ENCLOSURE 4

FA32-3702-0005 Rev. 2
Nuclear Energy Systems and Services Division
FPGA-based Safety-Related Systems Software Management Plan

Non-Proprietary

US Safety-Related

Toshiba Project Document No.	Rev. No.
FA32-3702-0005	2

NRW-FPGA-Based I&C System Qualification Project
Software Management Plan

Title: Nuclear Energy Systems and Services Division FPGA-based Safety-Related Systems Software Management Plan

Customer Name	None
Project Name	NRW-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
2	Mar 7, 2013	See DCN-FA32-3702-0005-02	T.Maekawa Mar 7, 2013	T.Miyazaki Mar 7, 2013	K.Sato Mar.7, 2013

Initial Issue Date	Issued by	Approved by	Reviewed by	Prepared by	Document filing No.
Oct 25,2011	Monitoring System Engineering Group Instrumentation & Control Systems Design & Engineering Dept.	T.Maekawa Oct 25, 2011	T.Miyazaki Oct 25, 2011	K.Sato Oct 25, 2011	RS-5156635

Record of Revisions

Rev No.	Date	History	Approved by	Reviewed by	Prepared by
0	See cover page	Initial Issue	See cover page	See cover page	See cover page
1	July 31,2012	See DCN-FA32-3702-0005-01	T.Maekawa July 31,2012	T.Miyazaki July 31,2012	K.Sato July 31,2012
2	See cover page	See DCN-FA32-3702-0005-02	See cover page	See cover page	See cover page

Table of Contents

1 Purpose

This Nuclear Energy Systems and Services Division (NED) Software Management Plan (NED SMP) describes the process to be followed by NED for the Non-Rewritable (NRW) FPGA-Based Safety-Related Instrumentation and Control (I&C) systems for US nuclear power plants.

NED establishes the system design of FPGA-based Safety-Related I&C systems, and procures the FPGA-based equipment from Toshiba Fuchu-PS Nuclear Instrumentation and Control Systems Department (NICSD).

Software development mostly occurs at NICSD. This NED SMP combined with the project document "NED Verification and Validation Plan" (NED VVP) (Reference (21)) and other software planning documents prepared by NICSD augment Quality Assurance (QA) requirements in the Toshiba Power Systems Company Nuclear Energy (PSNE) Quality Assurance Program Description (QAPD) (Reference (3)). The PSNE QAPD is the standard Toshiba QA program applied for US Safety-Related products. Since most software development activities occur at NICSD, there are only a limited number of software activities performed by NED. This SMP defines the management activities for this limited scope.

- Management process, including organization and responsibilities; the procedures to be used, and the methods for conducting software safety analyses;
- Methods, tools, and techniques used in the software safety analyses.

The Instrumentation and Control Systems Design and Engineering Department (ICDD) of NED is responsible for the I&C system design documents including System Design Descriptions (SDDs), Interlock Block Diagrams (IBDs) and Instrumentation Electrical Diagrams (IEDs) for FPGA-based Safety-Related I&C systems. These documents are input to the software design process at NICSD.

2 Scope

This NED SMP is prepared for FPGA-based Safety-Related I&C systems for US nuclear power plants.

Project document "Software Program Plan" (SPP) (Reference (20)) establishes requirements and provides guidance and expectations for the design, development, implementation, safety analysis, review, testing, installation, and configuration management of supporting software program plans, e.g., this NED SMP.

This NED SMP complies with the following sections of the SPP:

- Section 1, Introduction
- Section 2, Software Project Management Program Plan
- Section 6, Software Safety Program Plan

The NED VVP (Reference (21)) covers Section 4 of the SPP, and the following SPP sections do not apply to NED, because they are implemented only at NICSD:

- Section 3, Software Development Program Plan
- Section 5, Software Quality Assurance Program Plan
- Section 7, Software Configuration Management Program Plan
- Section 10, Software Training Program Plan

NICSD prepares the following planning documents complying with the above SPP sections

that are outside scope of this NED SMP and NED VVP:

- NRW-FPGA-Based I&C System Qualification Project, FA32-3702-1000 "Nuclear Instrumentation & Control Systems Department Software Management Plan for FPGA-based Safety-Related Systems" (NICSD SMP) (Reference (22))
- NRW-FPGA-Based I&C System Qualification Project, FA32-3701-1001 "Nuclear Instrumentation & Control Systems Department Software Quality Assurance Plan for FPGA-based Safety-Related Systems" (NICSD SQAP) (Reference (23))
- NRW-FPGA-Based I&C System Qualification Project, FA32-3708-1000 "Nuclear Instrumentation & Control Systems Department Software Configuration Management Plan for FPGA-based Safety-Related Systems" (NICSD SCMP) (Reference (24))
- NRW-FPGA-Based I&C System Qualification Project, FA32-3709-1000 "Nuclear Instrumentation & Control Systems Department Verification and Validation Plan for FPGA-based Safety-Related Systems" (NICSD VVP) (Reference (25))

This NED SMP shall be implemented by NED using NED AS standards. NICSD shall prepare the NICSD SMP.

If changes within the NED scope are required, the NED plans will be applied.

3 Acronyms

ABWR	Advanced Boiling Water Reactor
BRR	Baseline Review Report
BTP	Branch Technical Position
CFR	Code of Federal Regulations
DVR	Design Verification Report
FPGA	Field Programmable Gate Array
GPM	Group Manager
I&C	Instrumentation and Control
IBD	Interlock Block Diagram
ICDD	Instrumentation & Control Systems Design & Engineering Department
IED	Instrumentation Electrical Diagram
IR	Independent Review
ISRG	Information Security Rules and Guidelines
IV&V	Independent V&V
MCL	Master Configuration List
NED	Nuclear Energy Systems & Services Division
NICSD	Toshiba Fuchu-PS, Nuclear Instrumentation & Control Systems Department
NICS-QA	Quality Assurance Group for Nuclear Instrumentation & Control Systems
NQAD	Nuclear Quality Assurance Department
NRW	Non-Rewritable
PFT	Platform Factory Test

PIT	Platform Integration Test
PM	Project Manager
PPDD	Power Platform Development Department
PSNE	Power Systems Company Nuclear Energy
QA	Quality Assurance
QAG	Quality Assurance Group
QAPD	QA Program Description
RTM	Requirements Traceability Matrix
SDD	System Design Description
SDOE	Secure Development and Operational Environment
SES	Sub-master Engineering Schedule
SM	Senior Manager
SMP	Software Management Plan
SPP	Software Program Plan
SSAR	Software Safety Analysis Report
USNRC	United States Nuclear Regulatory Commission
V&V	Verification and Validation
VVP	V&V Plan
VVR	V&V Report

4 References

(1) USNRC, NUREG-0800 Branch Technical Position (BTP) 7-14
"Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems" Rev.5

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

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

(4) Toshiba Corporation, Power Systems Company Nuclear Energy Systems and Services Division 4401-5
"NED QA Manual," Toshiba Corporation, Power Systems Company

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

(6) Toshiba Nuclear Energy Systems and Services Division AS-100A008
"Procedure for Indoctrination and Training"

(7) Toshiba Nuclear Energy Systems and Services Division AS-200A005
"Design Review Meeting Convening Standard"

(8) Toshiba Nuclear Energy Systems and Services Division AS-200A014
"Procedure for Documentation of Design Inputs"

(9) Toshiba Nuclear Energy Systems and Services Division AS-200A016
"Subcontracting Procedure from NED to Other Organizations within Toshiba Corporation"

(10)Toshiba Nuclear Energy Systems and Services Division AS-200A017
"Design Planning Procedure"

(11)Toshiba Nuclear Energy Systems and Services Division AS-200A114
"Preparation Procedure for System Design Description"

(12)Toshiba Nuclear Energy Systems and Services Division AS-200A121
"Preparation Procedure for Interlock Block Diagram (IBD)"

(13)Toshiba Nuclear Energy Systems and Services Division AS-200A122
"Preparation Procedure for Instrumentation Electrical Diagram (IED)"

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

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

(16)Toshiba Nuclear Energy Systems and Services Division AS-200A131
"Digital System Configuration Management Procedure"

(17)Toshiba Nuclear Energy Systems and Services Division AS-200A132
"Digital System Safety and Hazards Analysis Procedure"

(18)Toshiba Nuclear Energy Systems and Services Division AS-300A012
"Internal Audit Procedure"

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

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

(21)NRW-FPGA-Based I&C System Qualification Project, FA32-3709-0001
"Nuclear Energy Systems and Services Division FPGA-based Safety-Related Systems Verification and Validation Plan" Rev.2

(22)NRW-FPGA-Based I&C System Qualification Project, FA32-3702-1000
"Nuclear Instrumentation & Control Systems Department Software Management Plan for FPGA-based Safety-Related Systems" Rev. 0

(23)NRW-FPGA-Based I&C System Qualification Project, FA32-3701-1001
"Nuclear Instrumentation & Control Systems Department Software Quality Assurance Plan for FPGA-based Safety-Related Systems" Rev.1

(24)NRW-FPGA-Based I&C System Qualification Project, FA32-3708-1000
"Nuclear Instrumentation & Control Systems Department Software Configuration Management Plan for FPGA-based Safety-Related Systems" Rev. 1

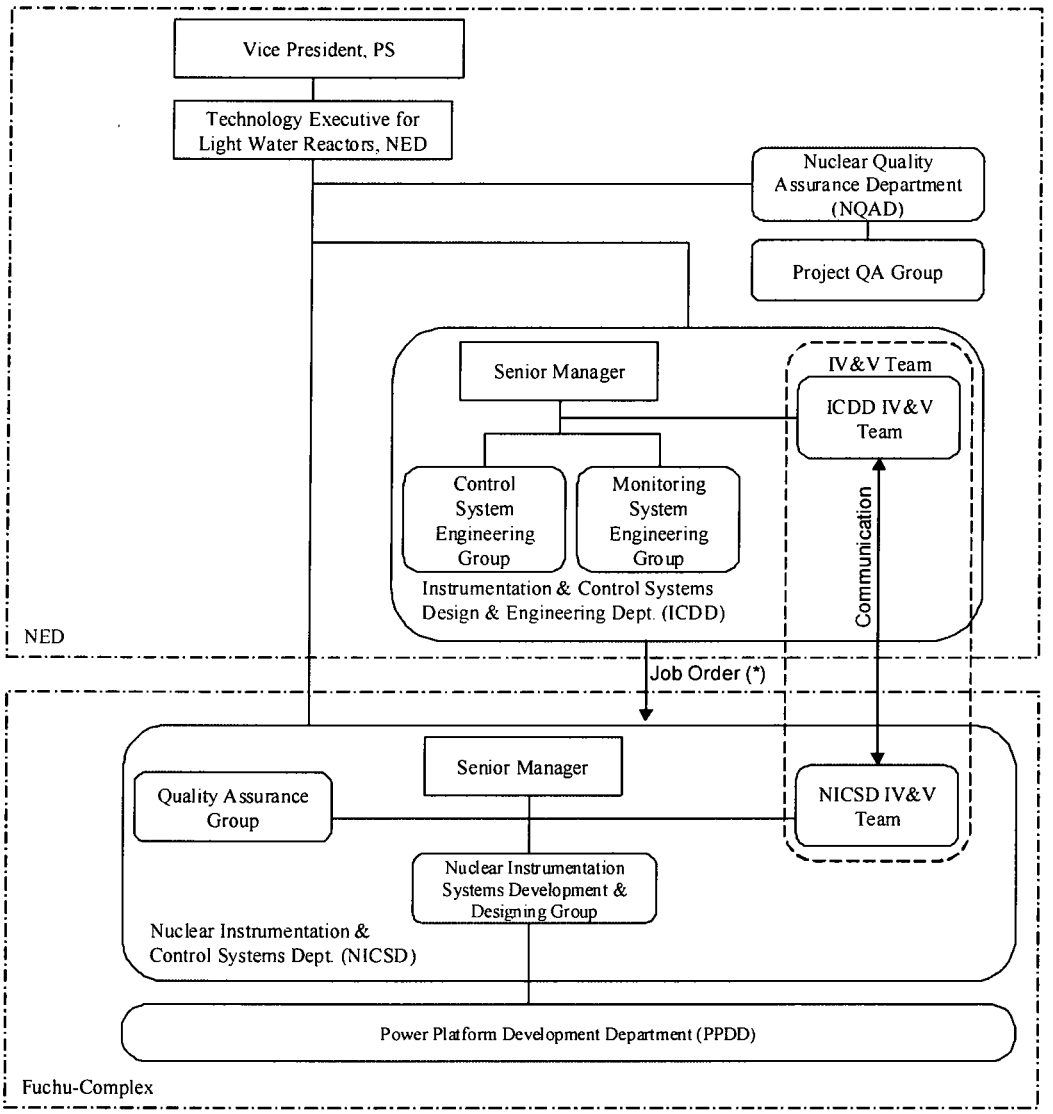
(25)NRW-FPGA-Based I&C System Qualification Project, FA32-3709-1000
"Nuclear Instrumentation & Control Systems Department Verification and Validation Plan for FPGA-based Safety-Related Systems" Rev.5

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

5 Organizations and Responsibilities

5.1 Organizations

Figure 5-1 shows the organizations responsible for development of the FPGA-based Safety-Related I&C systems software design. The Instrumentation and Control Systems Design and Engineering Department (ICDD) of NED is responsible for FPGA-based Safety-Related I&C system design documents. There are two groups in ICDD, the Control System Engineering Group and Monitoring System Engineering Group responsible for design and development of FPGA-based Safety-Related I&C systems. These two groups are referred as "engineering/design group" in this NED SMP.



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

Figure 5-1 Organizations for FPGA-based Safety-Related I&C Systems

The Nuclear Quality Assurance Department (NQAD) of NED is responsible for quality assurance in NED. Responsibilities for the NQAD are assigned in the standard QA Program.

NICSD has their own set of software plans to augment their QA requirements. NICSD is responsible for detailed design of FPGA-based equipment, procures the modules for the FPGA-based equipment from the Power Platform Development Department (PPDD), and assembles the FPGA-based equipment from the modules. The Quality Assurance Group in NICSD (NICS-QA) is responsible for QA in NICSD.

Engineers from ICDD and NICSD organize Independent Verification and Validation (IV&V) Teams for the V&V of the FPGA logic. The engineers from ICDD and the engineers from NICSD in the IV&V Teams communicate with each other, and work together as one IV&V Team as needed for the quality of the products.

5.2 Responsibilities

This section identifies the only required responsibilities for software life cycle at NED. The other positions defined in the SPP are not required.

NED Project Manager

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

The NED PM assigns the Independent Verification and Validation (IV&V) Lead and other V&V personnel in the ICDD IV&V Team, in accordance with NED AS-200A017 "Design Planning Procedure" (Reference (10)) and ensures independence of the ICDD IV&V Team from the design groups. The NED PM assigns the ICDD System Safety Lead to ensure independence of the ICDD System Safety Lead. The NED PM shall ensure financial independence of V&V activities and Safety activities from design activities.

ICDD System Safety Lead

The ICDD System Safety Lead shall be responsible for the system safety analysis, personnel training for safety analysis staff, and planning of safety analysis contained in this NED SMP. The ICDD System Safety Lead shall assign individuals responsible for specific system safety activities, as necessary. The ICDD System Safety Lead shall ensure that NICSD is aware of plant requirements provided directly or indirectly in the Job Order Sheet, and shall be responsible for ensuring compliance of NICSD Software Safety Plan to the NED Software Safety Plan described in Section 11 of this NED SMP.

The ICDD System Safety Lead, the ICDD IV&V Lead, and the NED PM shall all be different people ensuring independence among the organizations.

Group Manager

Each Group Manager (GPM) of the Control System Engineering Group and Monitoring System Engineering Group is responsible for system development, and personnel training except training for safety analysis.

IV&V Lead

The ICDD IV&V Lead shall be responsible for the V&V activities of NED and NICSD. the ICDD IV&V Lead is assigned by the NED PM. The ICDD IV&V Team shall perform the V&V activities technically, managerially, and financially independent of the system

development. The ICDD IV&V Team shall oversee the software safety activities ensuring independence of the activities, review the Software Safety Analysis Reports (SSARs), and perform baseline reviews.

Table-A lists the activities and the personnel who are responsible for the activities. The table also provides the cross reference to the applicable AS-standards, which describe the roles and responsibilities for ICDD.

Customer Support Lead

The NED PM shall be also responsible for the customer support activities.

The each manager and lead can designate staff for defined aspects of their roles. The person holding the responsible position shall be able to designate staff for defined aspects of their roles. The person holding the responsible position shall always be responsible for the actions and decisions of their designated staff.

The each manager and lead or their designate staff shall review this NED SMP.

5.3 Interfaces with Other Organization

The FPGA-based Safety-Related I&C system have the following interface items designed outside this FPGA-based Safety-Related I&C system project scope:

1) Sensor design specification,
2) Communication specification with other I&C systems in the nuclear power plant, and
3) Hardware indications, switches in the Main Control Console or local panels.

These interface items are designed by organizations within or outside Toshiba. The NED PM shall be responsible for interfacing with these organizations. Under the NED PM, ICDD shall make necessary arrangement with the organizations in order to determine the interface specifications with FPGA-based Safety-Related I&C systems. The interface specifications shall be described or delineated in SDDs, IBDs, IEDs, or Inputs and Outputs lists, which are included in the procurement specification of the FPGA-based Safety-Related I&C system being sent to NICSD.

6 QA Programs and Procedures

Toshiba Power Systems Nuclear Energy (PSNE) has a QA Program complying with the US nuclear safety regulations. The PSNE QAPD (Reference (3)) is compliant to 10 CFR 50 Appendix B and establishes the quality system document structure which includes the NED "AS" standards. Design procedures are defined in the AS standards. In addition, NED established the NED QA Manual (Reference (4)). ICDD works under the PSNE QAPD and the NED QA Manual using the AS standards. NQAD performs QA activities including internal audits.

ICDD requires NICSD to work under the NICSD QA program, complying with US nuclear safety regulations. NQAD shall perform audits of NICSD in accordance with AS-300A012 "Internal Audit Procedure" (Reference (18)).

7 Management Process

Project management occurs throughout the software life cycle for preparing and maintaining the design documents, including SDDs, IBDs and IEDs at NED. In addition to the schedule, budget, and resource metrics that the NED PM shall generate, maintain, and use for process

correction and control, the NED PM shall ensure that appropriate metrics are generated, and used for appropriate process correction and control.

The project phases included in this NED SMP are as follows:

- Initiation – The project begins with the award of a contract.
- Planning and scheduling – The NED PM is responsible for defining, planning, scheduling, costing, and resourcing the project, with the assistance and data provided by the appropriate management and technical staff who are to be assigned to the project in NED.
- Execution – Processes are performed in accordance with this NED SMP.
- Closeout – Finalize the project or task and complete delivery in accordance with the applicable contract.

Project monitoring and controls are important throughout the project life cycle. This NED SMP describes project control mechanisms applied in each phase as follows:

Initiation – The NED PM shall be responsible for producing the preliminary schedule, which shall consider resource availability and allocate these resources according to the approved schedule and budget.

Planning and Scheduling – The NED PM shall be responsible for developing the process model, schedule, design inputs and outputs, deliverables, QA requirements and resource allocation in NED. Resources for the V&V and software safety activities shall be considered in the resource allocation.

Project management systems used to accomplish these activities are described in Section 8.1 of this NED SMP. The NED PM shall verify that all software tools that NED uses are listed, including the software version as needed, and accepted for their intended use. Work packages including issued documents at NED are design documents and include SDDs, IBDs and IEDs which are inputs to the NICSD work for software development and the Job Order Sheets to NICSD to procure FPGA based equipment from NICSD. NQAD will conduct review of the NED procurement documents. NED Engineering Information Systems Department will be responsible for retaining the records.

Execution –ICDD is responsible for defining the work breakdown structure. The organizational work breakdown structure is shown in Figure 5-1. The NED PM is responsible to convene design review meetings in accordance with AS-200A005 "Design Review Meeting Convening Standard" (Reference (7)). The NED PM will convene periodical meetings within ICDD, and between ICDD and NICSD to check and monitor the project progress. An issue tracking spread sheet is used to track the issues found. For design documents for which ICDD is responsible, the project document "Project Specific Document Control Procedure" (Reference (19)), and NED AS-100A004 "Document Control Procedure" (Reference (5)) shall be applied. The Sub-master Engineering Schedule (SES) will be developed as described in Section 9 to setup the milestones of the project. The SES shall be shared among ICDD and NICSD. The SES shall be consistent with the customer overall integrated project schedule. The performance index such as Schedule Performance Index (SPI) will be used to measure the performance. The other items listed in Section 2.3.4 of the SPP do not apply to ICDD. The NED PM shall monitor and measure progress toward execution using the tools mentioned above.

Closeout – The NED PM shall ensure that all process requirements are complete, that the system has been evaluated and accepted by the customer, that deliveries and signoffs are complete, and that final disposition of documentation is performed according to this NED SMP.

7.1 Management Objectives and Priority

The NED PM shall be responsible for project management. The NED PM shall ensure that all planning documents are prepared on schedule, in accordance with the PSNE QAPD (Reference (3)), and that they meet the project requirements.

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

7.2 Risk Management

The NED PM shall be responsible for project risk management, concerning schedule, budget, resources, and technical issues, and must take appropriate actions to minimize project risks. The NED PM should use design review meetings per AS-200A005 (Reference (7)) and periodical meetings mentioned above for identifying risks. When the NED PM identifies any risks that may have considerable impacts on the project, the NED PM shall report the risks to customer in a timely manner.

7.3 Monitoring and Controlling Mechanisms and Metrics

The NED PM shall monitor the performance of the works. One of the methods that the NED PM can use for the performance monitoring is Schedule Performance Index (SPI). In addition, engineering/design groups prepare SESs as described in Section 9. The NED PM shall monitor the work performance against the SESs based on reports from engineering/design groups and the ICDD IV&V Team. The NED PM shall

- Ensure software being produced fulfills requirements,
- Monitor design and V&V outputs and determine when a task is completed,
- Assess proposed changes to the software to identify affected requirements and any new hazards or risks as well as changing and re-performing V&V tasks as necessary to address the changes, and
- Determine when changes or updates to the NED VVP are necessary.

The SPI can be used to determine whether resources and manpower levels are appropriate.

The ICDD IV&V Team shall define metrics to monitor the quality of the work in the NED VVP (Reference (21)).

7.4 Staffing Plan

The NED PM shall require the GPM of each engineering/design group to prepare an appropriate staffing plan commensurate with the workload and specialties required for the work. Assignment of the ICDD IV&V Team and the ICDD System Safety Lead shall be made by the NED PM to ensure their independence from the engineering/design groups.

8 Technical Process

8.1 Tools, Techniques and Methodologies

ICDD will use the following electrical document control systems:

- NUPDM2

- Customer Portal (if required)

In addition, ICDD uses software tools for requirements management activities. The tools will be special purpose requirements traceability tools, (e.g., IBM® Rational® Doors®), or a general purpose office software.

The NED PM shall be responsible for evaluation of the tools including impact on the safety, design integrity, and quality, if the tool produces incorrect results as well as the ability of the V&V activities to detect such errors.

For project support, SPI and other metrics are used as described in Section 7.3.

8.2 Software Documentation

Documentation is included in the life cycle phase outputs described in Section 12.

8.3 Secure Development and Operational Environment

Appendix C of the SPP addresses the requirements for Secure Development and Operational Environment (SDOE). Regarding to SDOE, NED is only responsible for preparing and maintaining the design documents including SDDs, IBDs and IEDs. NICSD is responsible for the software development. The NICSD SMP (Reference (22)) addresses the compliance to the requirements for SDOE for software development. This NED SMP addresses SDOE to protect the design documents above.

The design documents shall be protected in accordance with Toshiba Information Security Rules and Guidelines (ISRGs) in a manner that shall not compromise the security of the digital systems, other systems, or the plant. The Toshiba ISRGs mandate application of security measures including access control using passwords, anti-theft devices, hard disk encryption, and anti-virus software. In addition, the customer may require Toshiba to take some special cyber security measures during development. The NED PM shall require the GPM of each engineering/design group to implement SDOE in accordance with the ISRGs listed in Table 8-1 and the customer's requirements.

Table 8-1 Toshiba Information Security Rules and Guidelines

No	Classified into	Title	Content Description	Issued by
1	Toshiba Group Standard / Guidelines	Basic Regulation for Information Security Management (English language version exists)	Provide indoctrination of basic issues in treating proprietary information	Toshiba Information Security Center (SEC)
2	Toshiba Group Standard / Guidelines	Information Security Standard (English language version exists)	Provide standard measures in handling proprietary information	Toshiba Information Security Center (SEC)
3	Toshiba Group Standard / Guidelines	Information Security Guideline (English language version exists)	Provide guidelines especially for personnel who are in charge of indoctrinating and training employees of each company	Toshiba Information Security Center (SEC)

Table 8-1 Toshiba Information Security Rules and Guidelines

4	Toshiba Group Standard / Guidelines	Information Security Handbook (English language version exists)	Explains rules and key points to be complied by Toshiba group company employees.	Toshiba Information Security Center (SEC)
5	TANE Company Policies and Procedures	Information Security and Handling Policy	Prescribes information security policies and procedures for all TANE employees.	TANE IT Department
6	TANE IT Indoctrination Material	Information Security	Explains especially focused on an area of handling information in electronic devices/systems	TANE IT Department

For electrical document control systems described in Section 8.1, the NED PM shall be aware of registration of users to the systems, and supervision of access control to the systems

9 Work Packages, Schedule, and Budget

Design planning is performed in accordance with NED AS-200A017 "Design Planning Procedure" (Reference (10)). The GPM of each engineering/design group shall assign applicable engineers using the Design/Engineering Work Order Sheet defined in NED AS-200A017. The IV&V Team and the ICDD System Safety Lead shall be assigned by the NED PM, ensuring independence of the ICDD IV&V Team and the ICDD System Safety Lead.

The assigned engineers shall prepare Sub-master Engineering Schedule (SES) consistent with the customer overall integrated project schedule. The SES shall be planned considering the work breakdown structure. The SES shall document the work dependencies, and reflect the requirements of this NED SMP and the NED VVP (Reference (21)). The SES shall include a schedule of baseline reviews. The NED PM is responsible for making appropriate work breakdown structure, and keeping the SES consistent with the customer overall integrated project schedule. If the overall integrated project schedule is changed, the SES shall be changed appropriately.

The format of the Design/Engineering Work Order Sheet and the SES are defined in NED AS-200A017.

A Project Control Document List (PCDL) is prepared to list all project documents that shall be produced and retained as quality record for the project in accordance with NED AS-100A004 "Document Control Procedure" (Reference (5)). The GPMs, the ICDD System Safety Lead, and the ICDD IV&V Lead shall provide necessary information to prepare and to revise the PCDL. The format of the PCDL is defined in NED AS-100A004.

A Job Order Sheet is prepared for subcontracting with NICSD for the FPGA-based Safety-Related I&C system in accordance with NED AS-200A016 "Subcontracting Procedure from NED to Other Organizations within Toshiba Corporation" (Reference (9)). The Job Order Sheet includes the scope of work, technical requirements, material requirements, and QA requirements. The format of the Job Order Sheet is defined in NED AS-200A016.

Through the life cycle, the NED PM shall be responsible for management of the schedule, resources, and budget.

10 Baseline Review and Disposition of Nonconformance

The ICDD IV&V Team shall participate in all life cycle baseline reviews with NICSD IV&V Team. The NED PM and NICSD PM shall participate in the baseline review meetings to conclude the baseline reviews for all phase. 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 before shipment.

Each of the baseline reviews shall confirm disposition of each design, documentation, and test nonconformance identified during the phase. The software safety work product shall be reviewed in the baseline reviews.

In addition, the Design Phase baseline review shall confirm that if it is acceptable to issue the purchase order of the equipment. The purchase order shall not be issued without the acceptance of the Design Phase baseline review.

The ICDD IV&V Team shall document the result of each baseline review in a Baseline Review Report (BRR), and report to NQAD for review.

11 Software Safety Analyses

NED AS-200A132 "Digital System Safety and Hazard Analysis Procedure" (Reference (17)) defines a safety and hazard analysis procedure through the life cycle process, and states that the system safety and hazard analysis should include:

- Identification of system requirements (e.g., from the requirements traceability matrix) which are safety critical, and
- Consideration of all hazards associated with the intended use of the system including:
  - Identification of hazardous events and their cause,
  - The consequence and level of concern of these events,
  - The methods to control or mitigate these events, including corrective measures or aspects of the design to eliminate, reduce, or warn of hazardous events.

In identification of safety-critical system requirements, permanently attached equipment to the FPGA-based Safety-Related I&C systems shall require safety classification. Software safety analyses by ICDD for the FPGA-based Safety-Related I&C systems should focus on the following:

- Identify the software safety requirements and ensure the requirements are included in the SDD, IBD, and IED, as described in Section 12.1.
- Support of NICSD software safety analysis through all life cycle phases. The elements of the NICSD software safety analysis are identified in the NICSD SMP (Reference (22)).

NED Software Safety Analysis Reports (SSARs) shall documents the results of the safety analysis. SSARs shall be controlled in accordance with project document "Project Specific Document Control Procedure" (Reference (19)), and retained in accordance with NED AS-100A004 "Document Control Procedure" (Reference (5)).

12 Life Cycle Phase Activities

NED AS-200A128 "Digital System Life Cycle Procedure" (Reference (14)), defines a life cycle process that NED follows in digital systems development. For FPGA-based Safety-Related I&C systems, the life cycle phases of NED AS-200A128 are used with a modification that divides the Validation Testing Phase into the Module Validation Testing Phase and the System Validation Testing Phase. Table 12-1 maps the life cycle phases of the BTP 7-14 (Reference (1)), IEEE Std 1012 (Reference (2)), SPP (Reference (20)), AS-200A128, and the FPGA-based Safety-Related I&C systems.

Table 12-1 Mapping of Life Cycle Phases

BTP7-14	IEEE1012	AS-200A128	FPGA-based Safety-Related I&C Systems
Software Life Cycle Process Planning	Planning	Project Planning and	Project Planning and
Requirements	Concept	Concept Definition	Concept Definition
	Requirements	Requirements Definition	Requirements Definition
Design	Design	Design	Design
Implementation	Implementation	Implementation and Integration	Implementation and Integration
Integration			
Validation	Test	Validation Testing	Module Validation Testing
			System Validation Testing
Installation	Installation and Checkout	N/A*	N/A*
Operations and Maintenance	Operation	Operations and Maintenance.	Operations and Maintenance.
	Maintenance		
Not included	Retirement	Retirement	Retirement

*) FPGA-based Safety-Related I&C systems use Non-Rewritable (NRW) FPGA, one-time programmable devices. Because FPGA logic is implemented and fixed as physical contacts in the chips, there is no need for software installation after manufacturing, which embeds the final logic in the FPGA.

The following sections describe the activities in the life cycle phases used in development of the FPGA-based Safety-Related I&C systems. All references to phases are from the "FPGA-based Safety-Related I&C Systems" column of Table 12-1.

12.1 Project Planning and Concept Definition Phase

This phase is where system design requirements and software development plans are addressed.

12.1.1 Project Planning and Concept Definition Phase Inputs

Base documents include the plant specific documents, customer requirements, regulations, and applicable industry codes and standards as inputs to this Project Planning and Concept Definition Phase. To prepare SDDs, IBDs, and IEDs, ICDD shall define design inputs using Design Input Sheets as defined in NED AS-200A014 "Procedure for Documentation of Design Inputs" (Reference (8)).

12.1.2 Project Planning and Concept Definition Phase Outputs

Table-A lists the ICDD outputs of this Project Planning and Concept Definition Phase. NICSD shall define their outputs of this phase.

12.1.3 Software Management Plan

ICDD prepares the NED SMP (this document) for the FPGA-based Safety-Related I&C system.

12.1.4 Software Quality Assurance and Configuration Management

ICDD shall use the standard nuclear QA program: PSNE QAPD (Reference (3)) for these activities.

12.1.5 Verification and Validation Plan

The ICDD IV&V Team shall prepare the NED V&V Plan (NED VVP) (Reference (21)) in accordance with NED AS-200A130 (Reference (15)).

12.1.6 Design Documentation

ICDD shall prepare a SDD for the FPGA-based Safety-Related I&C system in accordance with NED AS-200A114 "Preparation Procedure for System Design Description" (Reference (11)). The SDD describes functions, comprehensive system design description, operation, system interfaces, instrumentation and control, specific requirements for components, and system and equipment design data of each system.

In addition to the SDD, ICDD shall prepare IBDs in accordance with NED AS-200A121 "Preparation Procedure for Interlock Block Diagram (IBD)" (Reference (12)), and IEDs in accordance with NED AS-200A122 "Preparation Procedure for Instrumentation Electrical Diagram (IED)" (Reference (13)). The IBDs describe operation interlock and protective functional information. AS-200A121 defines the format and symbols used in IBDs, and contents to be drawn. ICDD prepares the IEDs to depict the I&C system configuration and functions. AS-200A122 defines the symbols used in each IED, and the required contents. The SDDs, IBDs, and IEDs include system level requirements.

12.1.7 Job Order

ICDD issues a Job Order Sheets to procure the FPGA-based Safety-Related I&C system from NICSD in accordance with NED AS-200A016 "Subcontracting Procedure from NED to Other Organizations within Toshiba Corporation" (Reference (9)).

12.1.8 Safety Analysis

ICDD shall perform a preliminary safety analysis on the ICDD design using the method in NED AS-200A132 (Reference (17)), and document the result in the preliminary NED Software Safety Analysis Report (NED SSAR). The requirements for this analysis are provided in Section 11.

12.1.9 Requirements Traceability Matrix

ICDD shall perform requirements management activities and prepare the Project Planning and Concept Design Phase Requirements Traceability Matrix (RTM). The RTM in this phase includes the base requirements that are collected from the SDDs, and traces the requirements to the IBDs and IEDs. The base requirements include safety critical requirements. ICDD shall ensure that the base requirements covers all regulatory and customer requirements. The RTM will be developed along with the NICSD design.

12.1.10 Verification and Validation

The ICDD IV&V Team shall prepare a V&V Plan (VVP) to define the NED V&V activities for the FPGA-based Safety-Related I&C system, and perform V&V activities following the NED VVP. The NICSD IV&V Team prepares the NICSD VVP and performs V&V activities following the NICSD VVP. The NICSD IV&V Team shall produce a NICSD V&V Report (VVR) documenting the NICSD V&V activities in this phase. The ICDD IV&V Team shall produce an NED VVR documenting the NED V&V activities performed by ICDD in this phase, and incorporating the evaluation of the NICSD VVR. For the V&V activities, see the NED VVP (Reference (21)).

12.1.11 Baseline Review and Disposition of Nonconformance

The ICDD IV&V Team shall perform a baseline review, as described in Section 10. The baseline review shall confirm completion of the ICDD activities in the Project Planning and Concept Definition Phase, including review and accept of the NICSD baseline review. The baseline review shall confirm disposition of design and/or documentation nonconformances identified during this phase. The ICDD IV&V Team shall issue a BRR.

12.2 Requirements Definition Phase

The Requirements Definition Phase is where implementing equipment design requirements and configuration requirements are addressed. The FPGA-based Safety-Related I&C system consists of a number of chassis called units. The specifications of each unit to implement the equipment requirements are defined.

The ICDD IV&V Team and the ICDD System Safety Lead provide oversight of NICSD activities during this phase. There are no NED design activities in this phase except those described in the following subsections.

12.2.1 Safety Analysis

ICDD will support NICSD safety analysis. The ICDD System Safety Lead shall evaluate the NICSD SSAR, and document a NED SSAR based on the evaluation. The NICSD SSAR shall be combined with the NED SSAR to generate the integrated Project SSAR.

12.2.2 Verification and Validation

The ICDD IV&V Team shall produce an NED VVR for this phase incorporating the evaluation of the NICSD VVR. See the NED VVP (Reference (21)).

12.2.3 Baseline Review and Disposition of Nonconformance

The NICSD IV&V Team shall perform a baseline review to complete this phase. The ICDD IV&V Team provides oversight of NICSD.

12.3 Design Phase

The Design Phase is where design of software architecture, design of program structure elements, and software module functions are addressed. NICSD procures the modules, which are parts of the units, from the Power Platform Development Department (PPDD). NICSD shall identify safety-critical software included in the modules. If non-safety-critical software is used in a module, the safety-critical software shall be separated from non-safety software in separate FPGAs, or the non-safety-critical software shall be treated as safety-critical software.

The ICDD IV&V Team and the NED System Safety Lead provide oversight of NICSD activities during this phase. There are no NED design activities in this phase except those

described in the following subsections.

12.3.1 Safety Analysis

ICDD will support NICSD safety analysis. The ICDD System Safety Lead shall evaluate the NICSD SSAR, and document a NED SSAR based on the evaluation. The NICSD SSAR shall be combined with the NED SSAR to generate the integrated Project SSAR.

The NED SSAR shall:

- Identify and document those qualitative and quantitative characteristics of the FPGA-based Safety-Related I&C system that could affect safety, with defined limits as appropriate.
- Identify and document known and foreseeable hazards associated with the FPGA-based Safety-Related I&C system in both normal and fault conditions, ensuring that the hazards are reflected in plant specific documents and plant safety analysis information.
- Identify risk controls that mitigate risks in the later phases.
- Evaluate acceptability of residual risks.

In addition, the NED SSAR shall include the information required in Section 6.7 of the SPP as applicable.

12.3.2 Verification and Validation

The ICDD IV&V Team shall produce an NED VVR for this phase incorporating the evaluation of the NICSD VVR. See the NED VVP (Reference (21)).

12.3.3 Baseline Review and Disposition of Nonconformance

The NICSD IV&V Team shall perform a baseline review to complete this phase. The ICDD IV&V Team provides oversight of NICSD.

12.4 Implementation and Integration Phase

The Implementation and Integration Phase is where software coding activities and testing activities of FPGA logic and integrated individual software modules containing the FPGAs for the FPGA-based Safety-Related I&C system, are addressed.

Unlike a microprocessor-based system, the anti-fuse type FPGA that Toshiba selected requires software installation to be performed before hardware assembly. The Software Coding Phase and the Integration Phase are unified as the Implementation and Integration Phase for this reason.

The ICDD IV&V Team and the NED System Safety Lead provide oversight of NICSD activities during this phase. There are no NED design activities in this phase except those described in the following subsections.

12.4.1 Safety Analysis

ICDD will support NICSD safety analysis. The ICDD System Safety Lead shall evaluate the NICSD SSAR, and document a NED SSAR based on the evaluation. The NICSD SSAR shall be combined with the NED SSAR to generate the integrated Project SSAR.

12.4.2 Verification and Validation

The ICDD IV&V Team shall produce an NED VVR for this phase incorporating the evaluation of the NICSD VVR. See the NED VVP (Reference (21)).

12.4.3 Baseline Review and Disposition of Nonconformance

The NICSD IV&V Team shall perform a baseline review to complete this phase. The ICDD IV&V Team provides oversight of NICSD.

12.5 Module Validation Testing Phase

For the FPGA-based Safety-Related I&C system, the validation phase is divided into two phases, the Module Validation Testing Phase and the System Validation Testing Phases. In the Module Validation Testing Phase, PPDD performs module validation testing using the module test procedures.

The ICDD IV&V Team and the NED System Safety Lead provide oversight of NICSD activities during Module Validation Testing. There are no NED design activities in this phase except those described in the following subsections.

12.5.1 Safety Analysis

ICDD will support NICSD safety analysis. The ICDD System Safety Lead shall evaluate the NICSD SSAR, and document a NED SSAR based on the evaluation. The NICSD SSAR shall be combined with the NED SSAR to generate the integrated Project SSAR.

12.5.2 Verification and Validation

The ICDD IV&V Team shall produce an NED VVR for this phase incorporating the evaluation of the NICSD VVR. See the NED VVP (Reference (21)).

12.5.3 Baseline Review and Disposition of Nonconformance

The NICSD IV&V Team shall perform a baseline review to complete this phase. The ICDD IV&V Team provides oversight of NICSD.

12.6 System Validation Testing Phase

The System Validation Testing includes the Software Validation Test and the Platform Factory Test (PFT) of the SPP. First, NICSD integrates the units, and performs unit validation testing using the unit test procedures, and evaluates the result of the unit validation testing. After the unit validation testing has finished with satisfactory results, NICSD assembles the system from the validated units, and perform system validation testing using the system test procedure. The NICSD test personnel prepare the system test report.

The ICDD IV&V Team and the ICDD System Safety Lead provide oversight of NICSD activities during this phase, and confirm the completion of the software development process. There are no NED design activities in this phase except those described in the following subsections.

12.6.1 Safety Analysis

ICDD will support NICSD safety analysis. The ICDD System Safety Lead shall evaluate the final NICSD SSAR, and document the final NED SSAR based on the evaluation. The final NICSD SSAR shall be combined with the final NED SSAR to generate the integrated Project SSAR.

The final NED SSAR shall:

- Document the intended use of the FPGA-based Safety-Related I&C system and any reasonably foreseeable misuse.

- Identify and document those qualitative and quantitative characteristics of the FPGA-based Safety-Related I&C system that could affect safety, with defined limits as appropriate.
- Identify and document known and foreseeable hazards associated with the FPGA-based Safety-Related I&C system in both normal and fault conditions, ensuring that the hazards are reflected in plant specific documents and plant safety analysis information..
- Estimate and document the risk(s) for each hazardous situation.
- Identify risk controls that mitigate risks.
- Evaluate acceptability of residual risks.

In addition, the final NED SSAR shall include the following information required in Section 6.7 of the SPP:

- Name, Description, and Version of the Software Evaluated
- System
- Software Classification
- Purpose and Scope
- Reference Inputs
- Software Safety Analysis Body of Report, i.e., ICDD
- Anomalies Noted
- Conclusion
- Responsible Engineer
- Approving Authority

12.6.2 Verification and Validation

The NICSD IV&V Team prepares the final NICSD VVR to report the completion of NICSD V&V activities of this phase. The ICDD IV&V Team prepares the final NED VVR to report the completion of NED V&V activities of this phase, incorporating the evaluation of the final NICSD VVR. See the NED VVP (Reference (21)).

12.6.3 Baseline Review and Disposition of Nonconformance

NICSD shall perform a baseline review to review the baseline of this System Validation Testing Phase.

The ICDD IV&V Team shall perform the final baseline review to confirm the completion of the software development process, and issue the final Baseline Review Report. Each nonconformance of design documentation and test results identified during the development phases shall be resolved and disposed of.

After the validation testing, Toshiba will ship the FPGA-based Safety-Related I&C system to the US nuclear power plant for Site Acceptance Test (SAT) by customer. Prior to installation to nuclear power plant and acceptance by customer, the systems may be integrated with other I&C systems and subjected to a Platform Integration Test (PIT).

Note that the final NED VVR will be issued before the PIT and SAT. The PIT and SAT might require design change or error correction of the FPGA-based system. In that case, the life cycle process described above must be reactivated from an appropriate point, and necessary documents including the final NED VVR shall be updated in accordance with the NED VVP.

12.7 Operations and Maintenance Phase

The Operations and Maintenance Phase begins with the completion of the System Validation Testing Phase.

ICDD and NICSD shall address any problem developed after the system validation testing, and take necessary activities in accordance with NED AS-200A128 (Reference (14)), which include update of the design documents, Master Configuration List (MCL), codes, RTM, SSAR, and VVR. To perform these activities, NICSD shall implement the established software change control procedure. ICDD shall use the standard QA program.

For making changes, regression analysis shall be done to determine the extent of testing to be repeated if proposed changes occur to:

- Assess side effects and impacts of change to software
- Rerun test cases based on changes to detect errors associated with modification

The NED PM shall evaluate risks in resolving the problem, identify and provide ways to reduce, mitigate, or eliminate the risks

12.8 Retirement Phase

ICDD plans no activity for the Retirement Phase beyond those written in the SPP (Reference (20)).

13 Qualification and Training

The SM of ICDD and the GPMs of engineering/design groups shall be responsible for training and qualification of ICDD personnel except IV&V Team and safety analysis staff in accordance with NED AS-100A008 "Procedure for Indoctrination and Training" (Reference (6)). The IV&V Lead shall be responsible for training and qualification of the ICDD IV&V Team members, and the ICDD System Safety Lead shall be responsible for training and qualification of safety analysis staff.

Personnel including the ICDD IV&V Team and safety analysis staff shall be trained in accordance with NED AS-100A008 "Procedure for Indoctrination and Training" (Reference (6)), and NED AS-200A017 "Design Planning Procedure" (Reference (10)). NED AS-200A017 defines planning of a project specific indoctrination training for assigned engineers to be qualified for the scope of work.

The GPMs shall be responsible for documenting the training as a QA record, and retaining the record in accordance with NED AS-100A008.

14 Deviation Policy

14.1 Activity Iteration Policy

The responsible leads shall evaluate effect on existing work products, and iterate necessary work according to the evaluation, when iteration becomes necessary. Section 7.2 of the NED VVP (Reference (21)) describes the procedures and methods for iteration.

14.2 Deviation Policy

Deviation from this NED SMP may be considered for the following reasons, including but not limited to:

- Revision of the SPP (Reference (20))
- Requests from the customer, including change of the project
- Comments from the United States Nuclear Regulatory Commission (USNRC)
- Revision of the PS QAPD including the NED QA Manual (Reference (4)) and AS standards
- Unacceptably low performance of work
- Unacceptably low quality of work

The NED PM, GPMs, the ICDD System Safety Lead, or the IV&V Lead shall be responsible for evaluating the deviation on identification of the task or activity, rationale, and effect on quality of work, and determine whether the deviation is acceptable without changing the plan.

If the degree of the deviation is too large to keep compliance with the current revision of this NED SMP, this NED SMP shall be revised.

14.3 Plan Maintenance

The NED PM, the GPMs, the ICDD System Safety Lead, and the IV&V Lead should verify that the processes defined in this NED SMP are effective, adequate, suitable, sufficient, and implement the requirements and expectations in the SPP (Reference (20)). They shall be responsible for correcting and extending the plan as required, to meet the requirements and expectations in the SPP.

When changes to this NED SMP are necessary, this NED SMP shall be revised in accordance with the project document "Project Specific Document Control Procedure" (Reference (19)). Changes may be necessary due to the following reasons, including but not limited to:

- Revision of the SPP
- Requests or requirements from the customer
- Comments from the USNRC
- Revision of the PS QAPD including the NED QA Manual (Reference (4)) and AS standards
- Requests or requirements from NQAD by Corrective Action Requests (CARs), or Nonconformance Notice Report (NNRs)
- Deviation from the current revision of the NED SMP
- Changes of named personnel in Table 5-1

Because changes of this NED SMP may broadly affect life cycle activities, a draft of the revised NED SMP should be available for and be reviewed by the NED PM, the GPMs, the ICDD System Safety Lead, the IV&V Lead, NQAD, and responsible personnel of NICSD as necessary.

Table-A ICDD Output Documents

Table-A defines responsible organization for prepare, review, and approval of ICDD Output documents, and plans or procedures used for those activities.

Documents	Task	Responsible of	Plans or Procedures (Section)	Remarks
Project Planning and Concept Definition Phase				
NED SMP	Prepare	ICDD / Design	SPP	
	Review	ICDD / Design		
	Approve	ICDD / PM		
NED VVP	Prepare	ICDD / V&V	AS-200A130 (6.1.1)	
	Review	ICDD / V&V		
	Approve	ICDD / PM		
SDD	Prepare	ICDD / Design	AS-200A114 AS-200A129 (5.1.4) AS-200A130 (6.1.2)	NED DVR is used in review.
	IR[1)]	ICDD / V&V		
	Approve	ICDD / Design		
IBD	Prepare	ICDD / Design	AS-200A121 AS-200A129 (5.1.4) AS-200A130 (6.1.2)	NED DVR is used in review.
	IR[1)]	ICDD / V&V		
	Approve	ICDD / Design		
IED	Prepare	ICDD / Design	AS-200A122 AS-200A129 (5.1.4) AS-200A130 (6.1.2)	NED DVR is used in review.
	IR[1)]	ICDD / V&V		
	Approve	ICDD / Design		
NED SSAR	Prepare	ICDD / Design	AS-200A130 (6.1.2) AS-200A132 SPP Section 6 NED SMP Section 11	NED DVR is used in review.
	IR[1)]	ICDD / V&V		
	Approve	ICDD / System Safety Lead		
NED VVR	Prepare	ICDD / V&V	AS-200A130 (5, 6.1.6) NED VVP	
	IR[1)]	ICDD / V&V		
	Approve	ICDD / PM		
Baseline Review Report	Prepare	ICDD / V&V	NED SMP, NED VVP	
	Review	ICDD / V&V		
	Approve	ICDD / PM		
	Review and Accept[2)]	NQAD		

Documents	Task	Responsible of	Plans or Procedures (Section)	Remarks
Requirements Definition Phase				
NED SSAR	Prepare	ICDD / Design	AS-200A130 (6.1.2) AS-200A132 SPP Section 6 NED SMP Section 11	NED DVR is used in review.
	IR[1)]	ICDD / V&V		
	Approve	ICDD / System Safety Lead		
NED VVR	Prepare	ICDD / V&V	AS-200A130 (5, 6.2.5) NED VVP	
	IR[1)]	ICDD / V&V		
	Approve	ICDD / PM		
Design Phase				
NED SSAR	Prepare	ICDD / Design	AS-200A130 (6.1.2) AS-200A132 SPP Section 6 NED SMP Section 11	NED DVR is used in review.
	IR[1)]	ICDD / V&V		
	Approve	ICDD / System Safety Lead		
NED VVR	Prepare	ICDD / V&V	AS-200A130 (5, 6.5.9) NED VVP	
	IR[1)]	ICDD / V&V		
	Approve	ICDD / PM		
Implementation and Integration Phase				
NED SSAR	Prepare	ICDD / Design	AS-200A130 (6.1.2) AS-200A132 SPP Section 6 NED SMP Section 11	NED DVR is used in review.
	IR[1)]	ICDD / V&V		
	Approve	ICDD / System Safety Lead		
NED VVR	Prepare	ICDD / V&V	AS-200A130 (5, 6.2.5) NED VVP	
	IR[1)]	ICDD / V&V		
	Approve	ICDD / PM		
Module Validation Testing Phase				
NED SSAR	Prepare	ICDD / Design	AS-200A130 (6.1.2) AS-200A132 SPP Section 6 NED SMP Section 11	NED DVR is used in review.
	IR[1)]	ICDD / V&V		
	Approve	ICDD / System Safety Lead		
NED VVR	Prepare	ICDD / V&V	AS-200A130 (5, 6.5.9) NED VVP	
	IR[1)]	ICDD / V&V		
	Approve	ICDD / PM		

Documents	Task	Responsible of	Plans or Procedures (Section)	Remarks
System Validation Testing Phase				
Final NED SSAR	Prepare	ICDD / Design	AS-200A130 (6.1.2) AS-200A132 SPP Section 6 NED SMP Section 11	NED DVR is used in review. [f1]
	IR[1)]	ICDD / V&V		
	Approve	ICDD / System Safety Lead		
Final NED VVR	Prepare	ICDD / V&V	AS-200A130 (5, 6.5.9) NED VVP	
	IR[1)]	ICDD / V&V		
	Approve	ICDD / PM		
Baseline Review Report	Prepare	ICDD / V&V	NED SMP, NED VVP	
	Review	ICDD / V&V		
	Approve	ICDD / PM		
	Review and Accept[2)]	NQAD		

1) IR: Independent Review, a member of the IV&V Team.

2) NQAD accepts the BRR after reviewing that BRR is established in accordance with the NED SMP, and includes the required contents described in the NED VVP.

Table-B Compliance to SPP

Compliance to SPP

No.	SPP Section	Title	SMP Section(s)	Remark
1.	1	Introduction	N/A	Section Title
2.	1.1	Purpose	N/A	No requirement
3.	1.2	Use of the Software Program Plan	N/A	No requirement
4.	1.2.1	Vendor Plan Use	5, 6	
5.	1.2.2	Licensing Basis Documents	N/A	No requirement
6.	1.2.3	[Deleted]	---	---
7.	1.3	Scope	N/A	No requirement
8.	1.3.1	Use of Existing Software Plans and Processes	N/A	No existing software plans is used.
9.	1.3.2	Nonsafety Plan Requirements	N/A	This section is for nonsafety systems.
10.	1.3.3	Defining Software	Comply	This SMP regards "software" as defined in this SPP section.
11.	1.4	Roles and Responsibilities	N/A	Section Title
12.	1.4.1	Organization	5	See also NICSD SMP
13.	1.4.2	Independence	5	See also NICSD SMP
14.	1.4.3	Responsibilities	5.2	See also NICSD SMP
15.	1.4.4	Qualifications and Training	13	See also NICSD SMP
16.	1.4.5	Organizational Interfaces	5.2, 5.3	
17.	1.5	Terms and Definitions	Comply	This SMP uses terms and definition in accordance with this SPP section.
18.	1.6	Acronyms	3	
19.	1.7	Secure Development and Operational Environment	8.3	See also NICSD SMP
20.	1.8	Applicable Standards and References	4	
21.	1.9	Software Life Cycle Overview	12	See also NICSD SMP
22.	1.10	Software Classification	-	See NED AS-200A129
23.	1.11	General Policies for All Plans	N/A	No requirement
24.	1.11.1	Use of IEEE Standards	N/A	See the reference sections of SDD
25.	1.11.2	Life Cycle Task Iteration Policy	14.1	See also NICSD SMP
26.	1.11.3	Deviation Policy	14.2	See also NICSD SMP
27.	1.11.4	Control Procedures	14.3	See also NICSD SMP
28.	1.11.5	Standards, Policies, and Conventions	6, 8.3	See also NICSD SMP
29.	1.11.6	Schedule	9	
30.	1.11.7	Use of Designees	5.2	
31.	1.11.8	Modifications to PDS and COTS	N/A	See NICSD SMP
32.	1.11.9	Modifications to Configuration	N/A	See NICSD SMP
33.	1.11.10	Use of Metrics	7.3	See also NICSD SMP

Compliance to SPP

No.	SPP Section	Title	SMP Section(s)	Remark
34.	1.12	EPC Team Member Software Plan Maintenance	14.3	See also NICSD SMP
35.	1.13	[Deleted]	---	---
36.	2	Software Project Management Program Plan (SPMPP)	N/A	Section Title
37.	2.1	Introduction	N/A	No requirement
38.	2.1.1	Purpose	1, 2, 5, 7	See also NICSD SMP
39.	2.1.2	Scope	2	
40.	2.1.3	[Deleted]	---	---
41.	2.1.4	Relationship of the SPMPP to Other SPP Sections	N/A	No requirement for this NED SMP.
42.	2.2	Project Organization	---	Contents are in subsections
43.	2.2.1	Process Model	2, 5, 9	See also NICSD SMP
44.	2.2.2	Organizational Structure	5.1	See also NICSD SMP
45.	2.2.3	Organizational Boundaries and Interfaces	7, 9, 12.1.6, 12.1.7	See also NICSD SMP
46.	2.2.4	Project Responsibilities	5	See also NICSD SMP
47.	2.3	Managerial Process	N/A	Section Title
48.	2.3.1	Management Objectives and Priorities	7.1, 7.3	See also NICSD SMP
49.	2.3.2	Assumptions, Dependencies, and Constraints	N/A	Section 2.3.2 of SPP describes global requirements See also NICSD SMP
50.	2.3.3	Risk Management	7.2	See also NICSD SMP
51.	2.3.4	Monitoring and Controlling Mechanisms and Metrics	7, 8.1, 9, 10, 11, 12	See also NICSD SMP
52.	2.3.5	Staffing Plan	7.4, 9, 13	See also NICSD SMP
53.	2.4	Technical Process	N/A	Section Title
54.	2.4.1	Methods, Tools, and Techniques	8.1	See also NICSD SMP
55.	2.4.2	Software Documentation	8.2, 10	See also NICSD SMP
56.	2.4.3	Secure Development and Operational Environment and Cyber Security	8.3	See also NICSD SMP
57.	2.4.4	Project Support Functions	8.1	See also NICSD SMP
58.	2.5	Work Packages, Schedule, and Budget	9	See also NICSD SMP
59.	2.5.1	Work Packages	9	See also NICSD SMP
60.	2.5.2	Dependencies	7, 9	See also NICSD SMP
61.	2.5.3	Resource Requirements	7, 9	See also NICSD SMP
62.	2.5.4	Budget and Resource Allocation	5.2, 7, 9	See also NICSD SMP
63.	2.5.5	Schedule	9	See also NICSD SMP
64.	6	Software Safety Program Plan (SSPP)	N/A	Section Title
65.	6.1	Introduction	N/A	Section Title
66.	6.1.1	Purpose	11	

Compliance to SPP

No.	SPP Section	Title	SMP Section(s)	Remark
67.	6.1.2	Scope	11	
68.	6.1.3	[Deleted]	---	---
69.	6.1.4	Relationship of the SSPP to Other SPP Sections	N/A	
70.	6.2	Reference Documents	N/A	No requirements
71.	6.3	Software Safety Management	5.2	
72.	6.3.1	Organization and Responsibilities	5.2, 11, 12	
73.	6.3.2	Resources	7	
74.	6.3.3	Schedule	9	
75.	6.3.4	Qualifications and Training	13	
76.	6.3.5	Software Life Cycle	12	
77.	6.3.6	Documentation Requirements	5.2, 10, Table-A 12.1.8, 12.6.1	
78.	6.3.7	Software Safety Program Records	11, 13	See also NED AS-100A004
79.	6.3.8	Software Configuration Management Activities	N/A	See NICSD planning documents listed in Section 1.
80.	6.3.9	Software Quality Assurance Activities	N/A	See NICSD SQAP
81.	6.3.10	Software Verification and Validation Activities	N/A	See NED VVP
82.	6.3.11	Tool Support and Approval	N/A	See NICSD SMP
83.	6.3.12	Previously Developed or Purchased (COTS) Software	N/A	See NICSD SMP
84.	6.3.13	Subcontract Management	9	
85.	6.3.14	Process Certification	N/A	See NICSD SMP
86.	6.4	Software Safety Analyses	11	See also NICSD SMP
87.	6.4.1	Preparatory Analyses	11	
88.	6.4.2	Software Safety Requirements Analysis Preparation	5.2, 11, 12.1.8	
89.	6.4.3	Software Safety Requirements Analysis	N/A	See NICSD SMP
90.	6.4.4	Software Safety Design Analysis	N/A	See NICSD SMP
91.	6.4.5	Software Safety Code Analysis	N/A	See NICSD SMP
92.	6.4.6	Software Safety Integration and Validation Test Analyses	12.6.1	See also NICSD SMP
93.	6.4.7	Software Safety Installation Analysis	N/A	See Section 12
94.	6.4.8	Software Safety Change Analysis	12.7	
95.	6.5	Post Development	12.7	
96.	6.5.1	Training	13	
97.	6.5.2	Deployment	N/A	
98.	6.6	Plan Approval	N/A	
99.	6.7	Software Safety Analysis Reporting	N/A	