PSNN-2020-0035

US Safety-Related

Document No.	FPG-DRT-C51-0022	Rev	1

NRW-FPGA-Based PRM System Qualification Project

Document Title System Validation Testing Phase Hazard Analysis Report

CUSTOMER NAME	None
PROJECT NAME	NRW-FPGA-Based PRM System Qualification Project
ITEM NAME	PRM Equipment
ITEM NO.	C51
JOB NO.	FPG

TOSHIBA NED verified this Design Document;

Method : Design Review

Verification Report No. : DVR-IM-20080416-5

Verified by Toshiaki Ito

Group Name Monitoring System Engineering Group

Date April 18, 2008

TOSHIBA

Date	Issued by	Approved by	Reviewed by	Prepared by	Document Filing No.
Apr. 18, 2008	Monitoring System Engineering Group	Apr. 18, 2008	Apr. 17, 2008	Apr. 16, 2008	RS-5125805

Rev No.	Date	History	Approved by	Reviewed by	Prepared by
0	Mar 21,2008	The first issue	N. Oda	Y.Goto	H. Sakai
1	Apr 18, 2008	Correction	N. Oda	Y.Goto	T.Miyazaki

Table of Contents

1 Purpose

This document provides the results of the Hazard Analysis for the Non-Rewritable Field Programmable Gate Array (NRW-FPGA)-Based Power Range Monitor (PRM) System for use as a reactor safety protection system in Boiling Water Reactor (BWR) plants.

This hazard analysis is performed to determine if the PRM design and associated activities throughout the life cycle were established in a manner that minimizes risk and design errors. Toshiba used the Hazard Analysis process throughout the design and development process to ensure that Toshiba engineers identified, evaluated, and resolved potential failures as the design evolved. The Hazard Analysis process also ensures that appropriate emphasis is provided in reviews and tests through the design and development life cycle.

2 Scope

Throughout the PRM design and development, Toshiba engineers performed appropriate Hazard Analysis activities. Toshiba engineers performed Preliminary Hazard Analyses (PHA) for the Project Planning and Concept Definition Phase (Concept Phase)(Reference 3), the Requirements Definition Phase (Requirements Phase)(Reference 4), the Design Phase (Reference 5), the Implementation and Integration Phase (Implementation Phase)(Reference 6), and the Unit/Module Validation Testing Phase (Reference 7). This report summarizes the previous analyses and completes the hazard analysis by including the results of the System Validation Testing Phase Hazard Analysis, in accordance with Section 4.2.4 of the Software Quality Assurance Plan (SQAP) (Reference 2).

3 Approach

Toshiba used both a top down and bottom up approach for hazard analyses. The Concept and Design Phases used a top down Fault Tree Analysis (FTA) approach, using NUREG-0492 handbook (Reference 18) as a guideline. The Requirements Phase used a bottom up Failure Modes and Effects Analysis (FMEA) approach, using IEEE Std 352 (Reference 19) as a guideline. The FTA in the Design Phase resolved concerns identified in the Requirements Phase. In subsequent phases of the development process, Toshiba engineers verified and validated that the concerns identified in the Hazards Analyses were appropriately addressed in design, review, and test activities.

4 PRM System

The PRM system is designed to provide information used for monitoring the average power level of the reactor core, and for monitoring the local power density distribution associated with the withdrawal or insertion of control rods. The PRM system monitors the core for local and full-core power transients when the reactor is in the power range above approximately 10 percent of rated power. It provides trip signals to initiate reactor scrams under excessive neutron flux conditions, or when the rate of neutron flux increase is excessive. It provides data to the Oscillation Power Range Monitor (OPRM) to detect coupled neutron and thermal-hydraulic reactor instability. The PRM provides alarms to warn the operator of the impending or actual trip occurrences. The PRM also provides power information to the operator and performs the rod block monitoring function.

The PRM system configuration used as the basis for establishing the hazard analysis is described in

Equipment Requirement Specification (ERS) (Reference 1). It is represented in Figure 4-1. Figure 4-1 omits the OPRM subsystems because the OPRM is not included in the design and qualification of the PRM. This PRM system used in the qualification process is configured to support the BWR-5 type reactor core configuration.

The hazard analysis is based on system hardware and configuration features:

- Two redundant divisions
- 172 Local Power Range Monitor (LPRM) Detectors input signals
- Four Flow channels
- Two redundant safety related serial communication links to division-specific Oscillation Power Range Monitors (OPRM)
- Two redundant safety related serial communication links to division-specific Rod Block Monitor (RBM) channels

Toshiba developed the FPGAs used in the PRM using a similar process to that used in software development. The process uses software tools to convert written Very High Speed Integrated Circuit (VHSIC) Hardware Description Language (VHDL) source code into a fusemap, which in turn is then embedded in the FPGAs.

When software tools are used in the development process, section 5.3.2 of the IEEE Std 7-4.3.2 (Reference 20) requires one or both of the following methods to confirm suitability of use:

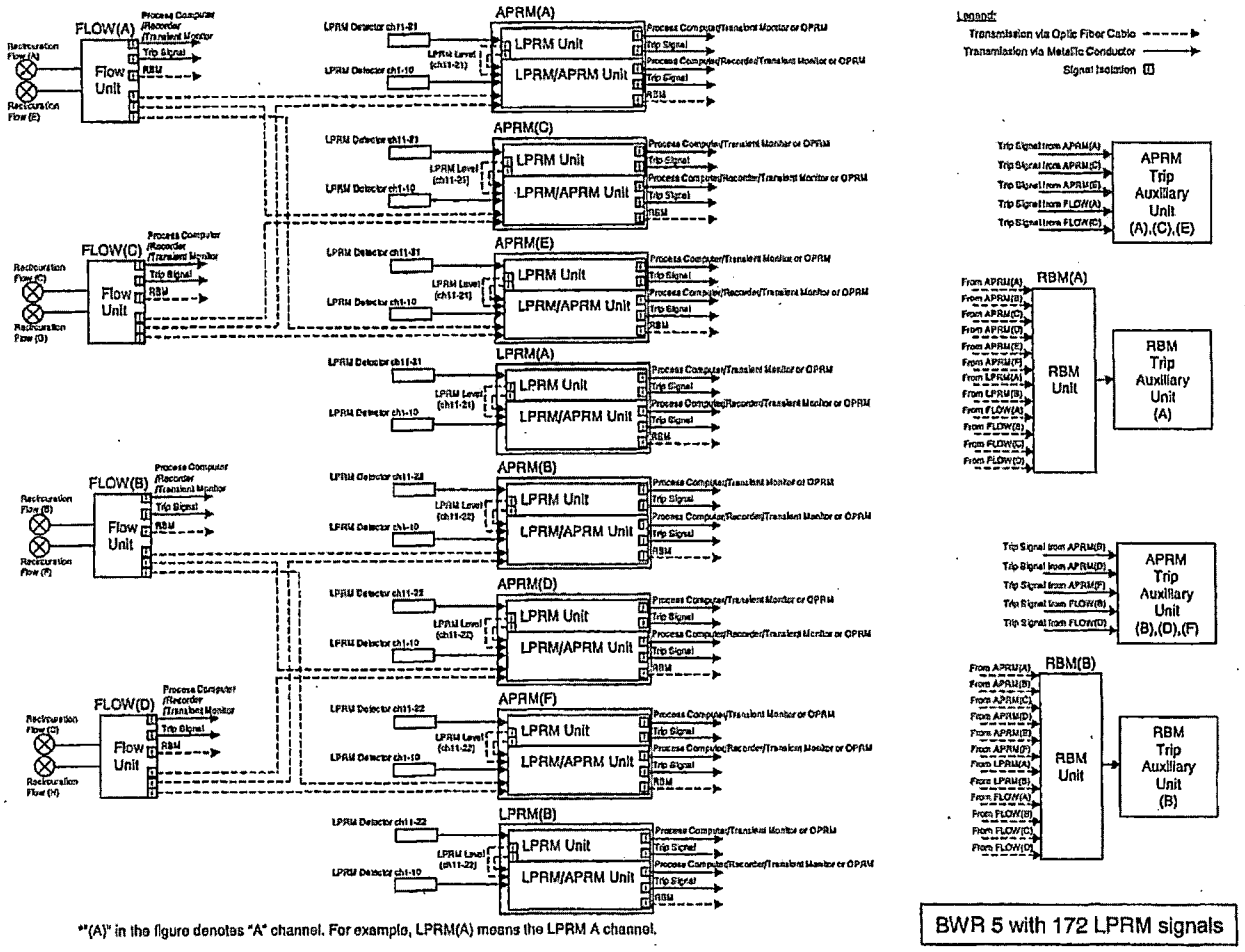
a) A test tool validation program shall be developed to provide confidence that the necessary features of the software tool function as required.

b) The software tool shall be used in a manner such that defects not detected by the software tool will be detected by V&V activities.*

The software was evaluated and engineering review processes were put in place that make use of the errors detected by the software tools, along with providing full-pattern testing of the basic functions Toshiba designed and implemented to build the PRM logic.

The FPGA-based PRM system development process includes foreseeing potential hazards inherently associated with the FPGA development process itself. These hazards associated with the FPGA development process are likely to become apparent in the Implementation phase. Figure 4-2 shows the FPGA-based System Development Process and potential hazards associated with each phase.

* V&V: Verification and Validation



*"(A)" in the figure denotes "A" channel. For example, LPRM(A) means the LPRM A channel.

Figure 4-1: PRM System Configuration (BWR-5)

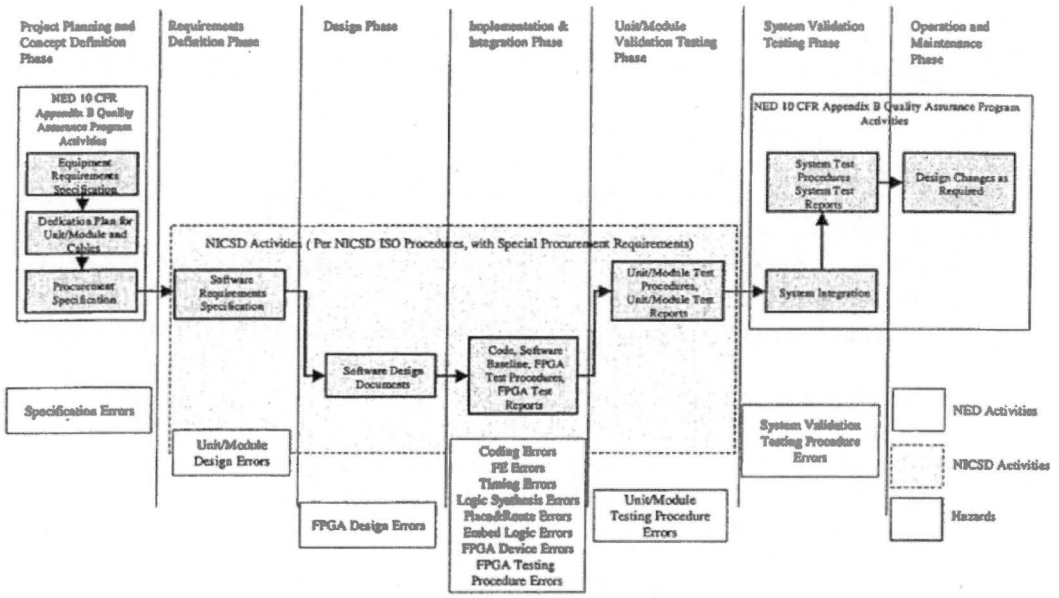


Figure 4-2 FPGA-based Systems Development Process and Associated Hazards

5 Summary of Preliminary Hazard Analyses

This section summarizes the PHA performed from the Concept Phase through the Unit/Module Validation Testing Phase. Each of the following sections summarizes the activities performed to mitigate the risks of hazards during the complete development process. Figure 4-2 serves as guideline for the next sub-sections.

5.1 System Planning and Concept Definition Phase PHA

In the Concept Phase, a top down and bottom up approach of hazard analysis is established. The Preliminary Hazard Analysis Report (Reference 3) describes more details of the Concept Phase Analysis. Below is a summary of the activities:

An FTA was performed for the PRM system configured as mentioned in Section 4.

The PRM FTA identified three events that can affect plant safety or operation. These events were:

- Loss of APRM Trip Output to the Reactor Protection System (RPS)
- Incorrect APRM Trip Outputs to the RPS
- Incorrect output to the OPRM

Three subsequent Fault Trees were developed, one for each of the above events.

A review of each Fault Tree concluded:

(1) Two concurrent occurrences of basic events are required to affect plant operation. A single non-common mode failure is not critical to plant safe operation, public health and the environment.

(2) Multiple failures can occur due to a Common Cause Failure (CCF) of a component that is located throughout the PRM system. The analyses in the later phases addressed this concern.

The Failure Mode and Effects Analysis (FMEA) performed in the next phase, i.e. in the Requirements Phase, addresses these two issues, along with others found during the FMEA process. In addition, from this FTA, two CCF sources were identified:

- Errors in the software tools may introduce flaws in the FPGAs that can cause a failure of the PRM system.
- Timing errors or glitches in an FPGA may cause a failure of the PRM system.

Based on the evaluation performed by Toshiba, the hazards in the Concept Phase result from "Specification Errors." The V&V activities implemented by Toshiba (the Concept Phase V&V Report) (Reference 11)) substantially reduced this hazard to a minimum and acceptable level of risk.

5.2 Requirements Definition Phase PHA

In the Requirements Phase, Nuclear Instrumentation and Control Systems Department (NICSD) established Unit/Module Equipment Design Specifications. An FMEA was performed based on the specifications for the units and modules that constituted the PRM system. The analysis concentrated on CCF reflecting the second conclusion of the Concept Phase PHA.

The FMEA revealed the following concerns relating to CCF:

- The [ ]a,c FPGA ([ ])a,c of the TRN module does not update the output data.
- The [ ]a,c FPGA ([ ])a,c of the TRN module does not update the output data.
- The [ ]a,c FPGA ([ ])a,c of the TRN module sends incorrect data.
- The [ ]a,c FPGA ([ ])a,c of the RCV module does not update the output data.
- The [ ]a,c FPGA ([ ])a,c of the RCV module does not update the output data.

These concerns indicate that further Design Phase Analysis is warranted.

In addition, the FMEA identified recommendations to support detecting hazards of the PRM device. For example, to guard against failures of rotary switches used to set values, the FMEA suggested having operational procedures require technicians and engineers to check the set value by comparing the rotary switch setting against the value displayed on the module front panel.

The potential hazards in the Requirements Phase all relate to "Unit/Module Design Errors." The V&V activities implemented by Toshiba (the Requirements Phase V&V Report (Reference 12)) minimize the possibility for these hazards to what Toshiba considers a minimum and acceptable risk.

5.3 Design Phase PHA

In the Design Phase, NICSD established the FPGA Design Specification for each FPGA, and established internal design of the FPGAs. Using the FPGA Design Specifications, the concerns identified from the Requirements Phase were further considered. In addition, the[ ]^{a,c} [ ]^{a,c}FPGA was analyzed because the analysis of the[ ]^{a,c}FPGA indicated a possibility that failures of[ ]^{a,c}FPGA could be CCF related. The Design Phase PHA report (Reference 5) describes the details of the Design Phase Analysis.

The concerns about these FPGAs ([ ]^{a,c}and their failure modes are:
(1) Output data non-update or incorrect data transmission events occur.
(2) These events remain unnoticed.

The Design Phase PHA examined each FPGA design and identified the following unresolved items.

- Is the FPGA is designed to prevent the event?
- Can a limited number of practically performable test cases assure that the event is unlikely?
- Can the event occurrence be detected?

The analysis concluded:

(1) The failure that the[ ]^{a,c}FPGA does not update the output data is unlikely, based on the design of the[ ]^{a,c}FPGA.
(2) Appropriate testing of the[ ]^{a,c} FPGAs could assure that the FPGA failing to update the output data or sending incorrect data transmission would be unlikely. Testing of the actual FPGAs is required to close this issue, which Toshiba performed in the Unit/Module Test Phase.

The hazards for the Design Phase are effectively "FPGA Design Errors." The V&V activities adopted by Toshiba (the Design Phase V&V Report (Reference 13)) substantially reduce this hazard to minimum and acceptable risk.

5.4 Implementation and Integration Phase PHA

NICSD developed the VHDL source codes based on the FPGA design. Toshiba used commercial tools to convert the VHDL source codes into netlists and convert the netlists into fusemaps. NICSD then embedded the fusemaps in the FPGAs and performed testing. NICSD also performed some special V&V activities (the Implementation Phase V&V Report (Reference 14)), to assure the FPGA reliability.

Toshiba performed two analyses in the Implementation Phase. One addressed the concern from the Design Phase. The other addressed the hazards identified with the FPGA-based systems development process.

To resolve the concern from the Design Phase, Toshiba examined the FPGA test methods. The concerns for the[ ]^{a,c}FPGAs are that these FPGAs may continue transmitting the same data without updating it, or that the FPGA may send incorrect data. Examination of the test cases confirmed that they toggle all connections among functional elements (FE) constituting the functional block that updated the output data. These test cases validated correct operation, as documented in the Implementation Phase V&V Report.

The[ ]a,c FPGA was designed to repeat reception and transmission of data. The concern the[ ]a,c FPGA might transmit incorrect data is assessed by performing further testing. The test cases were designed to toggle all connections among FEs that perform this operation. These test cases demonstrate that circuit blocks constituting the[ ]a,c FPGA continue their operation independently of the data values. Therefore, the incorrect data transmission event of [ ]a,c FPGA output data is unlikely.

Other identified hazards associated with FPGA-based systems development process result from: Coding Errors, FE Errors, Timing Errors, Logic Synthesis Errors, Place and Route Errors, Logic Embedding Errors, FPGA Device Errors, and FPGA Testing Procedure Errors.
All issues were resolved satisfactorily by incorporating;

- Suitable V & V activities directed at source code reviews, FPGA testing, software tools, configuration management,
- Synchronous design techniques,
- Performing static and dynamic timing analyses on the fusemaps,
- Not using a state-machine based design,
- Using two different formats for storing data,
- Using an anti-fuse design for immunity against high energy particle strikes that could cause a Single Event Upset (SEU), and,
- Implementing Unit/Module Validation Testing to address the concern that the FPGA would operate at its intended design frequency (presented in section 5.5. below).

As a result, the Implementation Phase PHA report (Reference 6) concluded:
(1) All the concerns from the Design Phase were resolved.
(2) The only remaining issue is to verify that the FPGAs operate at their "design" operating frequency, which shall be addressed in the next Unit/Module Validation Testing Phase.

5.5 Unit/Module Validation Testing Phase PHA

The Unit/Module Validation Testing Phase PHA addressed the concern from the Implementation Phase and hazards relating to whether the FPGAs operate at their design frequency. In the Unit/Module Validation Testing Phase, the FPGAs were integrated into modules and tested in a situation simulating the actual plant operations. All FPGAs operated at their design frequency. Therefore, the concern was resolved.

Additional testing was performed outside the qualification project where the modules were tested at frequencies above their design frequency until faults and failures occurred. That testing is reported in "Over Clock Test Report" (Reference 17).

The Unit/Module Validation Testing Phase includes hazards tied to errors in testing procedures. The test procedures were independently reviewed through the NICSD V&V activities. It is unlikely that the testing that followed Unit/Module Test Procedures left any errors leading to any hazards in the PRM devices and Toshiba concluded that the test procedures covered the identified hazards appropriately.

However, there exists the remote possibility that errors in the test procedures could, however unlikely, cause damage to the PRM devices. Possibilities of physical and electrical damages to the PRM devices were assessed. Toshiba concluded that they were unlikely, because the testing was performed by well-trained personnel, following the reviewed procedures and using test equipment designed to not damage the PRM equipment.

Therefore Toshiba concludes that any remaining risks present in the Unit/Module Validation Testing Phase were acceptable and minimum.

6 Hazard Analysis for this System Validation Testing Phase

6.1 System Validation Testing

The qualified testers from the Nuclear Energy Systems and Services Division (NED) Quality Assurance Department performed the System Validation Testing. Prior to the System Validation Testing, NICSD integrated the test specimen following the order issued by NED (see Figure 4-2). The test specimen consisted of:

- One LPRM unit
- One LPRM/APRM unit
- Two FLOW units

Figure 6-1 shows the Test Setup for the System Validation Testing. The System Validation Testing was performed in an air-conditioned room at Fuchu Complex. The testing was performed based on the System Validation Test Procedure (Reference 9) and results were recorded for later review and acceptance (Reference 10).

Figure 6-1 Setup of System Validation Testing

The test setup was similar to that for the Unit/Module validation testing except that the Trip Auxiliary unit, the current monitor box, and the data recorder were attached. The System Validation Test Procedure defined the test cases as follows:

- Check-Out Testing

- Operability Testing
- Prudency Testing
- Power Quality Tolerance Testing
- Burn-in Testing

6.2 Hazard in System Validation Testing

Hazards Analysis evaluated the test procedure to ensure that the testing covers the identified risks and that the testing does not damage the PRM devices, creating new faults and failures. The remainder of this section addresses this issue.

Coverage of Identified Risks and Hazards: All risks and hazards identified by Toshiba have been addressed in either this phase or earlier phases through testing, review, inspection, and analysis.

System Test Procedure Errors: If the System Validation Test Procedures have errors, the testing could fail to find defects present in the system, leading to unresolved hazards in the PRM system. To eliminate the test procedure errors, the NED design engineers prepared a Requirements Traceability Matrix (RTM) (Reference 8). In addition, the NED V&V team reviewed the System Validation Test Procedure for completeness, correctness, consistency, and accuracy. See the System Validation Testing Phase V&V Report (Reference 9).

Physical and Electrical Damage: For the NRW-FPGA based devices, because the logic is embedded in the anti-fuse FPGAs, the only risk of logic change is by damaging the devices physically or electrically. For the operations and maintenance phase, this risk will be reduced by requiring all handling to use anti-static procedures and equipment for modules and units.

The System Validation Testing was performed in an air-conditioned room. The test procedures were reviewed by the NED V&V team. The testers were qualified personnel, and dealt with the PRM system carefully to avoid damaging the equipment.

Additional Equipment: The Trip Auxiliary Unit was developed by NICSD to this PRM system. This unit was designed to have compatible interfaces with the PRM system. The current monitoring box, and the data recorder only received signals from the PRM system. It was unlikely that any of these devices had any harmful effects on the PRM system, because they were designed to have compatible interfaces with the PRM system.

7 Risk Assessment

Toshiba performed Hazard Analysis of the PRM system. As discussed in this document, and in the individual Hazards Analysis Phase Reports, all identified Hazards and Risks were evaluated and addressed during the progression of the design, development, review, and testing activities at Toshiba. Appropriate actions will be defined in the Users Manual for the Operation and Maintenance Phase.

8 Conclusions

The Hazards Analysis activities performed during the PRM life cycle discovered several hazards and risks. Review of the Toshiba responses to those hazards and risks shows that the design process used, when combined with targeted reviews and testing, minimized the risk of faults and failures in the PRM system. Other analyses of boiling water reactors have accepted the

multiple division design that this PRM system supports.
This Hazard Analysis Report concludes that hazards and risks associated with this PRM system design is within acceptable level, and that the following conditions have been met:

(1) The system configuration satisfies the prerequisites in the Concept Phase.
(2) The recommendations raised from the FMEA in the Requirements Phase were incorporated in the system life cycle.
(3) The Toshiba NRW-FPGA life cycle processes, as they affect the Hazards Analysis process, have been implemented correctly.

9 References

1	FPG-RQS-C51-0001	Equipment Requirement Specification of FPGA based Units, Rev. 7
2	FPG-PLN-C51-0002	Software Quality Assurance Plan, Rev. 2
3	FPG-DRT-C51-0002	Preliminary Hazard Analysis Report, Rev. 2
4	FPG-DRT-C51-0018	Requirements Definition Phase Preliminary Hazard Analysis Report, Rev. 0
5	FPG-DRT-C51-0019	Design Phase Preliminary Hazard Analysis Report, Rev. 1
6	FPG-DRT-C51-0020	Implementation and Integration Phase Preliminary Hazard Analysis Report, Rev. 1
7	FPG-DRT-C51-0021	Unit/Module Validation Testing Phase Preliminary Hazard Analysis Report, Rev. 1
8	FPG-DRT-C51-0017	System Validation Testing Phase Requirement Traceability Matrix Report, Rev. 0
9	FPG-TPRC-C51-0001	System Validation Test Procedure, Rev. 2
10	FPG-06-ETR-001	System Validation Test Records
11	FPG-DRT-C51-0011	Project Planning and Concept Phase V&V Report, Rev. 2
12	FPG-DRT-C51-0012	Requirements Definition Phase V&V Report, Rev. 1
13	FPG-DRT-C51-0013	Design Phase V&V Report, Rev. 1
14	FPG-DRT-C51-0014	Implementation and Integration Phase V&V Report, Rev. 0
15	FPG-DRT-C51-0015	Unit/Module Validation Phase V&V Report, Rev. 0
16	FPG-DRT-C51-0016	System Validation Testing Phase V&V Report, Rev. 0
17	NICSD 9H8H0232	Over Clock Test Report
18	NUREG-0492	Fault Tree Handbook
19	IEEE Std 352-1987	IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems
20	IEEE Std 7-4.3.2-2003	IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations

10 Abbreviation

APRM	Average Power Range Monitor
BWR	Boiling Water Reactor
CCF	Common Cause Failure
ERS	Equipment Requirement Specification
FE	Functional Element
FMEA	Failure Modes Effects Analysis
FPGA	Field Programmable Gate Array
FTA	Fault Tree Analysis
LPRM	Local Power Range Monitor
OPRM	Oscillation Power Range Monitor

NED	Nuclear Energy Systems and Services Division
NICSD	Nuclear Instrumentation and Control Systems Department
PHA	Preliminary Hazard Analysis
PRM	Power Range Monitor
RBM	Rod Block Monitor
RTM	Requirements Traceability Matrix
SEU	Single Event Upset
V&V	Verification and Validation
VHDL	Very High Speed Integrated Circuit Hardware Description Language
VHSIC	Very High Speed Integrated Circuit