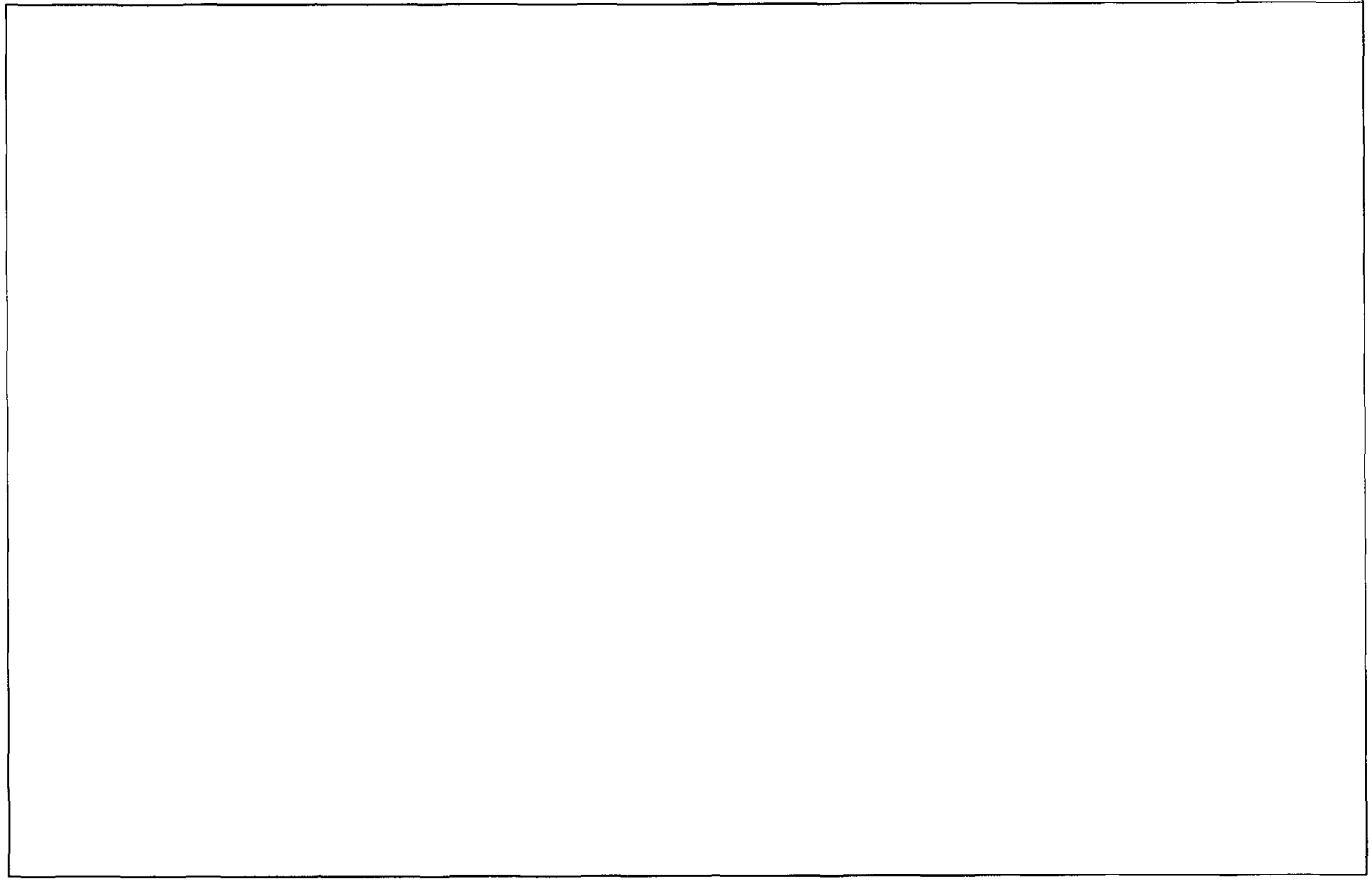


Fig. 4-4： V&V for FPGA-based System

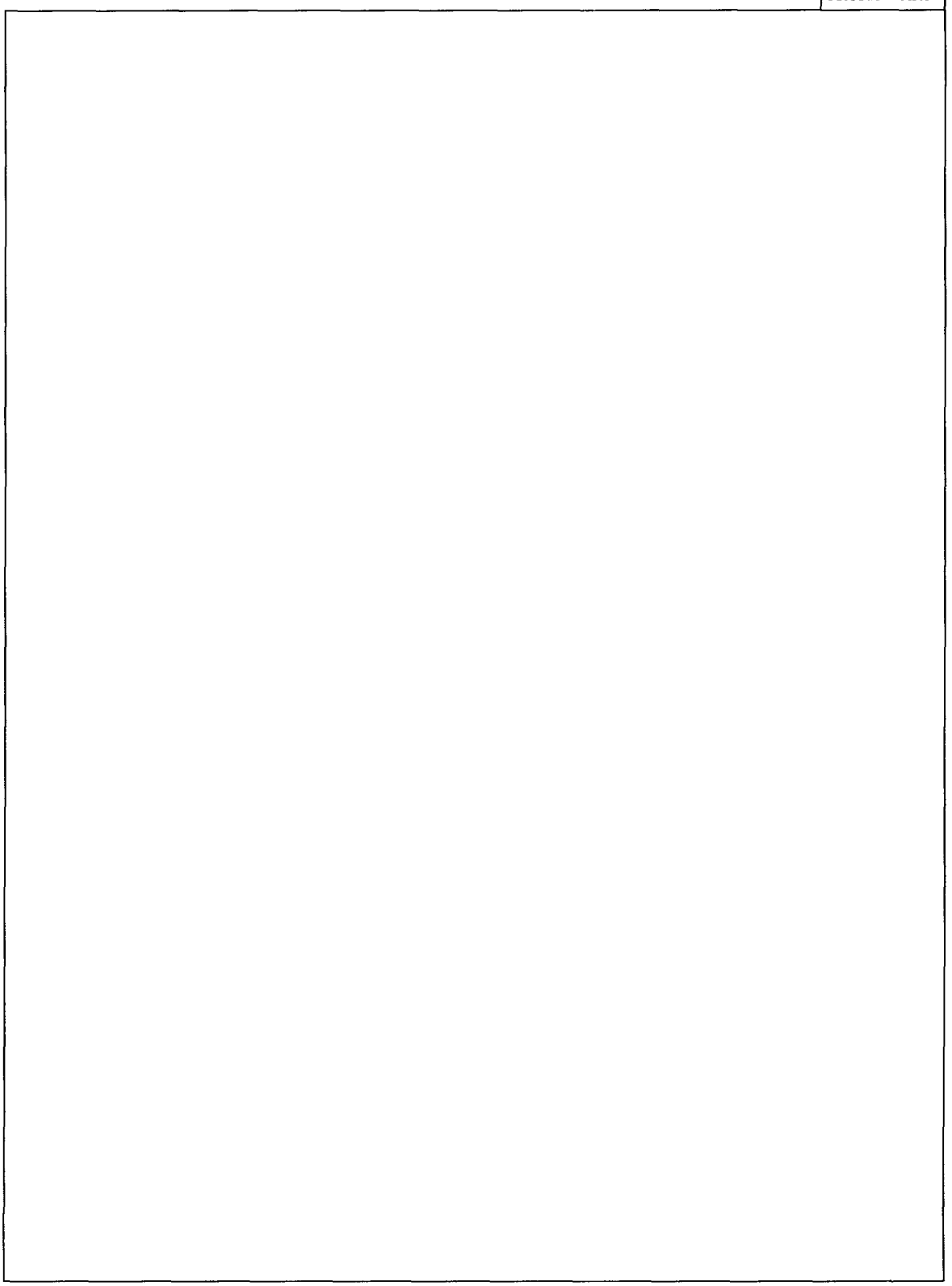
PROPRIETARY



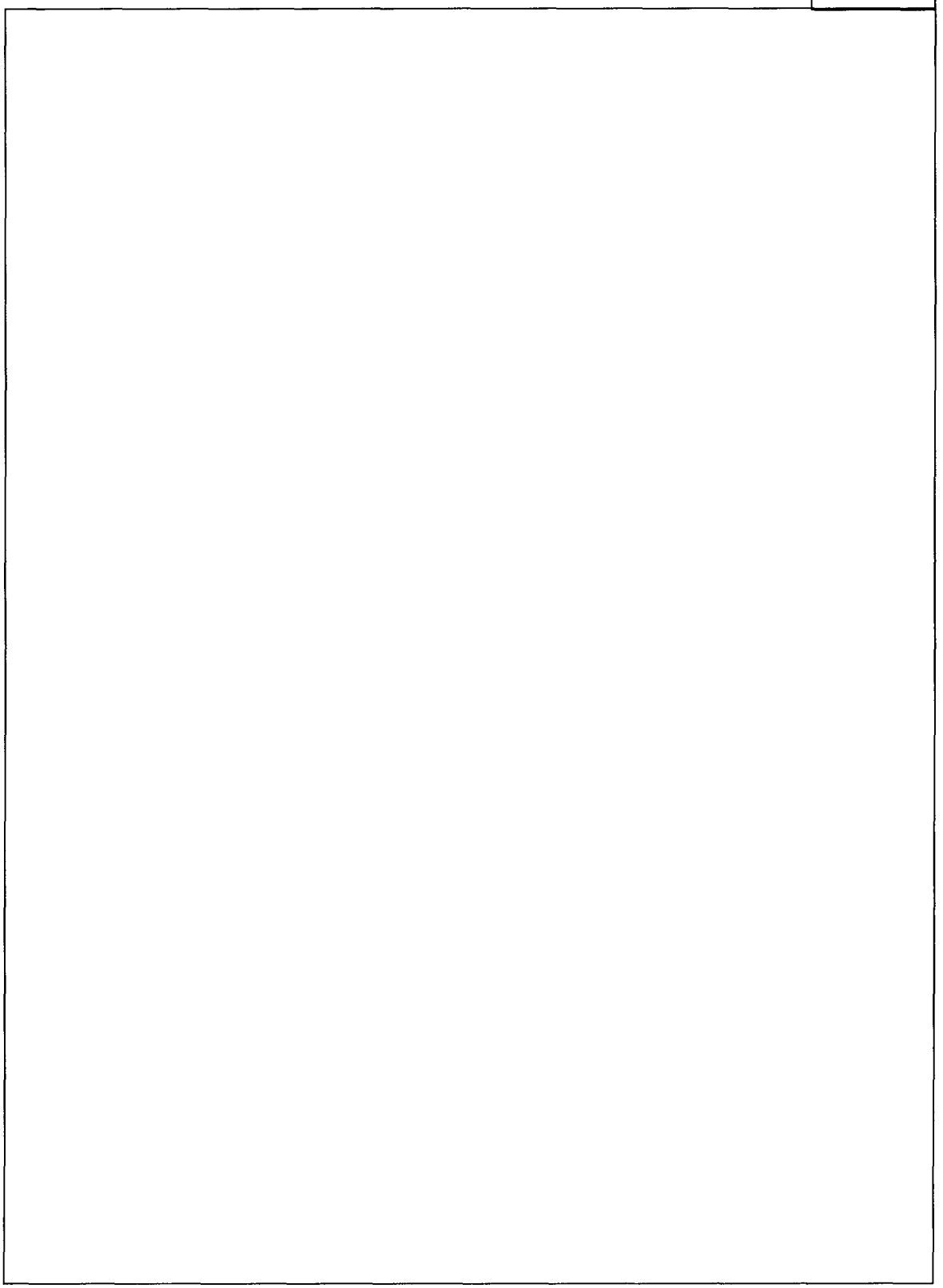
PROPRIETARY



PROPRIETARY



PROPRIETARY



PROPRIETARY

4.4. Validation Test

PROPRIETARY

4.5. V&V Results

PROPRIETARY

5. Qualification Process

This section describes the activities to be performed as part of the FPGA-based qualification testing. Fig.5-1 shows the flow diagram of the pre-qualification test, the qualification test, and the post-qualification test.

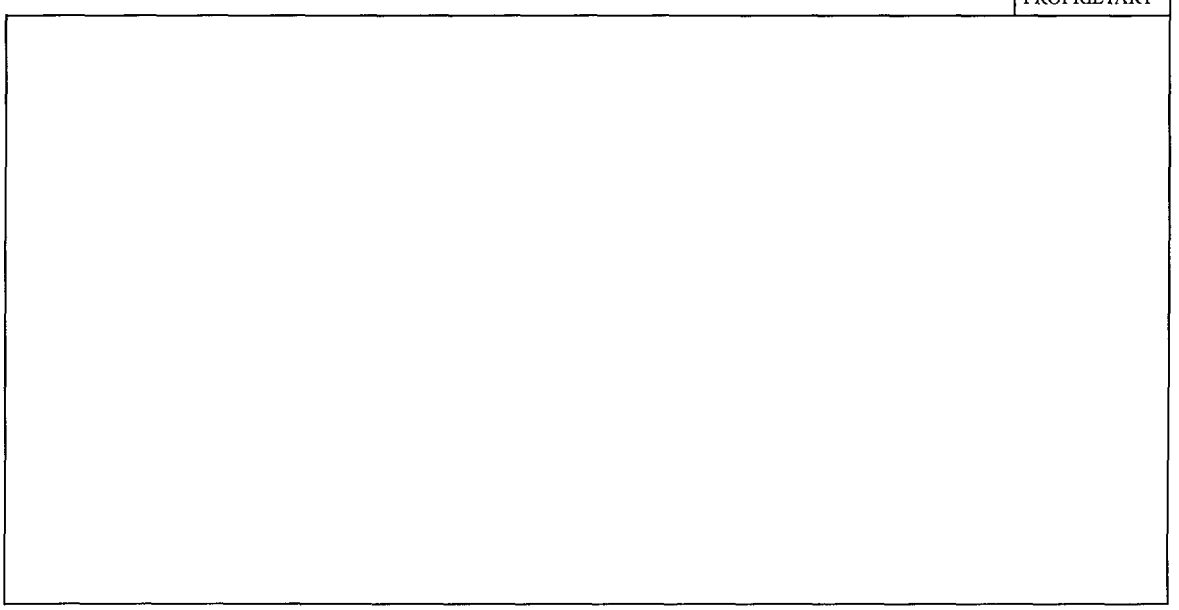
5.1. PRE-QUALIFICATION TESTS

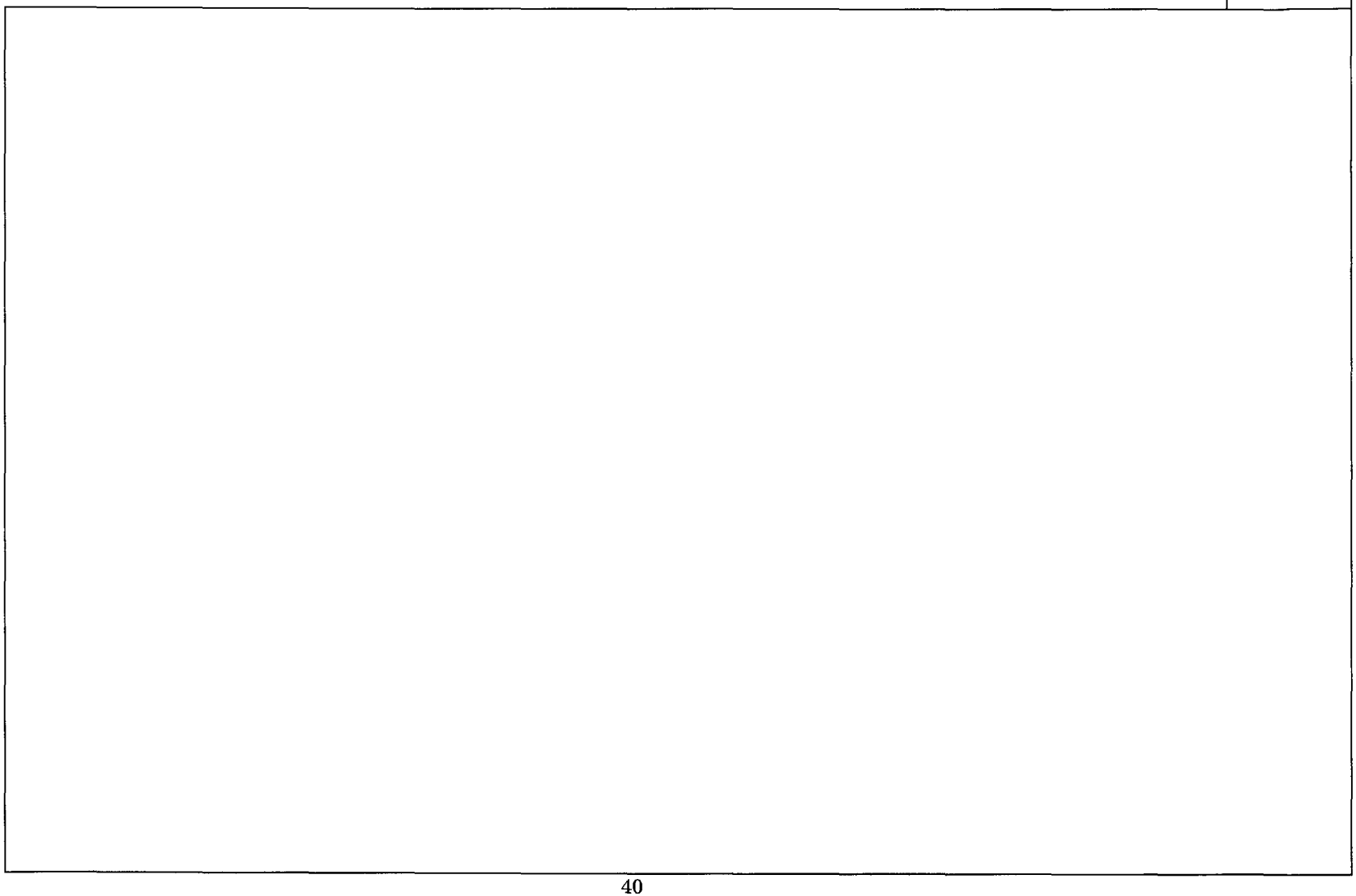
The pre-qualification tests are performed on the assembled qualified test system prior to start of qualification test to verify proper assembly, integration, operation and performance of the system.

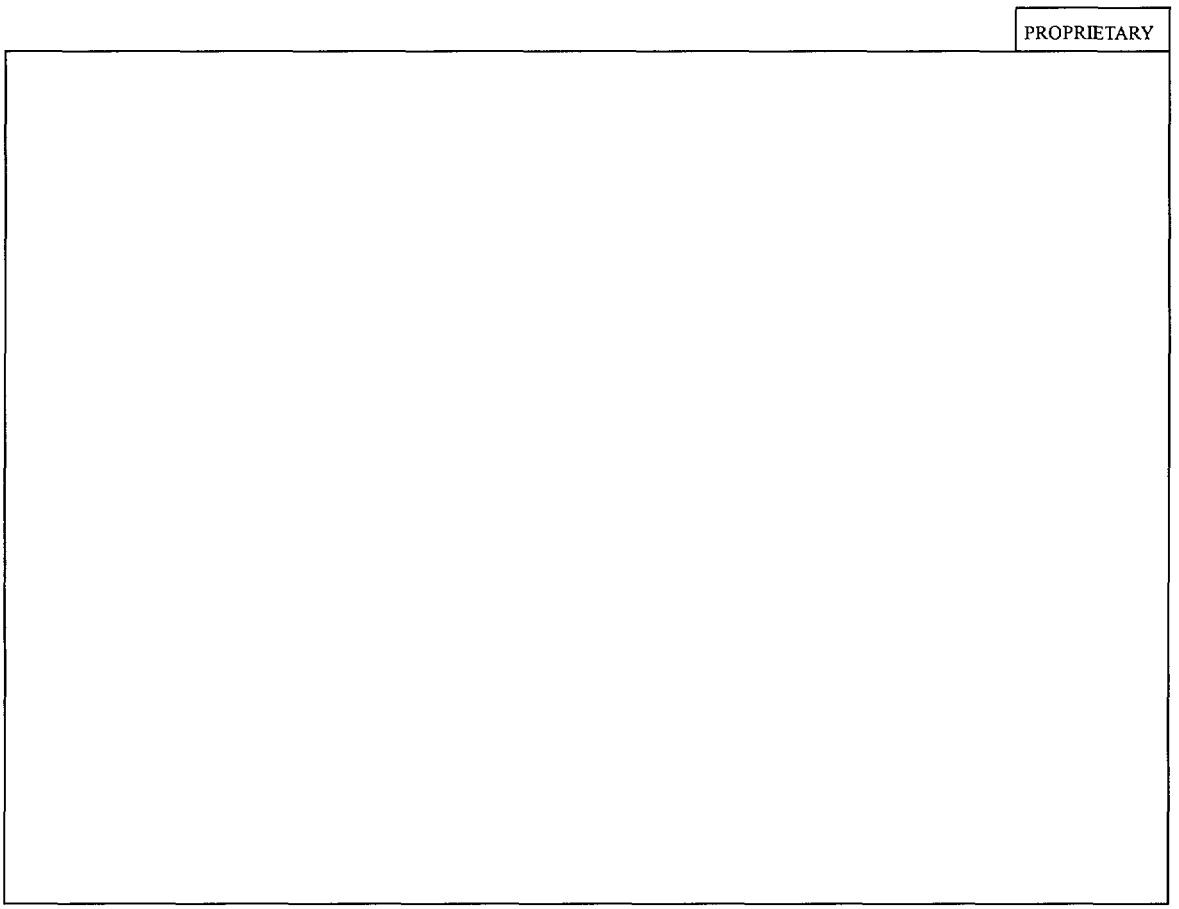
Prior to the pre-qualification test, a test system or specimen is assembled to represent the hardware and software functionality of the FPGA. The test specimen is a panel with one LPRM unit, one LPRM/APRM unit, two Recirculation Flow Measurement Units, one RBM Unit and one Relay Unit, which represents the PRM System.

The modules for the test specimen are individually manufactured and tested.
Fig.5-2 shows the test specimen, the signal simulation system and the data acquisition system.

PROPRIETARY






PROPRIETARY

5.1.1. Outline

This section describes the initial activities that will be performed as part of the FPGA-based generic qualification testing.

The pre-qualification test is carried out after setup of the test system to provide the baseline performance and to check the correct setup. The pre-qualification test requirements are indicated in section 5.2 in TR-107330.
The equipment with NRW-FPGA has no application software objects for test.

The pre-qualification tests are performed as shown below.

(1) System Set-up and Check-out Test. This test will verify proper assembly, integration and operation of the assembled qualification test system. All parameters and switches of each module of the test specimen will be set or confirmed after the system setup. Following system setup, the system will be calibrated to a traceable source.

(2) Operability Test. This test will be performed to establish baseline performance and to verify the test procedures.

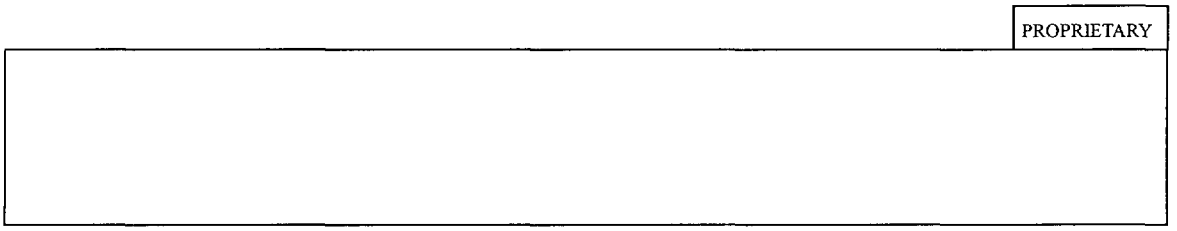
(3) Prudency Test. This test will be performed to establish baseline performance and to verify the test procedures.

(4) Burn-in Test. A burn-in test will be carried out on the test specimen.

A description of pre-qualification test activities, including test methods to be used, reference to applicable industry standards, test levels to be applied, arrangement and mounting of the test system, configuration of test system power monitoring, test instrumentation to be used, and monitoring of the system during testing will be provided later.

5.1.2. Results

PROPRIETARY



6. QUALIFICATION TEST

This section provides a description of qualification test activities, including test method to be used, reference to applicable industry standards, test levels to be applied, arrangement and mounting of the test system, configuration of test system power monitoring, test instrumentation to be used, monitoring of the system during testing, and the test acceptance criteria. Fig.5-1 summarizes the qualification test to be performed.

6.1. ENVIRONMENTAL TEST

6.1.1. Outline

The Environmental Test is carried out to verify that the TOSHIBA NRW-FPGA system provides the required performance in normal and abnormal environmental conditions.
The test requirements are indicated in section 6.3 of EPRI TR-107330.
The environmental test is performed as shown below.

(1) Temperature
(2) Humidity
(3) Power Source
(4) Radiation

The conditions of temperature and humidity exposure of the test specimen during in the environmental test are shown in Figure 4-4 of EPRI TR-107330.
Radiation exposure is also required for the aging evaluation in section 4.3.6.1 of EPRI TR-107330. Gamma irradiation for TOSHIBA NRW-FPGA equipment up to 10 Gy will be performed.

6.1.2. Results

PROPRIETARY

6.2. EMI/RFI TEST

6.2.1. Outline

The EMI/RFI Test is carried out to verify that the TOSHIBA NRW-FPGA system withstands the EMI/RFI levels given in EPRI TR-702323.
The tests will be performed according to sections 4.3.7 and 6.3.2 of EPRI TR-107330. EPRI TR-107330 refers to TR-102323.

The EMI/RFI susceptibility and emissions withstand capability will be tested as follows.

(1) Radiated susceptibility per TR-102323 Appendix B.
(2) Conducted susceptibility per TR-102323 Appendix B.
(3) Radiated emissions per TR-102323 section7.
(4) Conducted emissions per TR-102323 section7.

6.2.2. Results

PROPRIETARY

6.3. SURGE TEST

6.3.1. Outline

The Surge Test is carried out to verify that the TOSHIBA NRW-FPGA system withstands the surge levels given in section 4.6.2 of EPRI TR-107330.
The tests will be performed according to EPRI TR-107330 and IEEE C62.41

6.3.2. Results

PROPRIETARY

6.4. CLASS 1E/Non-1E ISOLATION TEST

6.4.1. Outline

The Class 1E/Non-1E Isolation Test is carried out to verify that the TOSHIBA NRW-FPGA system provides the isolation capability required for class 1E to non class 1E connections of the instrumentation and control system given in EPRI TR-107330 and IEEE 384 (Reference 3.1.3.4).

6.4.2. Results

PROPRIETARY

6.5. ELECTROSTATIC DISCHARGE (ESD) TEST

6.5.1. Outline

The ESD Test is carried out to verify that the TOSHIBA NRW-FPGA system provides the ESD withstand capability required in EPRI TR-102323 (Reference 3.1.3.4).

The tests will be performed according to sections 4.3.8 and 6.4.2 of EPRI TR-107330 and section 3.5 of Appendix B of TR-102323.
TR-102323 also refers to IEC Standard 801-2 and IEC6100-4-2.
IEC6100-4-2 provides the test voltage level on the contact and non-contact electric discharge.

6.5.2. Results

PROPRIETARY

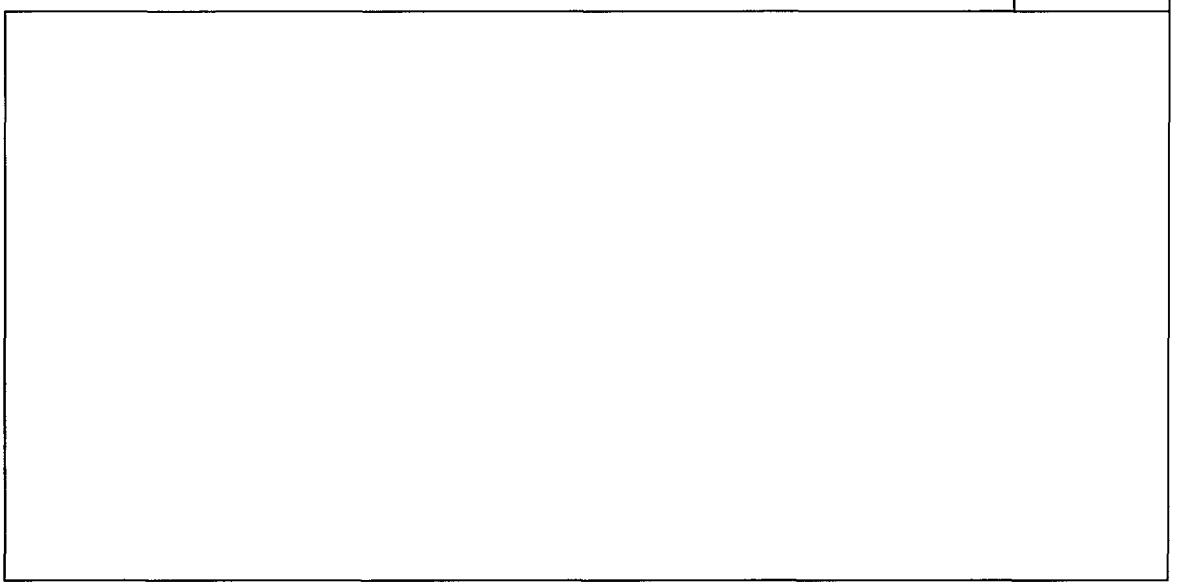
6.6. SEISMIC TEST

6.6.1. Outline

The Seismic Test is carried out to verify that the TOSHIBA NRW-FPGA system provides the seismic withstand capability required of a Seismic Category 1 Safety System.

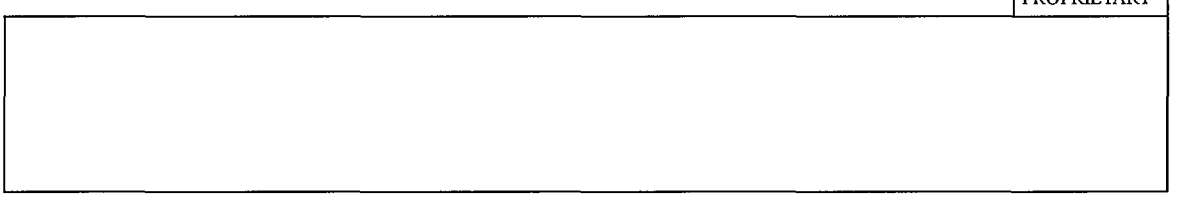
The tests will be performed according to sections 4.3.9 and 6.4.3 of EPRI TR-107330.
TR-107330 also refers to IEEE-344 (Reference 3.1.3.3) and the SQRTS specifications.

PROPRIETARY



6.6.2. Results

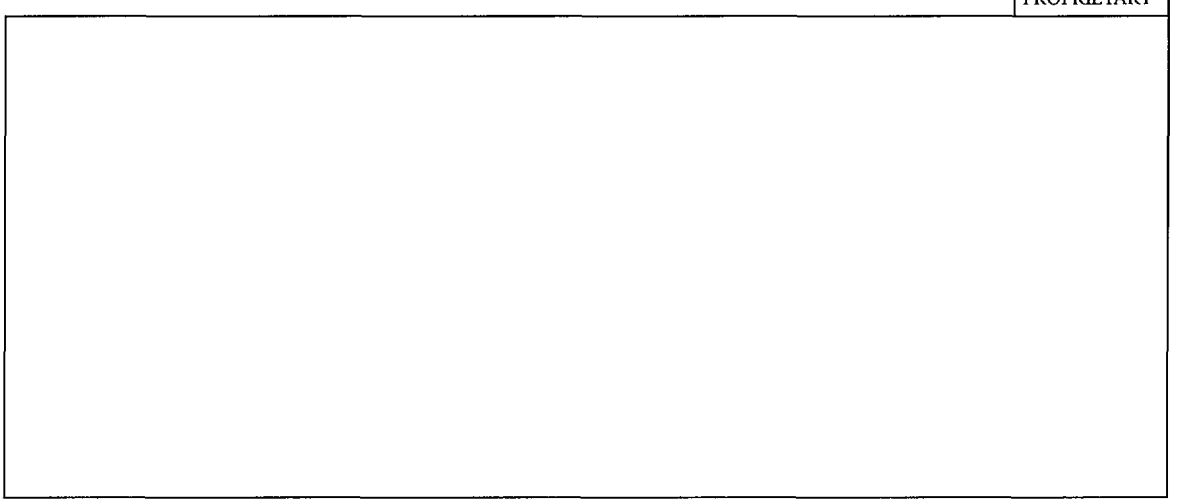
PROPRIETARY



6.7. PERFORMANCE PROOF TEST

6.7.1. Outline

PROPRIETARY



PROPRIETARY

6.7.2. Results

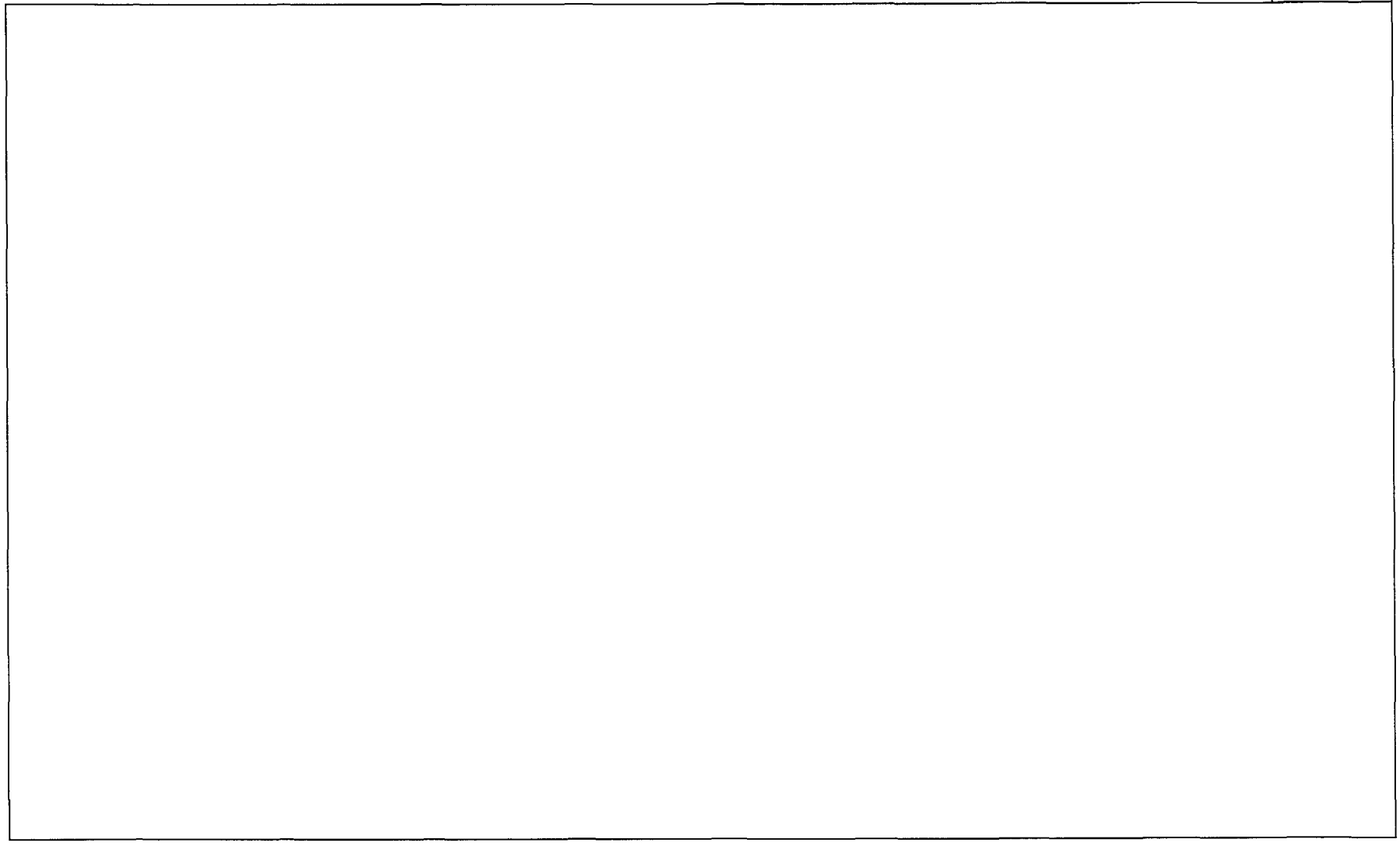
PROPRIETARY

6.8. POST-QUALIFICATION TESTS

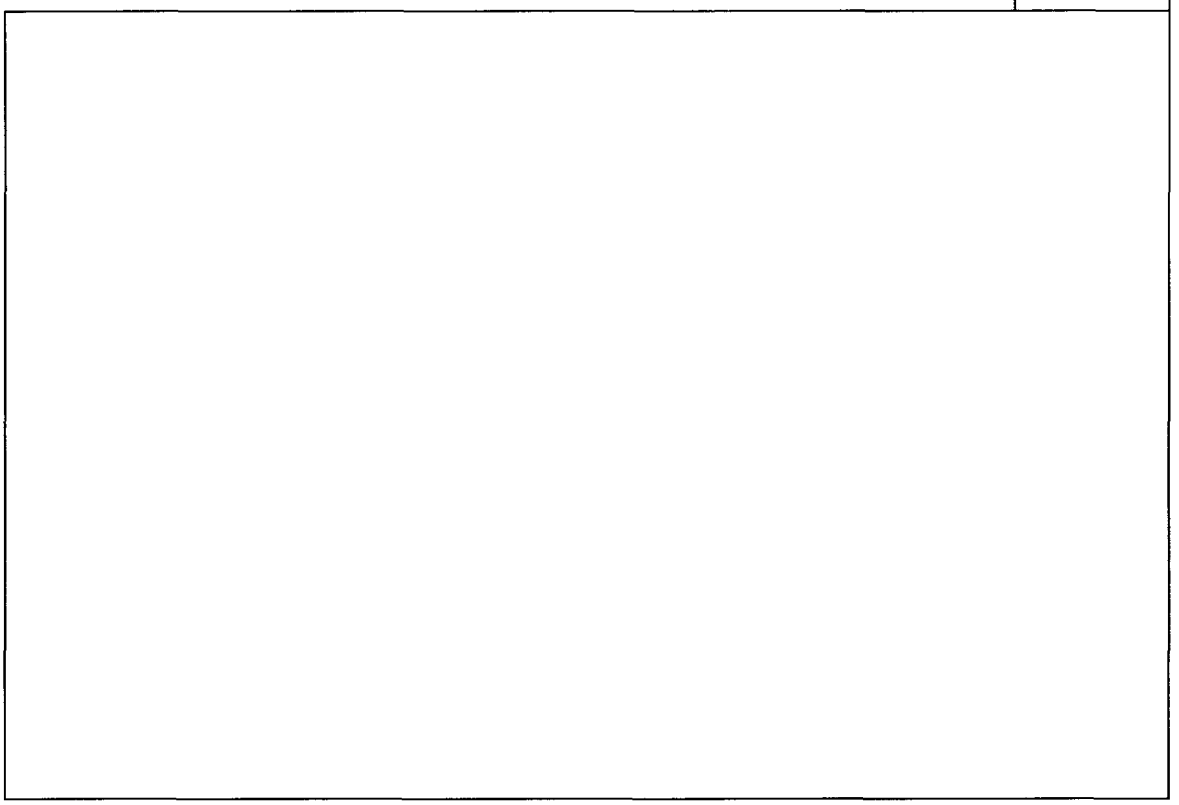
PROPRIETARY

7. SAFETY ANALYSIS

PROPRIETARY



PROPRIETARY



8. REFERENCES

1. NUREG-800; Standard Review Plan, Section 7.0, "Instrumentation and Controls - Overview of Review Process," Rev. 4- June 1997
2. NUREG/CR-6812, "Emerging Technologies in Instrumentation and Controls" March 2003
3. EPRI Report TR-107330, "Generic Requirements Specification for Qualifying Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants."
4. EPRI Report TR-106339, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications~~
5. EPRI Report TR-102323-R2, "Guidelines for Electromagnetic Interference Testing in Power Plants"
6. IEEE Std. 323-1983, "Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations"
7. IEEE Std. 344-1987, "Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations"
8. IEEE Std. 381-1977, "Standard Criteria for Type Tests of Class 1E Modules Used in Nuclear Power Generating Stations"
9. IEEE Std. 384-1981, "WEE Standard Criteria for Independence of Class 1E Equipment and Circuits"
10. IEC 801-5, January 1990, "Electromagnetic Compatibility for Industrial Process Measurement and Control Equipment, Part 5— Surge Immunity Requirements"
11. IEEE Std. 7-4.3.2-1993, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations"
12. IEEE Std. 1012-1986, "IEEE Standard for Software Verification and Validation Plans"
13. Actel Corporation, Actel's SX Family of FPGAs: A New Architecture for High-Performance Designs, April, 1998. http://www.actel.com/products/sxa/docs/SXbkgrndr.pdf
14. John Knight, "Glitches and Hazards in Digital Circuits"
15. Chris J. Myers, "CS/EE 3700: Fundamentals of Digital System Design"

APPENDIX A

EPRI TR-107330
REQUIREMENTS COMPLIANCE AND TRACEABILITY MATRIX

(This section will be provided later.)

APPENDIX B

APPLICATION GUIDE

(This section will be provided later.)

APPENDIX C

SUPPLEMENTAL MATERIAL

1. INTRODUCTION

This document provides the following contents:

- Supplemental Information of the Topical Report
- Responses to NRC's comments

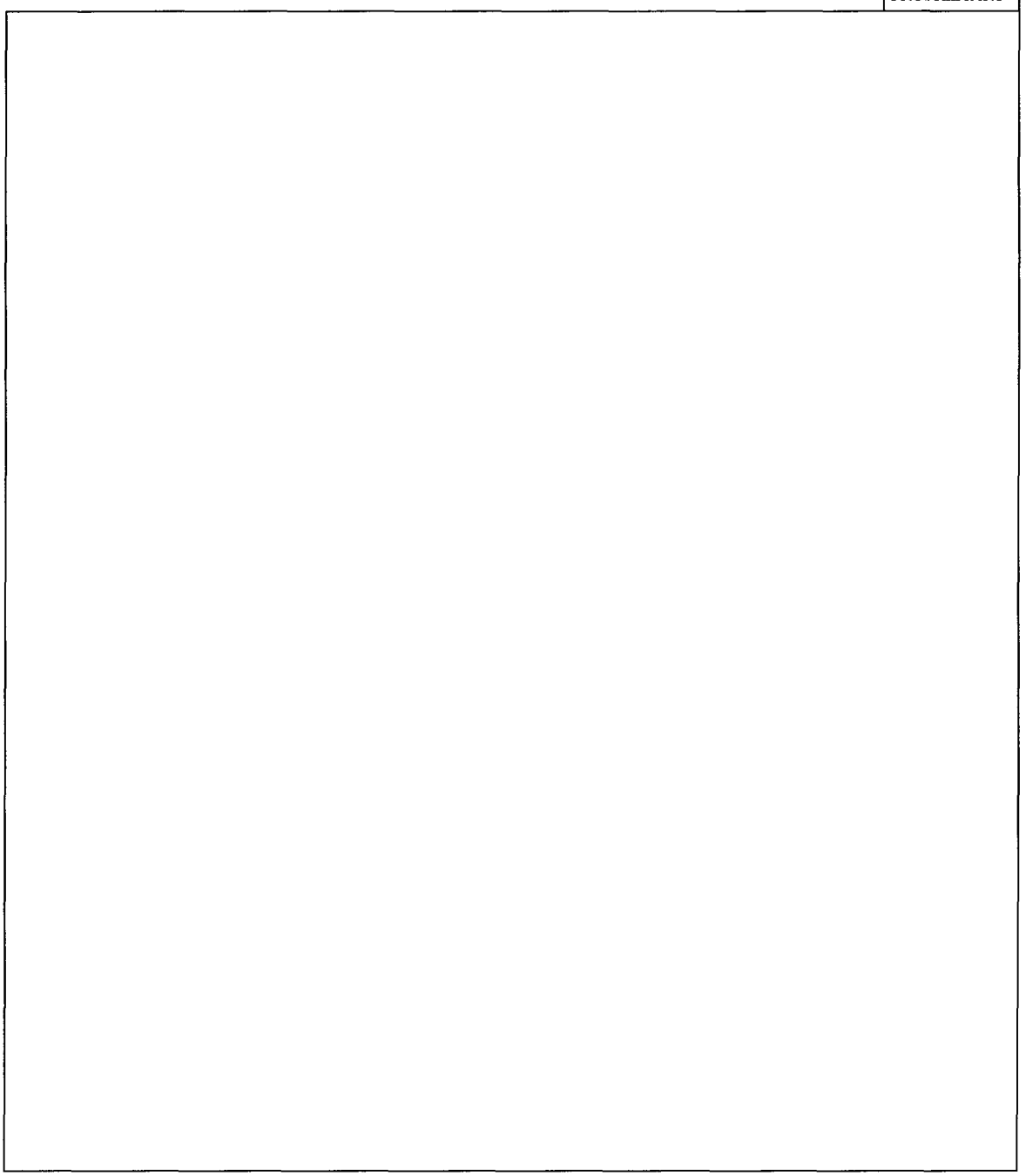
2. REFERENCE

1. "Topical Report of Generic Qualification Program for FPGA-Based Safety-Related I&C Systems"

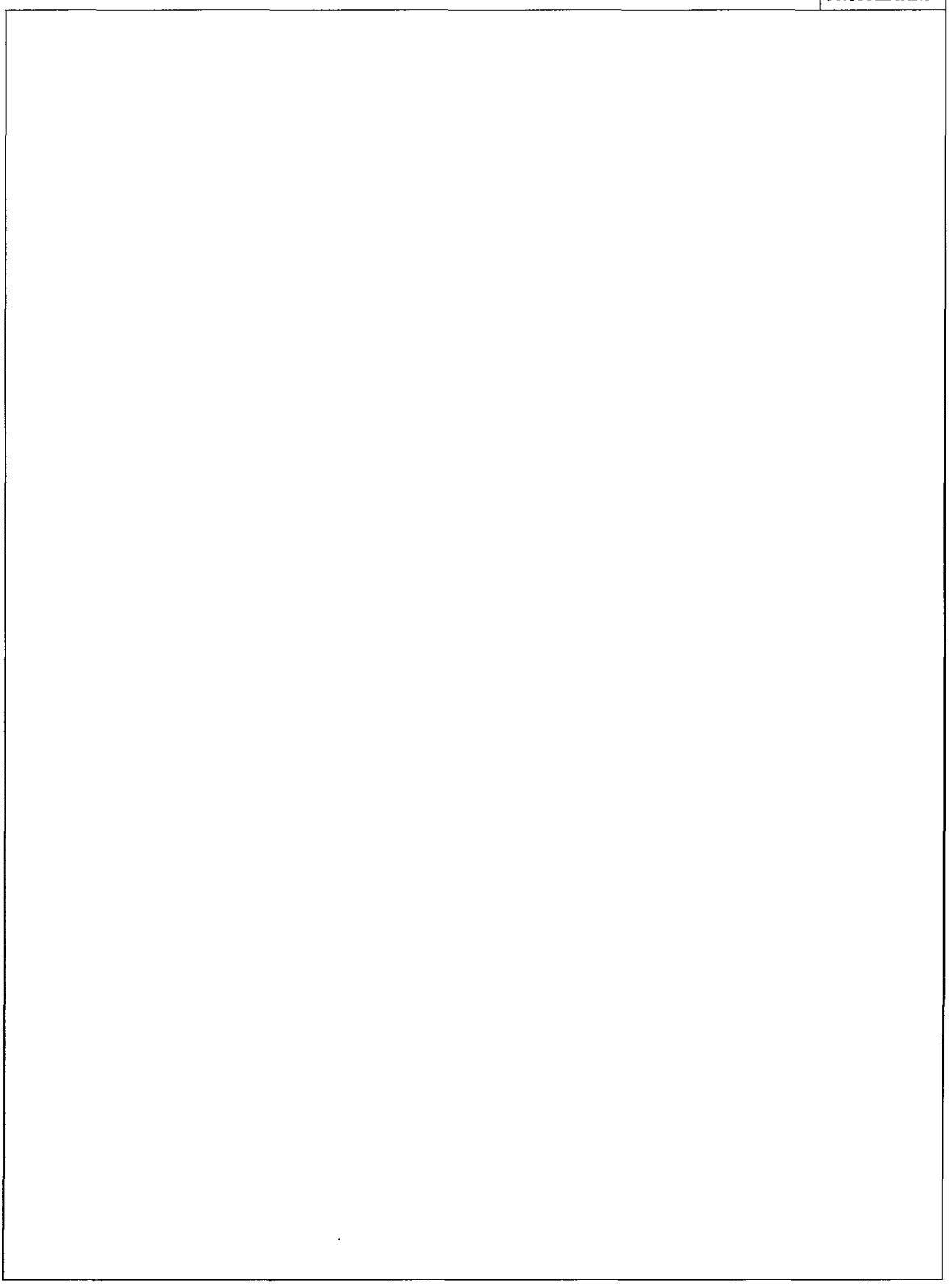
3. Contents

PROPRIETARY

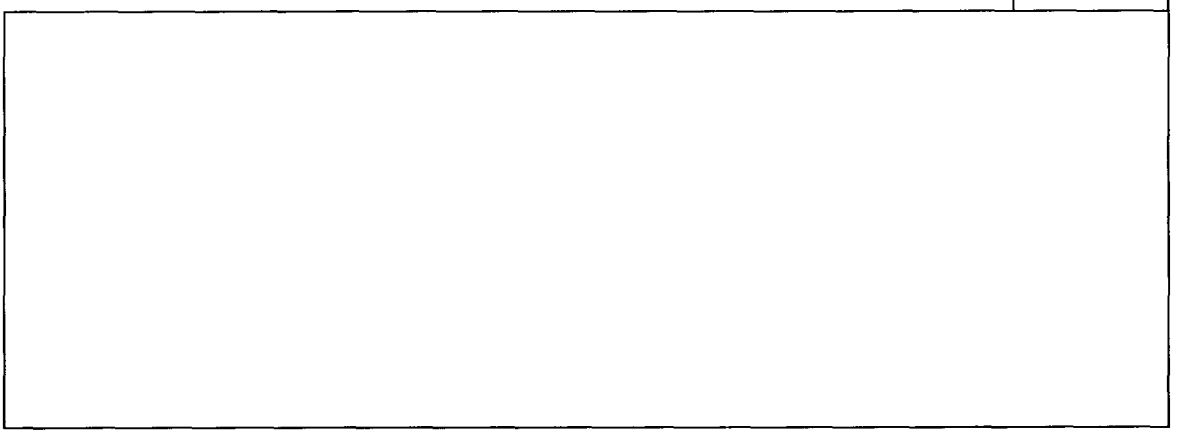
PROPRIETARY



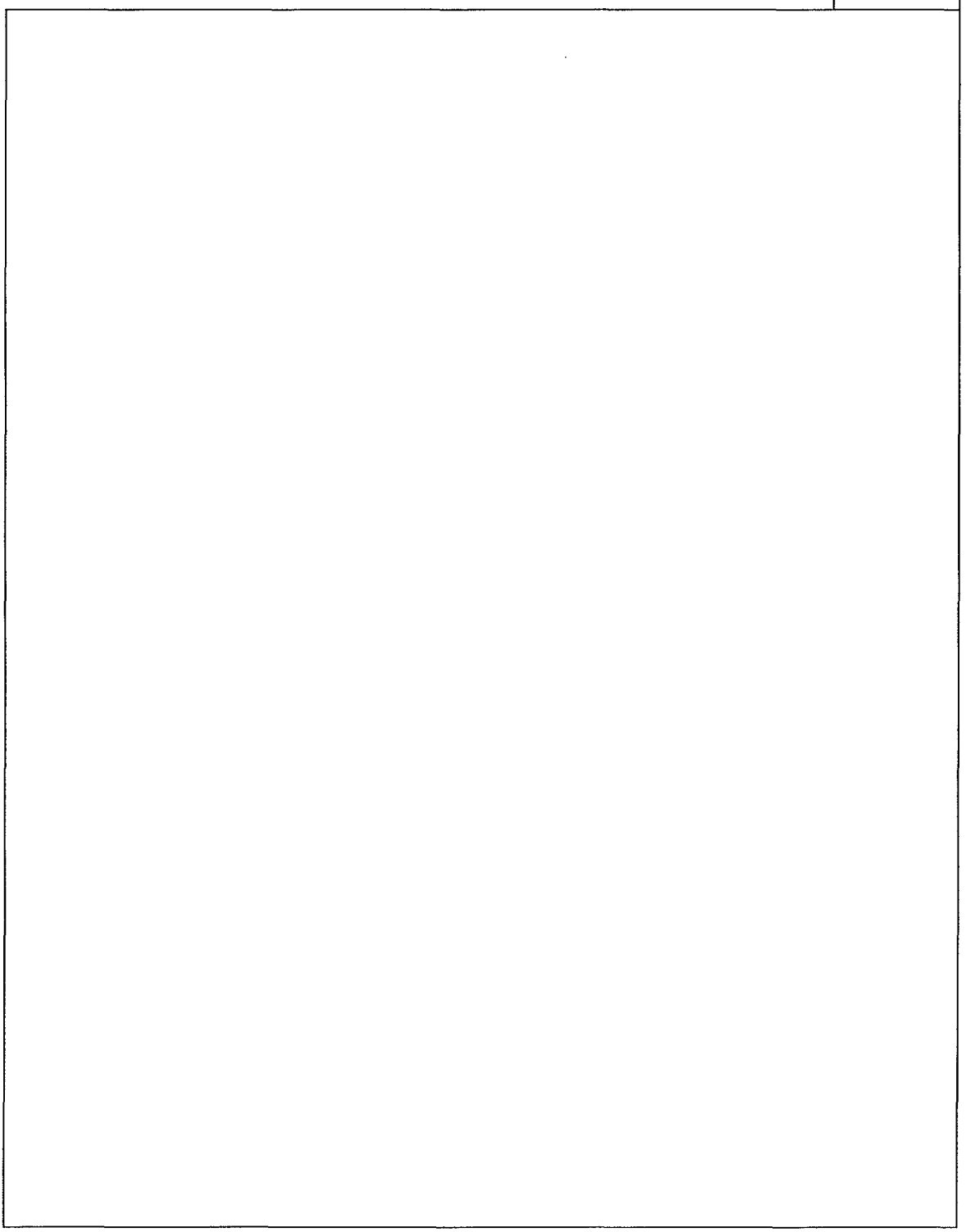
PROPRIETARY



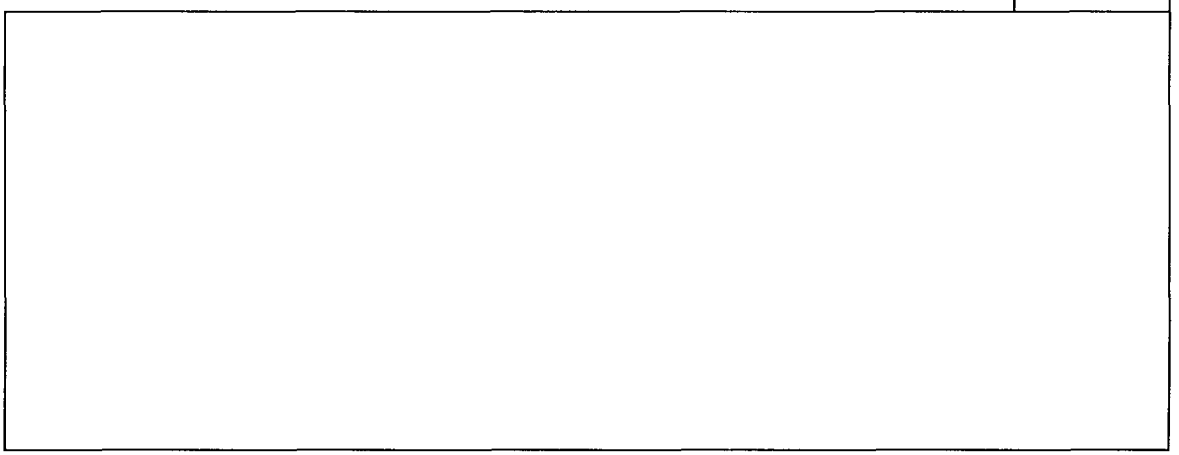
PROPRIETARY



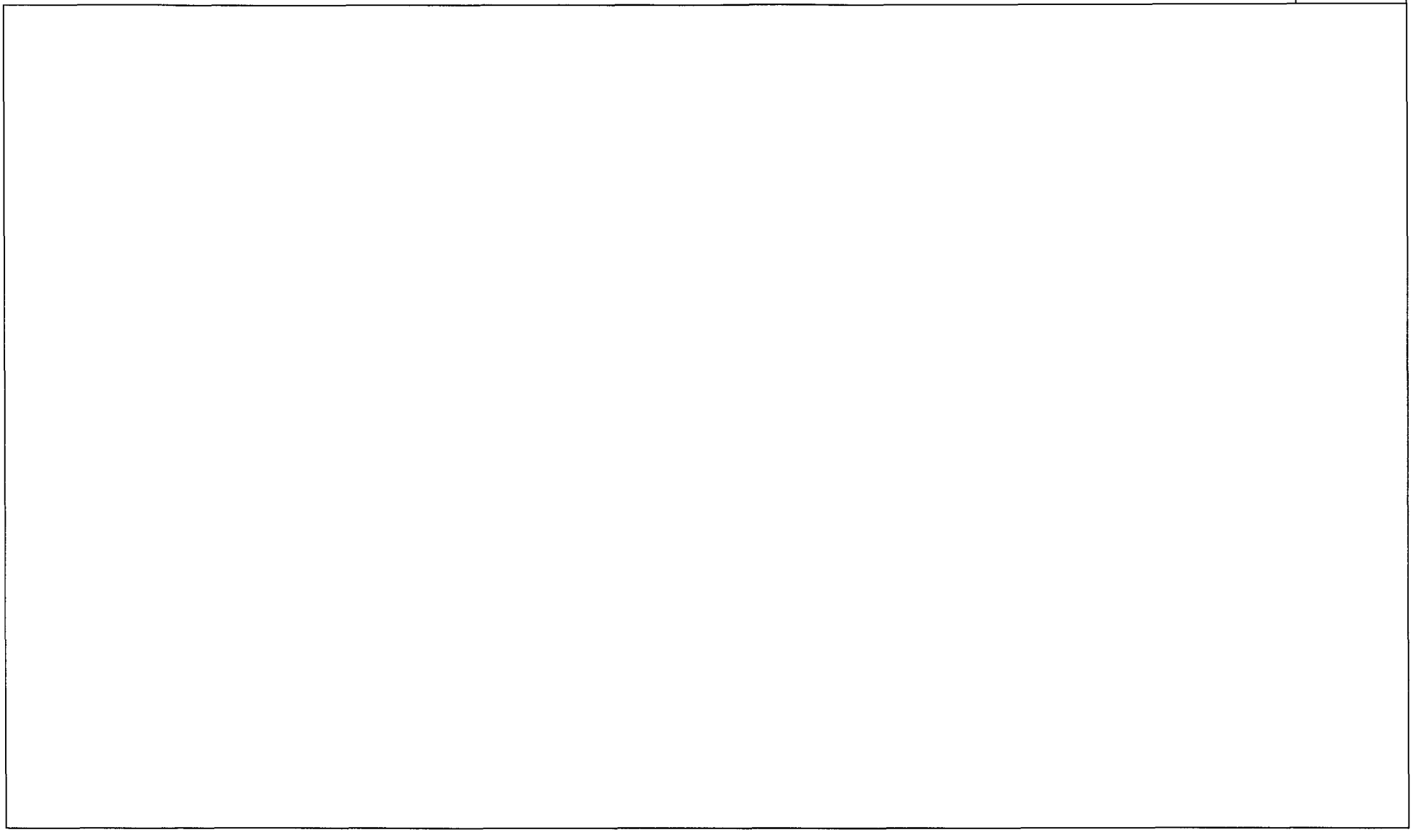
PROPRIETARY



PROPRIETARY



PROPRIETARY



PROPRIETARY