**Safety-Related**



| Toshiba Project Document No. | Rev. No. |
|---|---|
| FA32-3709-0001 | 4 |

# NRW-FPGA-Based I&C System Qualification Project
# **Software Verification and Validation Plan**

## Title: Nuclear Energy Systems and Services Division FPGA-based Safety-Related Systems Verification and Validation Plan

| | |
|---|---|
| Customer Name | None |
| Project Name | NRWS-FPGA-Based I&C System Qualification Project |
| Item Name | None |
| Item Number | A32 |
| Job Number | 9P04482 |
| Applicable Plant | None |

| Rev. No. | Issue Date | Description | Approved by | Reviewed by | Prepared by |
|---|---|---|---|---|---|
| 4 | Jun 27 2016 | See also DCN-FA32-3709-0001-004 (This revision resolves CAR-16-073 and CAR-16-075). | M. Hamada 27-Jun-2016 | T.Ito June 27,2016 | T. Hayashi June 23, 2016 |

| Initial Issue Date | Issued by | Approved by | Reviewed by | Prepared by | Document filing No. |
|---|---|---|---|---|---|
| Oct 17, 2011 | Electrical System Design & Engineering Department | T. Ito Oct 17, 2011 | T. Ito Oct 17, 2011 | T. Hayashi Oct. 17, 2011 | RS-5156262 |

# Record of Revisions

| Rev No. | Date | Description | Approved by | Reviewed by | Prepared by |
|---|---|---|---|---|---|
| 0 | See Cover Page | Initial Issue | See Cover Page | See Cover Page | See Cover Page |
| 1 | Jan 24, 2012 | See DCN-FA32-3709-0001-001 | T. Maekawa Jan 24, 2012 | T. Ito Jan 20, 2012 | T. Hayashi Jan 17, 2012 |
| 2 | July 31, 2012 | See DCN-FA32-3709-0001-002 | T. Maekawa Jul. 31, 2012 | T. Ito Jul. 31, 2012 | T. Hayashi Jul. 31, 2012 |
| 3 | Dec. 24, 2013 | See DCN-FA32-3709-0001-003 | N. Tahira Dec. 24, 2013 | T. Ito Dec. 24, 2013 | T. Hayashi Dec. 19, 2013 |
| 4 | See Cover Page | See Cover Page | See Cover Page | See Cover Page | See Cover Page |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

# Table of Contents

# 1 Introduction

## 1.1 Purpose

This Nuclear Energy Systems and Services Division (NED) Verification and Validation (V&V) plan (NED VVP) is prepared for Field Programmable Gate Array (FPGA)-based Safety-Related Instrumentation and Control (I&C) systems for US nuclear power plants.

The system design of FPGA-based Safety-Related I&C systems is determined by the Instrumentation & Control Systems Design and Engineering Department (ICDD) of NED, and ICDD procures the FPGA-based equipment from the Toshiba Fuchu Complex Power Systems Segment (Fuchu-PS) Nuclear Instrumentation and Control Systems Department (NICSD). NICSD procures FPGA-based components, including modules with FPGA logic from the Toshiba Fuchu-PS Power Platform Development Department (PPDD) using a commercial grade dedication process.

For FPGA-based Safety-Related I&C systems V&V activities, ICDD and NICSD organize independent V&V (IV&V) Teams, and the IV&V Teams work together.

The software lifecycle process, including V&V, is defined in the project document "Nuclear Energy Systems and Services Division Software Management Plan for FPGA-based Safety-Related Systems" (NED SMP) (Reference (19)). This NED VVP is prepared by the ICDD IV&V Team in accordance with the following reference documents:

- NED AS-200A128 "Digital System Life Cycle Procedure" (Reference (10)),
- NED AS-200A129 "Digital System Development Procedure" (Reference (11)), and
- NED AS-200A130 "Digital System Verification & Validation Procedure" (Reference (12)).

## 1.2 Scope

This NED VVP is prepared for the FPGA-based Safety-Related I&C systems for US nuclear power plant. Section 4 of the project document "Software Program Plan," (SPP) (Reference (18)) establishes requirements and provides guidance and expectations for the V&V activities. This NED VVP complies with Section 4 of the SPP for the NED portions of the V&V activities.

# 2 Reference Documents

## 2.1 Code of Federal Regulations

This NED VVP does not refer to the Code of Federal Regulations (CFR) directly. The Toshiba internal standards in Section 2.4 are based on the CFR.

## 2.2 Regulatory Guides and NRC Documents

(1) Regulatory Guide 1.168
"Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." Rev.1, 2004

(2) Regulatory Guide 1.152
"Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Rev.3, July 2011

Other regulatory guides may be referred to indirectly through the Toshiba internal standards in Section 2.4.

## 2.3 Industry Standards

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

(4) IEEE Std 1028-1997
"IEEE Standard for Software Reviews"

## 2.4 Toshiba Internal Documents

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

(6) Toshiba Nuclear Energy Systems and Services Division AS-100A004
"Document Control Procedure"

(7) Toshiba Nuclear Energy Systems and Services Division AS-200A002
"Design Verification Procedure"

(8) Toshiba Nuclear Energy Systems and Services Division AS-200A010
"Control Procedure of vendor generated documents"

(9) Toshiba Nuclear Energy Systems and Services Division AS-200A015
"Design Change Control Procedure"

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

(11) Toshiba Nuclear Energy Systems and Services Division AS-200A129
"Digital System Development Procedure"

(12) Toshiba Nuclear Energy Systems and Services Division AS-200A130
"Digital System Verification & Validation Procedure"

(13) Toshiba Nuclear Energy Systems and Services Division AS-300A006
"Nonconformance Control Procedure for Procured Items and Services"

(14) Toshiba Nuclear Energy Systems and Services Division AS-300A008
"Nonconformance Control and Corrective Action Procedure"

(15) Toshiba Nuclear Energy Systems and Services Division AS-300A009
"Corrective Action Request Application Procedure"

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

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

## 2.5 Project Documents

(17) NRW-FPGA-Based I&C System Qualification Project, FA10-0301-0001
"Project Specific Document Control Procedure" Rev.0

(18) NRW-FPGA-Based I&C System Qualification Project, FA10-0501-0024
"Software Program Plan" Rev. 1

(19) NRW-FPGA-Based I&C System Qualification Project, FA32-3702-0005
"Nuclear Energy Systems and Services Division FPGA-based Safety-Related Systems Software Management Plan" Rev.2

(20) NRW-FPGA-Based I&C System Qualification Project, FC51-3601-0001
"Procurement Specification for Equipment Qualification and EMC Qualification of Components of Oscillation Power Range Monitor (OPRM)" Rev.11

# 3 Definitions and Acronyms

## 3.1 Definitions

**Module:** A part of a unit. Each module consists of one or more printed circuit boards, on which the FPGAs and other circuitry are mounted, and a front panel.

**Unit:** A major component of the FPGA-based Safety-Related I&C systems. A unit is a chassis that has front slots and back slots to mount modules. Each unit consists of several modules. There is a vertical middle plane between the front and back slots in each unit. This plane consists of two circuit boards. These circuit boards provide backplanes for the front and rear modules. Modules plug into the backplanes using connectors. Once a module is plugged into the appropriate connector, it exchanges data with other modules in the unit, connects to other units and any external field equipment, and is powered.

**Validation:** Validation is used to ensure that the final product satisfies the user requirements. Validation shall be performed on the final product, although validation may be necessary or performed prior to the final code being produced. See Section 4.2 of the SPP (Reference (18)).

**Verification:** Verification consists of reviews performed on the results of each development phase to ensure the phase was completed appropriately and correctly. See Section 4.2 of the SPP.

## 3.2 Acronyms

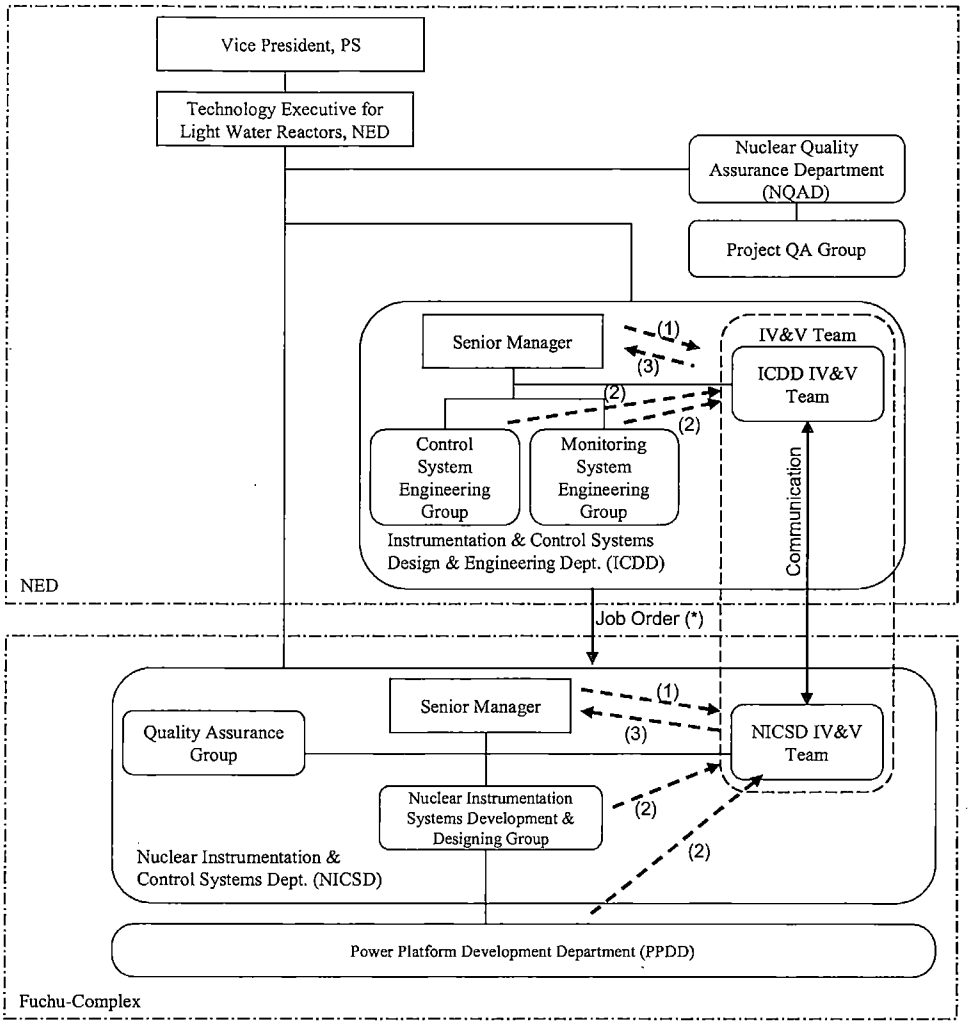
| | |
|---|---|
| BRR | Baseline Review Report |
| CAR | Corrective Action Request |
| CFR | Code of Federal Regulation |
| CM | Configuration Management |
| DCN | Design Change Notice |
| DVR | Design Verification Report |
| EDS | Equipment Design Specification |
| ES | Engineering Schedule |
| FPGA | Field Programmable Gate Array (a programmable logic device) |
| Fuchu-PS | Toshiba Fuchu Complex Power Systems Segment |
| I&C | Instrumentation and Control |
| IBD | Interlock Block Diagram |
| ICDD | Instrumentation & Control Systems Design and Engineering Department |
| IED | Instrumentation Electrical Diagram |
| IEEE | Institute of Electrical and Electronics Engineers |
| IV&V | Independent Verification and Validation |
| NED | Nuclear Energy Systems and Services Division |
| NICSD | Nuclear Instrumentation & Control Systems Department |
| NMS | Neutron Monitoring System |

| | |
|---|---|
| NNR | Nonconformance Notice Report |
| NQ | Nuclear Quality (standards for NICSD) |
| NQAD | Nuclear Quality Assurance Department |
| NRW | Non-Rewritable |
| PCD | Project Control Document |
| PCDL | Project Control Document List |
| PM | Project Manager |
| PPDD | Power Platform Development Department |
| PRM | Process Review Meeting |
| RG | Regulatory Guide |
| RTIS | Reactor Trip and Isolation System |
| RTM | Requirements Traceability Matrix |
| SDD | System Design Description |
| SDOE | Secure Development and Operational Environment |
| SIL | Software Integrity Level |
| SMP | Software Management Plan |
| SPP | Software Program Plan |
| SSAR | Software Safety Analysis Report |
| V&V | Verification and Validation |
| VDCL | Vendor generated Document Check List |
| VFS | Verification Follow Sheet |
| VVP | Verification and Validation Plan |
| VVR | Verification and Validation Report |

# 4 Verification and Validation Overview

## 4.1 Organizations

Figure 4-1 shows the Toshiba organizations for FPGA-based Safety-Related I&C system design and development. Engineers from ICDD and NICSD organize IV&V Teams (i.e., ICDD IV&V Team and NICSD IV&V Team) for the V&V of the FPGA logic. The engineers from ICDD and the engineers from NICSD in the IV&V Teams communicate with each other as one IV&V Team as needed for the quality of the products. The Control System Engineering Group and Monitoring System Engineering Group in ICDD are responsible for design and development of the FPGA-based Safety-Related I&C systems. The ICDD IV&V Team performs the V&V activities defined in this NED VVP independently of these design groups.




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

(1) Oversight of IV&V team
(2) Submittal of Design Documents
(3) Report of V&V Results

**Figure 4-1 Toshiba Organizations for the FPGA-based Safety-Related Systems Design and Development**

## 4.2 Master Schedule

The IV&V activities and milestones are developed and controlled as described in the NED SMP (Reference (19)).

## 4.3 Software Integrity Level Scheme

The software integrity level (SIL) scheme shall be determined based on Table A-1 of NED AS-200A129 (Reference (11)), which is substantially equivalent to the Appendix B of IEEE Std 1012 (Reference (3)).

For FPGA logics used in the FPGA-based Safety-Related I&C systems, the SIL shall be 4 in accordance with Regulatory Guide (RG) 1.168 (Reference (1)), because the FPGA logics are considered Safety-Related I&C software. All project software documents labeled as "US Safety-Related" on the cover sheet are considered SIL 4 software documents. All software embedded in the FPGA-based Safety-Related I&C systems shall be developed, verified, and validated as SIL 4 Safety-Related software.

## 4.4 Resource Summary

For NED V&V activities, only human resource is required. Resources for the V&V activities shall be prepared as described in Section 7 and Section 13 of the NED SMP (Reference (19)). For human resources, the following condition shall be met.

All ICDD IV&V Team members shall:

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

The ICDD IV&V Team members shall be aware of their independence from development, and shall be responsible for raising issues of their own qualification to the IV&V Lead as necessary.

## 4.5 Responsibilities

The NED SMP (Reference (19)) describes the responsibilities of the following personnel:

- Senior Manager (SM) of ICDD
- NED Project Manager (PM)
- Group Manager (GPM)
- IV&V Lead and IV&V Team

As stated in the NED SMP, the IV&V Lead shall be responsible for the V&V activities of NED and NICSD.

In addition to the responsibilities defined in the NED SMP, the IV&V Lead has responsibilities listed in Section 4.2.4 of the SPP (Reference (18)), including review of Secure Development and Operational Environment (SDOE) implementation. SDOE is defined in Regulatory Guide 1.152 (Reference (2)).

The ICDD IV&V Team may also oversee the work of ICDD, NICSD, and PPDD from a V&V point of view to ensure that their works are acceptable for development of Safety-Related systems.

Nuclear Quality Assurance Department (NQAD) of NED will conduct oversight of the ICDD

IV&V Team activities.

## 4.6 Tools, Techniques, and Methodologies

The ICDD IV&V Team will use several commercial software tools for V&V activities of the FPGA-based Safety-Related I&C systems. The NED SMP (Reference (19)) describes software tools used for engineering.

### 4.6.1 Verification

The ICDD IV&V Team will conduct the verification by reviewing the Requirements Traceability Matrix (RTM) and the Software Safety Analysis Reports (SSARs). The ICDD IV&V Team also reviews NICSD V&V Reports (VVRs) and SSARs. Verification shall be performed for the printed documents or for the electronic documents. The document management system called NUPDM will be used for distribution and archives of the documents. A set of standard business software tools will be used for verification.

Document review is a method of verification to assure that the design output is correct and satisfactory by addressing that, the design inputs were correctly incorporated into the design, and the design output is reasonable compared to the design input. The review shall be performed in accordance with NED AS-200A002 "Design Verification Procedure" (Reference (7)), and NED AS-200A130 (Reference (12)). IEEE Std 1012 (Reference (3)), and IEEE Std 1028 (Reference (4)) provide guidance for the reviews.

Document review performed as technical review confirms whether:

a) The document conforms to its upstream requirements

b) The document adheres to regulations, standards, guidelines, plans, and procedures applicable to the project

c) Changes to the document are properly implemented and affect only those system areas identified by the change specification

For planning documents, implementation process documents, and design outputs including SSAR and VVR, document review must be performed for completeness, consistency, correctness, and verifiability as applicable. The SPP "A Terms and Definition" provides definition for these words.

The review result shall be documented on the Design Verification Report (DVR), and when applicable the Verification Follow Sheet (VFS) shall be used for identification of comments and following up the comments to close.

### 4.6.2 Requirements Traceability Activities

Requirements Traceability Matrices (RTMs) shall be generated by the Software Development Team and reviewed by the IV&V Team to ensure the software has completely, accurately, correctly, and consistently addressed the requirements. The RTM shall provide traceability, verification, and validation of requirements.

### 4.6.3 Baseline Reviews

The ICDD IV&V Team shall attend all life cycle baseline reviews. The ICDD IV&V Team shall perform baseline reviews at the end of the Project Planning and Concept Definition Phase and the System Validation Testing Phase which ICDD is responsible for. The System Validation Testing Phase baseline review is the final baseline review, and confirms the completion of the system development.

The ICDD IV&V Team shall confirm the following:

- The NED design activities are performed, and the design outputs are prepared as planned in the NED SMP.
- NED V&V activities are performed as planned in this NED VVP.
- The NED design output document are controlled and listed on a Project Control Document (PCD) List (PCDL) in accordance with the project document "Project Specific Document Control Procedure" (Reference (17)), and NED AS-100A004 "Document Control Procedure" (Reference (6)).

  Documents which are issued or used for a specific plant (project) and specify technical and quality requirements or prescribe activities affecting quality, such as specification, instructions, procedures and drawings are categorized as Project Control Documents (PCDs). PCDL is the list of PCDs, including:

  (1) Contract name (or Project name)

  (2) Job Number

  (3) Project Document Number

  (4) Document Filing Number

  (5) Revision Number

  (6) Document Title.

All software life cycle activities for a given phase shall be complete prior to initiating a baseline review. Any anomalies or nonconformances found in baseline reviews shall be resolved through the software life cycle processes and controlled in accordance with Section 7.1.2. Each of the baseline reviews shall confirm disposition of design, documentation, and test nonconformances identified during the phase.

The ICDD IV&V Team shall document the result of a baseline review in a Baseline Review Report (BRR), and report to NQAD. NQAD accepts the BRR after reviewing that the BRR is established in accordance with the NED SMP, and includes the required contents. In accordance with Section 4.2.6.6 of the SPP, the BRR shall:

- Describe the review scope,
- Identify the reviewers,
- Identify the persons contacted during the review,
- Document the outputs and versions reviewed,
- Contain a summary of the review results, and
- Describe recommendations and findings.

### 4.6.4 Metrics

The ICDD IV&V Team should monitor and track the following metrics provided in the NED and NICSD VVRs through the lifecycle phases described in Section 5 to maintain the product quality.

- Number of changes applied for the design documents
- Number of new open items carried to next phases, and closed in current phases

- Number of Corrective Action Requests (CARs)
- Number of Nonconformance Notice Reports (NNRs)
- Number of problems found during testing

These metrics are used as indices to measure quality for both the work products and processes. The ICDD IV&V Team should evaluate value of these metrics throughout the life cycle, and consider replacement of metrics if they have no value.

# 5 Verification and Validation Activities

The following subsections describe the V&V activities for NED scope.

## 5.1 Management

### 5.1.1 Management of V&V

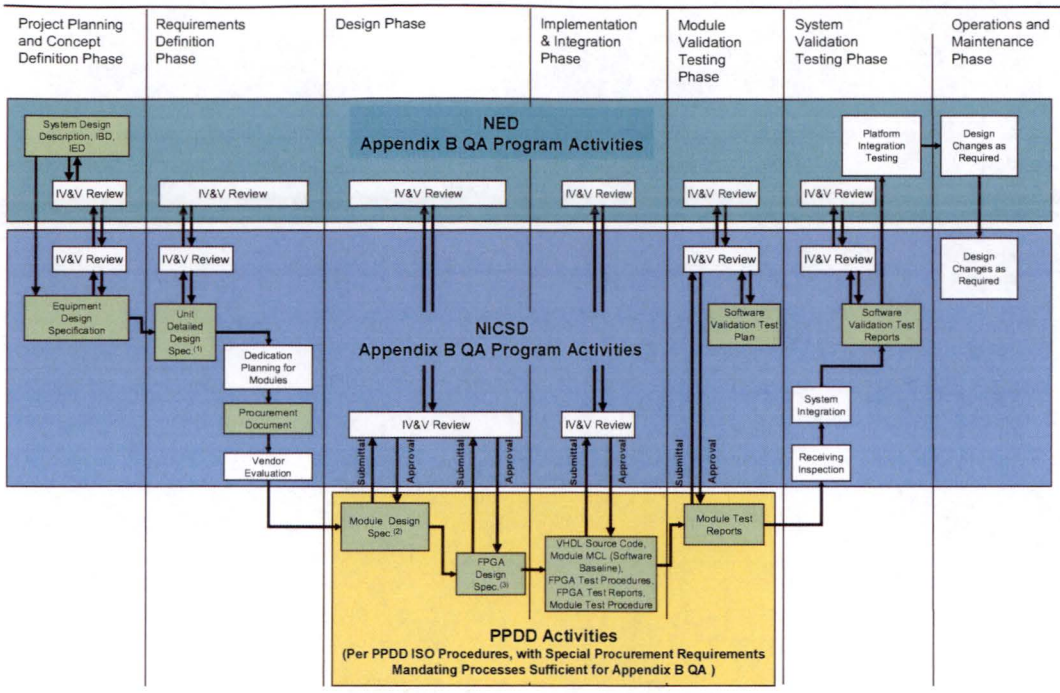
Section 4.3.1 of the SPP (Reference (18)) describes Management V&V Activities. The management of the V&V process is performed throughout the life cycle phase. Table 10 of the SPP defines the V&V management tasks, which are equivalent to the management tasks defined in IEEE Std 1012 (Reference (3)). Table 5-1 shows the corresponding activities to the management tasks in this NED V&V Plan (VVP).

**Table 5-1 V&V Management Activities for NED Scope**

| SPP Table 10 Tasks | Activity in this VVP |
|---|---|
| 1) Software Verification and Validation Plan (SVVP) Update | Establishment of this NED VVP |
| 2) Baseline Change Assessment | Activity Iteration Policy in Section 7.2 in this NED VVP covers the requirements of the Baseline Change Assessment. |
| 3) Management Review | The ICDD PM oversees the ICDD IV&V Team activities. |
| 4) Management and Technical Review Support | The ICDD IV&V Team should attend management meetings, and design reviews as necessary. In particular, NICSD holds a Process Review Meeting (PRM) every phase to ensure that the required activities during that phase were completed. The ICDD IV&V Team shall attend the PRM for management and technical support, as necessary. |
| 5) Organizational and Supporting Processes Interface | The ICDD IV&V Team shall attend the NICSD PRM and other project management meetings when the ICDD IV&V Lead considers necessary. The NQAD of NED will audit ICDD IV&V work when the NQAD determines such audits are needed. |

### 5.1.2 V&V Phases

Section 11 of the NED SMP (Reference (19)) defines the software life cycle for the FPGA-based Safety-Related I&C systems. Figure 5-1 illustrates the life cycle process for FPGA-based Safety-Related I&C systems.




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

**Figure 5-1 Life Cycle Process for FPGA-based Safety-Related I&C Systems**

The ICDD IV&V Team activities shall be performed for the lifecycle phases defined in the NED SMP. This NED VVP includes the life cycle phases from the Project Planning and Concept Definition Phase through the System Validation Testing Phase. This NED VVP ends after the System Validation Testing, prior to shipment from Toshiba. However, if any need for design change arises after finalizing the V&V activities, this NED VVP and the ICDDV&V activities shall be reactivated from the earliest phase affected by the change, and necessary activities shall be iterated. For design changes in the Operations and Maintenance Phase, another VVP will be prepared if necessary.

Table 5-2 shows the life cycle V&V activities and the responsible personnel for NED portion. Second column of Table 5-2 indicates the corresponding V&V activities in the SPP.

**Table 5-2 V&V Activities Assigned to Each Software Life Cycle (NED Portion)**

| This NED VVP | SPP | Project Planning and Concept Definition Phase V&V | Requirements Definition Phase V&V | Design Phase V&V | Implementation and Integration V&V | Module Validation Testing Phase V&V | System Validation Testing Phase V&V |
|---|---|---|---|---|---|---|---|
| Management Review of V&V, see Table 5-1 3) | Management Review of V&V | ICDD PM | ICDD PM | ICDD PM | ICDD PM | ICDD PM | ICDD PM |
| VVP Generation, see Section 5.2 | SVVP Generation | IV&V Lead | N/A | N/A | N/A | N/A | N/A |
| Document Review, see Section 5.2.1 | Concept Documentation Evaluation(1) | IV&V Lead | N/A | N/A | N/A | N/A | N/A |
| Document Review, see Section 5.2.1 | Program Plan Evaluation | IV&V Lead | N/A | N/A | N/A | N/A | N/A |
| RTM efforts, see Section 5.2.2 | Planning Traceability Analysis | IV&V Lead | (NICSD) | (NICSD) | (NICSD) | (NICSD) | IV&V Lead |
| Safety Analysis, see NED SMP | Hazard Analysis | ICDD SSL | ICDD SSL | ICDD SSL | ICDD SSL | ICDD SSL | ICDD SSL |
| Risk Analysis, see NED SMP | Risk Analysis | ICDD PM(2) | ICDD PM(2) | ICDD PM(2) | ICDD PM(2) | ICDD PM(2) | ICDD PM(2) |
| VVR, see Section 5.2 through 5.7 | Phase Summary Report(3) | IV&V Lead | IV&V Lead | IV&V Lead | IV&V Lead | IV&V Lead | IV&V Lead |
| Baseline Reviews Section 5.2 through 5.7 | Baseline Reviews | IV&V Lead | IV&V Lead | IV&V Lead | IV&V Lead | IV&V Lead | IV&V Lead |

(1) Conceptual documentation including the System Design Descriptions (SDDs), Interlock Block Diagrams (IBDs), and Instrumentation Electrical Diagrams (IEDs) are verified under Toshiba Power Systems Company Nuclear Energy Quality Assurance Program Description (QAPD) (Reference (5)), the standard QA program for US Safety-Related products.

(2) The IV&V Team reports risks identified in the V&V activities using the NED V&V Reports, see Section 5.2.3, 5.3.2, 5.4.2, 5.5.2, 5.6.3, 5.7.3

(3) In this qualification project, issue of phase summary report is not planned. Instead, the VVR includes the summary of V&V activities..

### 5.1.3 Interface with NICSD

(1) Review of NICSD V&V Documents by ICDD IV&V Team

The ICDD IV&V Team shall review and evaluate the following NICSD V&V documents, and the ICDD PM shall approve these documents in accordance with NED AS-200A010 "Control Procedure of vendor generated documents" (Reference (8)) using the Vendor generated Document Check List(VDCL).

- NICSD V&V Plan (VVP)
- NICSD V&V Report (VVR)

The reviewer of the ICDD IV&V Team shall review that the NICSD VVP and VVR are compliant with the procurement specification (Reference (20)) and this NED VVP. The reviewer shall describe the result of the review on the VDCL.

(2) Incorporation of NICSD V&V Reports to NED V&V Report

The ICDD IV&V Team shall review and incorporate NICSD VVRs to the NED VVRs issued for the same phases. Figure 5-2 shows the NED VVR preparation flow.

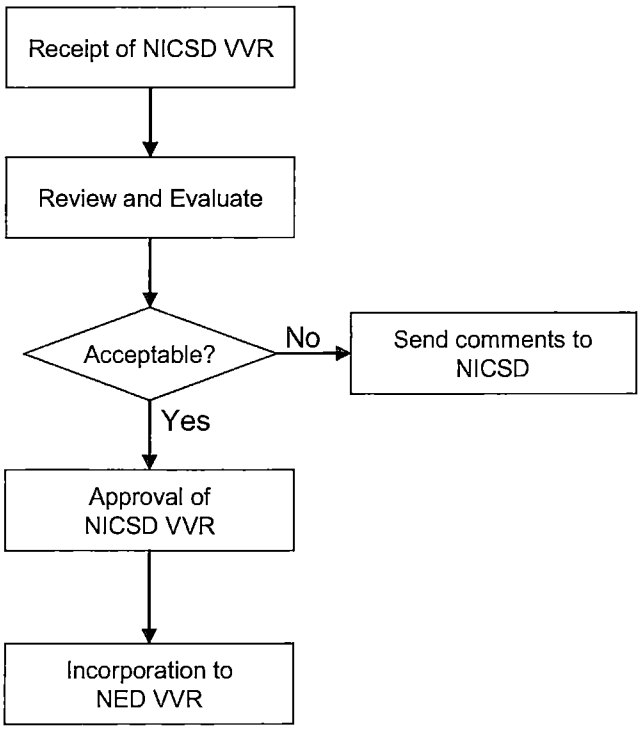



**Figure 5-2 NED V&V Report Preparation Flow**

If the NICSD VVR is not acceptable, the ICDD IV&V Team will send comments to NICSD. NICSD shall take appropriate comment resolution actions, and update the NICSD VVR. The ICDD IV&V Team shall iterate review and evaluate process in Figure 5-2 on the updated NICSD VVR.

### 5.1.4 Use of Commercial Software

The ICDD IV&V Team will not use any commercial software except standard business software tools widely used in the project.

### 5.1.5 Control of Inputs and Outputs Documents for V&V activities

As described in the following subsections, the ICDD IV&V Team performs V&V activities for each life cycle phase, where the inputs to the V&V activities includes the design, planning and reporting documents and the RTM. Each VVR shall identify these inputs and the independent reviewers for the documents. Table-A of the NED SMP (Reference (19)) provides a summary of the outputs of ICDD V&V activities for each life cycle phase. To identify the output documents, the ICDD IV&V Team referrers to the Project Control Document List (PCDL), which is produced in accordance with NED AS-100A004 "Document Control Procedure" (Reference (6)) and updated throughout the life cycle. The PCDL includes the following items:

- Toshiba internal document number and revision number,
- Document title,
- Issue Date, and
- Names of preparer and approver.

The ICDD IV&V Team shall identify the revision number of the PCDL in the BRRs.

## 5.2 Project Planning and Concept Definition Phase

During this phase, ICDD generates the System Design Descriptions (SDDs), Interlock Block Diagrams (IBDs), and Instrumentation Electrical Diagrams (IEDs). The ICDD IV&V Team should assess control of these documents considered as the ICDD configuration management (CM) process, and confirm that the CM activities comply with the project document "Project Specific Document Control Procedure" (Reference (17)), and NED AS-100A004 "Document Control Procedure" (Reference (6)).

The ICDD IV&V Team shall prepare the NED VVP (this document) in accordance with NED AS-200A130 (Reference (12)) that defines V&V activities throughout the software life cycle. The NED VVP shall be controlled and retained in accordance with NED AS-100A004 (Reference (6)).

### 5.2.1 Document Reviews

The ICDD IV&V Team shall review the following documents:

- NED VVP
- SDD
- IBD
- IED
- NED Software Safety Analysis Report (NED SSAR)
- NICSD VVP
- NICSD V&V Report (NICSD VVR) (See Section 5.2.3)
- NED V&V Report (NED VVR) (See Section 5.2.3)

For the procedures to be used for the document review, see Section 4.6.1 in this NED VVP.

### 5.2.2 Project Planning and Concept Definition Phase RTM efforts

(1) Preparation of the RTM

ICDD design engineers shall prepare the Project Planning and Concept Definition Phase RTM for SDDs, IBDs and IEDs.

The RTM preparer(s), the design engineer(s) who prepares the RTM, shall collects the base requirements from the plant specific documents and the customer requirements.

After the RTM is delivered to NICSD, the NICSD RTM preparer(s), or design engineers shall trace the base requirements in the ICDD documents to the Equipment Design Specification (EDS), and traced the EDS requirements back to the upper requirements.

The RTM efforts ensure the following:

- The requirements are traced "forwards" from the upstream documents to the downstream documents.
- The downstream requirements are traced back to the upstream documents.

(2) Compilation of the Project Planning and Concept Definition Phase RTM

The ICDD RTM Preparer(s) summarize open items revealed by the RTM efforts. The ICDD design engineers must resolve these items to the satisfaction of the RTM preparer(s).

The ICDD IV&V Team shall review the RTM for their portions. In the review of the RTM, the ICDD IV&V Team shall ensure that all entries are complete and unambiguous, and also contain sufficient details. Snapshots of the RTM that are reviewed shall be retained as review records. The ICDD IV&V Team shall document a summary of the RTM review in the NED VVR including the reference to the RTM snapshots.

### 5.2.3 Project Planning and Concept Definition Phase V&V Reporting

The ICDD IV&V Team shall document the V&V activities in the NED VVR for Project Planning and Concept Definition Phase, which includes:

(1) References to the reviewed documents

(2) References to the Design Verification Reports (DVR)

(3) Reference to the Project Planning and Concept Definition Phase RTM (ICDD portion) snapshot

(4) Summary of the ICDD portion of the RTM review including the open items and resolutions to the items

(5) Evaluation of the NICSD VVR for the Project Planning and Concept Definition Phase

(6) Metrics described in Section 4.6.4

(7) Result of the ICDD Configuration Management (CM) process assessment

(8) Any findings, recommendations, or suggestions to reduce any risks identified in the V&V activities

### 5.2.4 Baseline Review and Disposition of Nonconformances

The ICDD IV&V Team shall perform a baseline review for this Project Planning and Concept Definition Phase, as describe in Section 4.6.3.

The ICDD IV&V Team shall issue a Baseline Review Report (BRR) documenting the results of the baseline review.

## 5.3 Requirements Definition Phase

### 5.3.1 Document Reviews

The ICDD IV&V Team shall review the following documents:

- NED SSAR
- NICSD VVR
- NED VVR (See next section)

For the procedures to be used for the document review, see Section 4.6.1 in this NED VVP.

### 5.3.2 Requirements Definition Phase V&V Reporting

The ICDD IV&V Team shall update the NED VVR, by adding the descriptions on this phase activities. The descriptions shall include:

(1) Evaluation of the NICSD VVR for Requirements Definition Phase

(2) Any findings, recommendations, or suggestions to reduce any risks identified in the V&V activities

### 5.3.3 Baseline Review

The ICDD IV&V Team will participate in the NICSD baseline review of this phase.

## 5.4 Design Phase

### 5.4.1 Document Reviews

The ICDD IV&V Team shall review of the following documents:

- NED SSAR
- NICSD VVR
- NED VVR (See next section)

For the procedures to be used for the document review, see Section 4.6.1 in this NED VVP.

### 5.4.2 Design Phase V&V Reporting

The ICDD IV&V Team shall update the NED VVR, by adding the descriptions on this phase activities. The descriptions shall include:

(1) Evaluation of the corresponding NICSD VVR

(2) Any findings, recommendations, or suggestions to reduce any risks identified in the V&V activities

### 5.4.3 Baseline Review

The ICDD IV&V Team will participate in the NICSD baseline review of this phase.

## 5.5 Implementation and Integration Phase

### 5.5.1 Document Reviews

The ICDD IV&V Team shall review of the following documents:

- NED SSAR
- NICSD VVR
- NED VVR (See next section)

For the procedures to be used for the document review, see Section 4.6.1 in this NED VVP.

### 5.5.2 Implementation and Integration Phase V&V Reporting

The ICDD IV&V Team shall update the NED VVR, by adding the descriptions on this phase activities. The descriptions shall include:

(1) Evaluation of the NICSD VVR Implementation and Integration Phase

(2) Any findings, recommendations, or suggestions to reduce any risks identified in the V&V activities

### 5.5.3 Baseline Review

The ICDD IV&V Team will participate in the NICSD baseline review of this phase.

## 5.6 Module Validation Testing Phase

### 5.6.1 Document Reviews

The ICDD IV&V Team shall review of the following documents:

- NED SSAR
- NICSD VVR
- NED VVR (See next section)

For the procedures to be used for the document review, see Section 4.6.1 in this NED VVP.

### 5.6.2 Assessment of Test Equipment Software

The NICSD IV&V Team shall assess the PPDD control of the test equipment software, used in the Module Validation Testing. The NICSD IV&V Team shall review PPDD's records for test equipment software control to ensure that test equipment software used for the project is prepared in accordance with procedures that the NICSD has reviewed and approved.

The ICDD IV&V Team will participate in the assessment if the ICDD IV&V Lead deems it necessary.

### 5.6.3 Module Validation Testing Phase V&V Reporting

The ICDD IV&V Team shall update the NED VVR, by adding the descriptions on this phase activities. The descriptions shall include:

(1) Evaluation of the NICSD VVSR

(2) Any findings, recommendations, or suggestions to reduce any risks identified in the V&V activities

### 5.6.4 Baseline Review

The ICDD IV&V Team will participate in the NICSD baseline review of this phase.

## 5.7 System Validation Testing Phase

### 5.7.1 Document Reviews

The ICDD IV&V Team shall review of the following documents:

- NED SSAR
- NICSD VVR
- NED VVR

For the procedures to be used for the document review, see Section 4.6.1 in this NED VVP.

### 5.7.2 Assessment of Test Equipment Software

The NICSD IV&V Team shall assess the NICSD control of the test equipment software, used in the units and system validation testing. The NICSD IV&V Team shall review NICSD's records for test equipment software control to ensure that the test equipment software used for the tests is controlled in accordance with NQ-2003 (Reference (16)). The ICDD IV&V Team will participate in the assessment.

### 5.7.3 System Validation Testing Phase V&V Reporting

The ICDD IV&V Team shall finalize the NED VVR documenting the V&V activities from the Project Planning and Concept Definition Phase through the System Validation Testing Phase. All pertaining nonconformances shall be disposed of before the issue of the final NED VVR.

The final NED VVR shall include:

(1) Evaluation of the final NICSD VVR

(2) V&V activities completed, including V&V methods used

(3) Completion of the final NED SSAR, which shall confirm that:

- All system safety requirements have been satisfied by the life cycle phases.
- No additional hazards have been introduced by the work done during the life cycle activity.

(4) Any deviation from this NED VVP

(5) Summary of results including evaluation of metrics and assessment of software quality

(6) Compliance demonstration for each requirement

(7) Summary of anomalies, resolutions, and current anomaly status

(8) Summary of identified risks, and resolutions

(9) Configuration of the FPGA-based Safety-Related I&C system tested

(10) Recommendations

(11) Conclusion of the V&V activities

It should be noted that the software development is not complete until the specified V&V

activities have been completed, and the consistency of the developed software with the design documentation is confirmed through the V&V activities.

### 5.7.4 Baseline Review

The ICDD IV&V Team will participate in the NICSD baseline review of this phase.

The ICDD IV&V Team shall perform the final baseline review to complete the software development including the V&V activities. The ICDD IV&V Team shall issue a Baseline Review Report (BRR) documenting the results of this final baseline review.

### 5.7.5 Platform Integration Test and Site Acceptance Test

After the validation testing, Toshiba will ship the FPGA-based Safety-Related I&C systems to the US nuclear power plant for Site Acceptance Test (SAT) by customer. If the customer requests, the systems will be integrated other I&C systems and subjected to a Platform Integration Test (PIT) prior to installation to the nuclear power plant. If any need for design change arises during the PIT or SAT, the change shall be made in accordance with NED AS-200A015 "Design Change Control Procedure" (Reference (9)), and necessary V&V activities shall be reactivated and iterated from the earliest phase affected by the change. The ICDD IV&V Team shall update the necessary documents in accordance with the policy prescribed in Section 7.2 of this NED VVP in that case.

# 6 V&V Reporting

## 6.1 V&V Report

The ICDD IV&V Team prepares the NED VVR, which documents the ICDD V&V activities from the Project Planning and Concept Definition Phase through the System Validation Phase. The NED VVR also includes evaluation of the NICSD VVR. The NED VVR is first prepared at the Project Planning and Concept Definition Phase, and is updated at the end of each life cycle phase. Section 5.7.3 describes the contents to be included in this NED VVR.

It should be noted that even after the System Validation Testing Phase is completed, the VVR needs to be updated if some of the V&V activities have been iterated.

The ICDD PM shall approve above NED VVR. The ICDD PM shall submit the NED VVR to the customer for review and approval according to the customer's request.

## 6.2 Anomaly Reporting

Corrective Action Request (CAR) and Nonconformance Notice Report (NNR) are used for anomaly reporting. Section 7.1 explains CAR and NNR.

# 7 V&V Administrative Requirements

## 7.1 Anomaly Reporting and Resolution

### 7.1.1 Nonconformance Notice Report

If an anomaly is found for the FPGA-based Safety-Related I&C systems that will be shipped and used in US nuclear power plants, the anomaly is controlled in accordance with NED applicable AS Standards. In case that the anomaly is judged nonconforming parts, modules, units or systems (hardware) of which cause is generated by NED, Noncomformance Notice Report (NNR) is issued in accordance with NED AS-300A008 "Nonconformance Control and Corrective Action Procedure" (Reference (14)). In case that procurement modules, units or systems that do not meet NED procurement documents, Vendor NNR is used in accordance with NED AS-300A006 "Nonconformance Control Procedure for Procured Items and Services" (Reference (13)) to control. Anomalies on modules, units, or systems which are products of pre-established baselines are controlled in accordance with Section 4.6.1 (in case of NED caused anomalies) or Section 5.1.3 (in case of NICSD caused anomalies).

### 7.1.2 Corrective Action Request

A Corrective Action Request (CAR) is used to document a cause, corrective action to be taken, and to follow corrective action processes, when a condition adverse to quality is identified in PCDs of the established baseline. Anomalies on pre-established baseline documents are controlled in accordance with Section 4.6.1 (in case of NED documents) or Section 5.1.3 (in case of NICSD submittal documents).

The organizations and personnel responsible for corrective action process are described in NED AS-300A009 "Corrective Action Request Application Procedure" (Reference (15)).

## 7.2 Activity Iteration Policy

If a verified design is changed, the V&V activities for the changed portion shall be iterated. The V&V activities to be repeated shall be documented, reviewed, and approved in accordance with the corrective action process described in Section 7.1.2.

Changes to the design described in the ICDD design documents are controlled in accordance with NED AS-200A015 "Design Change Control Procedure" (Reference (9)). AS-200A015 prescribes a change control procedure consisting of change proposal, evaluation of the change, and authorization of change. In a change proposal, the design change is specified in a Design Change Notice (DCN) which includes the change item, current design, previous design, and the reason of the change.

For changes that are controlled by the RTMs, the effects caused by the change shall be traced using the RTM, and necessary design, development, safety analysis, or V&V activities shall be iterated for the affected portions. The iteration includes review of NED SSARs and NICSD VVRs, updates of the RTM and NED VVRs.

## 7.3 Deviation Policy

Deviation from this NED VVP will be necessary, if the planned items defined in Section 1 through 8 are changed. For example, one or more of the following situations will cause a deviation.

- Purpose or scope in Section 1 needs to be changed.

- Reference documents described in Section 2 are changed.
- The organization described in Section 4.1 needs to be changed.
- The one or more of the activities planned in Section 5 cannot be performed.

If deviation from this NED VVP is necessary, this NED VVP shall be updated through the same review and approval process by which this NED VVP was originally created.

The updated NED VVP shall be reviewed and approved in Toshiba, and get accepted by the customer according to the customer's request.

The information required for deviations shall identify activities to be deviated, and shall include rationale and effect on software quality.

Partial use of the V&V activities defined in Section 5 is permissible, as long as conditions described in Section 1 through 4, 6, and 7 are met. For example, this NED VVP can be used as a VVP for the V&V activities that are performed to resolve issues identified by an NNR or CAR for a previously developed product.

## 7.4 Control Procedures

The ICDD IV&V Team performs the V&V activities in accordance with Toshiba Power Systems Company Nuclear Energy (PSNE) Quality Assurance Program Description (QAPD) (Reference (5)), which is the standard Toshiba QA program applied for US Safety-Related products. PSNE established the quality system document structure which includes the NED "AS" standards. "AS" standards are used as control procedures.

## 7.5 Standards, Practices and Conventions

Toshiba Internal Documents in Section 2.4, and project documents in Section 2.5 shall be applied for the V&V activities. IEEE standards in Section 2.3 are used as guidance.

# Table A Compliance to SPP

Section 4 of the Software Program Plan (SPP) (Reference (18)) describes Software Verification and Validation Program Plan. Table A shows compliance to Section 4 of the SPP.

**Table A Compliance to Section 4 of the SPP**

| No | SPP Section | Title | VVP Section(s) | Remark |
|---|---|---|---|---|
| 1 | 4 | Software Verification and Validation Program Plan (SVVPP) | N/A | Section Title |
| 2 | 4.1 | Introduction | N/A | No requirement for this VVP |
| 3 | 4.1.1 | Purpose | 1.1 | |
| 4 | 4.1.2 | Scope | 1.2, 4.5, 4.6.3, 5.1.3 | |
| 5 | 4.1.3 | [Deleted] | --- | --- |
| 6 | 4.1.4 | Relationship of the SVVPP to Other SPP Sections | N/A | No requirement for this VVP |
| 7 | 4.2 | Verification and Validation Overview | 1 | |
| 8 | 4.2.1 | Organization | 4.1 | |
| 9 | 4.2.2 | Schedule | 4.2 | |
| 10 | 4.2.3 | Resource Summary | 4.4 | |
| 11 | 4.2.4 | Roles and Responsibilities | 4.5 | |
| 12 | 4.2.5 | Qualifications | 4.4, 4.5 | |
| 13 | 4.2.6 | Tools, Techniques, and Methodologies | 4.6 | |
| 14 | 4.3 | Life Cycle Verification and Validation | 5 | |
| 15 | 4.3.1 | Management of V&V Activities | 5.5.1 | |
| 16 | 4.3.2 | Planning Phase V&V Activities | 5.2 | |
| 17 | 4.3.3 | Requirements Phase V & V Activities | 5.3 | |
| 18 | 4.3.4 | Design Phase V & V Activities | 5.4 | |
| 19 | 4.3.5 | Implementation Phase V & V Activities | 5.5 | |
| 20 | 4.3.6 | Testing and Integration Phase V & V Activities | 5.5, 5.6, 5.7 | |
| 21 | 4.3.7 | Installation Phase V & V Activities | N/A | See Section 12 of NED SMP |
| 22 | 4.3.8 | Operation Phase V & V Activities | N/A | See Section 5.1.2 |
| 23 | 4.3.9 | Maintenance Phase V & V Activities | N/A | See Section 5.1.2 |
| 24 | 4.3.10 | Summary of V&V Activities | N/A | No requirement for this VVP |
| 25 | 4.3.11 | Previously Developed or Purchased Software | 5.1.4 | |
| 26 | 4.4 | V & V Reporting and Administrative Requirements | N/A | Section Title |
| 27 | 4.4.1 | Reporting For Each System or Logical Group of Systems | 6 | |

**Table A Compliance to Section 4 of the SPP**

| No | SPP Section | Title | VVP Section(s) | Remark |
|---|---|---|---|---|
| 28 | 4.4.2 | Anomaly Reporting and Resolution | 6.3 | |

Notice: The definition of phase for the FPGA-Based Safety-Related I&C systems differs from that in the SPP, see the NED SMP (Reference (19)).