ATTACHMENT 2

Letter from Mark L. Marchi (WPSC)

To

Document Control Desk (NRC)

Dated

July 30, 1999

Reactor Protection and Engineered Safety Features Upgrade

E3 Design, Verification and Validation Plan for Class 1E aud Category A Systems

– Non-Proprietary Class 3

E3
Design, Verification and Validation Plan for Class 1E and Category A Systems

Revision 0

27 July 1999

RECORD OF CHANGES

Revision 0 **27 July 1999**

Changes: Initial revision (created from Revision 0 of NPD-PD-00003-GEN).

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. INTRODUCTION AND SCOPE

This document was prepared in accordance to the [
]^{a,c}.

1.1. Purpose

The purpose of this document is to define, at a high level, the design, verification, and validation processes that are used to produce safety systems using the E3 [ ]^{a,c}. The E3 [ ]^{a,c} represents the integration of the commercially available Ovation™ hardware (with some enhancements) and the Eagle Series embedded safety software developed for the Eagle 21™ product line and the Sizewell primary protection system and subsequently used for the Temelin and Ignalina projects.

The intended uses of this document include: internal guidance and instruction, support of licensing submittals, support of audits, and support of proposal efforts.

1.2. Scope

This document addresses the design, verification and validation processes for the standard E3 [ ]^{a,c} and for projects using the [ ]^{a,c} to implement Class 1E and Category A systems for specific applications and customers. [
]^{a,c}.

1.3. Relationship to Previous Processes

The processes defined in this document and the subordinate documents referred to herein, are based on the processes previously used by Westinghouse to develop microprocessor-based safety systems.
[

]^{a,c}.

- [ ]^{a,c}.
- [
]^{a,c}.
- [ ]^{a,c}.
- [
]^{a,c}.

[

]^{a,c}.

[

]^{a,c}.

2. DEFINITIONS

2.1. Acronyms

E3	E3 is the temporary internal Westinghouse NPD name for a safety system product line based upon the Eagle series software and an Ovation™ compatible hardware platform.
EMI	Electromagnetic Interference
FAT	Factory Acceptance Test
HDS	Hardware Design Specification
HRS	Hardware Requirements Specification
I&C	Instrumentation and Control
I/O	Input/Output
PL/M	PL/M is a microprocessor programming language specified by Intel Corporation. It is based on the PL/1 programming language.
SAT	Site Acceptance Test
SDD	Software Design Description
SDR	System Design Requirements
SDS	System Design Specification
SRS	Software Requirements Specification

2.2. Terms

Analysis	A review technique that consists of a formally documented evaluation or calculation to confirm some aspect of a design. (See Section 8.2.2.)
[ ]^{a,c}	[ ]^{a,c}.
[ ]^{a,c}	[ ]^{a,c}.
Category A	A Function, and the associated Systems and Equipment (FSE) that implement it, which plays a principal role in the achievement or maintenance of Nuclear Power Plant safety. Category A FSE prevent Postulated Initiating Events (PIEs) from leading to a significant sequence of events, or mitigate the consequences of PIEs. [IEC 1226]

Class 1E	The safety classification of the electrical equipment and systems that are essential to emergency reactor shutdown, containment isolation, reactor core cooling, and containment and reactor heat removal, or are otherwise essential in preventing significant release of radioactive material to the environment. [IEEE 603]
[ ]^{a,c}	[ ]^{a,c}.
[ ]^{a,c}	[ ]^{a,c}.
Factory Acceptance Test	A formal test that provides validation of the system functionality as specified in the system functional requirements. (See Section 12.2.)
[ ]^{a,c}	[ ]^{a,c}.
Inspection	A review technique that consists of examining the entity being verified, either hardware or software. (See Section 8.2.1.)
Petri Net	A model of a concurrent system that is expressed in a specific graphical notation and can be used to explore certain properties of the system. [Dictionary of Computing]
[ ]^{a,c}	[ ]^{a,c}.
Qualification Testing	Testing conducted to determine whether a system or component is suitable for operational use. [IEEE 610.12]
Regression Testing	Selective retesting of a system or component to verify that modifications have not caused unintended effects, and that the system or component still complies with its specified requirements. [IEEE 610.12]
[ ]^{a,c}	[ ]^{a,c}.
[ ]^{a,c}	[ ]^{a,c}.
Site Acceptance Test	Site acceptance V&V accomplished through a testing activity in the nuclear power generating station. Site acceptance testing should be utilized to provide adequate confidence of the following: a) No damage has occurred due to shipment or installation b) Computer is compatible with the nuclear power generating station c) Correctness of interfaces to other plant systems that may have been simulated during the FAT. [IEEE 7-4.3.2]

Test	A review technique that consists of operating the system or component, either hardware or software, under specified conditions, observing or recording the results, and making an evaluation of some aspect of the system or component based upon the results. (See Section 8.2.3.)
[ ]^{a,c}	[ ]^{a,c}.
Validation	The test and evaluation of the integrated computer system (hardware and software) to ensure compliance with the functional, performance, and interface requirements. [IEC 880]
Verification	The process of determining whether or not the product of each phase of the computer system development process fulfills all the requirements imposed by the previous design phase. [IEC 880]

3. REFERENCES

[ ]a,c

[ ]a,c

[ ]a,c

Dictionary of Computing, Dictionary of Computing, Oxford University Press, 1983.

[ ]a,c

[ ]a,c

4. REGULATORY GUIDANCE

The following documents provide regulatory guidance from the United States Nuclear Regulatory Commission:

USNRC Regulatory Guide 1.152. "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants."

USNRC Regulatory Guide 1.168. "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

USNRC Regulatory Guide 1.169. "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

USNRC Regulatory Guide 1.170. "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

USNRC Regulatory Guide 1.171. "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

USNRC Regulatory Guide 1.172. "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

USNRC Regulatory Guide 1.173. "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

5. APPLICABLE STANDARDS

The following standards are used for [ ][a,c]:

ASME Std NQA-1-1994. "Quality Assurance Requirements for Nuclear Facility Applications."

CEI/IEC 1226-1993-05. "Nuclear power plants - Instrumentation and control systems important for safety - Classification."

IEC 880-1986. "Software for Computers in the Safety Systems of Nuclear Power Stations."

IEEE Std 7-4.3.2-1993. "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations" as endorsed by Reg. Guide 1.152.

IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

IEEE Std 610.12-1990, "IEEE Standard Glossary of Software Engineering Terminology."

IEEE Std 828-1990. "IEEE Standard for Software Configuration Management Plans" as endorsed by Reg. Guide 1.169.

IEEE Std 829-1983. "IEEE Standard for Software Test Documentation" as endorsed by Reg. Guide 1.170.

IEEE Std 830-1993. "IEEE Recommended Practice for Software Requirements Specifications" as endorsed by Reg. Guide 1.172.

IEEE Std 1008-1987. "IEEE Standard for Software Unit Testing" as endorsed by Reg. Guide 1.171.

IEEE Std 1012-1986. "IEEE Standard for Software Verification and Validation Plans" as endorsed by Reg. Guide 1.168.

IEEE Std 1028-1988. "IEEE Standard for Software Reviews and Audits" as endorsed by Reg. Guide 1.168.

IEEE Std 1042-1987. "IEEE Guide to Software Configuration Management" as endorsed by Reg. Guide 1.169.

IEEE Std 1074-1995. "IEEE Standard for Developing Software Life Cycle Processes" as endorsed by Reg. Guide 1.173.

IEEE/EIA Std 12207.0-1996. "Industry Implementation of International Standard ISO/IEC 12207." This standard shall be used in preference to IEEE 1074 as the primary guidance for Software Life Cycle Processes.

IEEE Std 12207.1. "IEEE Guide for Information Technology - Software Life Cycle Processes - Life Cycle Data" used as guidance in the application of ISO/IEC 12207.

IEEE Std 12207.2. "IEEE Guide for Information Technology - Software Life Cycle Processes - Implementation" used as guidance in the application of ISO/IEC 12207.

6. OVERVIEW OF THE DESIGN, VERIFICATION AND VALIDATION PROCESSES

Figure 1 and Figure 2 show overviews of the design, verification, and validation processes. [

]^{a,c}.

The Eagle Series embedded safety system software architecture recognizes [

]^{a,c}.

[

]^{a,c}.

6.1. [ ]^{a,c} Design, Verification and Validation Process Overview

[

]^{a,c}.

a,c [

]

Figure 1: [ ]^{a,c} Design Verification and Validation Overview

(Detailed process is shown in Figure 3 and Figure 4)

[

]^{a,c}.

6.2. [ ]^{a,c} Design, Verification and Validation Process Overview

Figure 2 graphically shows an overview of the [ ]^{a,c} Design, Verification and Validation Process.
[

]a,c.

a,c

Figure 2: [ ]a,c Design Verification and Validation Overview
(Detailed process is shown in Figure 5)

[

]a,c.

6.3. Snpporting Processes

Processes that support both the [ ]a,c Design, Verification and Validation Process and the [ ]a,c Design, Verification and Validation Process include the [

]a,c.

7. [ ]^{a,c} DESIGN ACTIVITIES

The [ ]^{a,c} Design, Verification, and Validation Process is detailed in Figure 3. The figure emphasizes system and software activities. Hardware activities are presented in Figure 4. The figures show the activities as purely sequential (similar to the classic "Waterfall" methodology). [

]^{a,c}.

7.1. [ ]^{a,c} Definition Activity

The [ ]^{a,c} Definition Activity produces the following types of items:

1. Identification of the intended application(s) of the [ ]^{a,c}.
2. Identification of the licensing requirements for the intended applications.
3. Documentation of the objectives and/or goals of the [ ]^{a,c}.
4. An early evaluation of potential problems.
5. Identification of external system interfaces.
6. Definition of particular options and features.
7. Identification of design constraints.

This information shall become part of the [ ]^{a,c}.

a,c

Figure 3: [ ]^{a,c} Design Verification and Validation Detail

(Overview is shown in Figure 1)

7.2. [ ]^{a,c} System Design Activities

The Platform System Design Activities include two major efforts: [ ]^{a,c} System Requirements Analysis and [ ]^{a,c} System Architectural Design.

7.2.1. System Requirements Analysis

The System Requirements Analysis activity determines the system requirements based on the intended applications (and other information) as identified in the [ ]^{a,c}. Items to be considered include:

1. Regulatory Requirements
2. Safety Requirements
3. Reliability and Availability Requirements
4. Qualification Requirements
5. Power and Grounding Requirements
6. Human System Interface Requirements
7. External Interface Requirements
8. Test Requirements
9. Development Tools
10. Maintenance Tools
11. Design Constraints
12. Typical Installation Constraints
13. Abnormal Conditions and Events
14. Verification and Validation Requirements
15. Quality Assurance Requirements
16. Time Response
17. Accuracy

This information is documented in the System Design Requirements. [ ]^{a,c}.

7.2.2. System Architectural Design

The System Architectural Design activity consists of defining the architectural elements that will be supported by the platform and establishing typical top-level [ ]^{a,c}. The architectures shall identify [ ]^{a,c}. It shall ensure that all system requirements are allocated among the items.

Items to be considered include:

1. Consistency with the System Design Requirements.
2. Appropriateness of reusing previously developed software items and previously developed hardware items.
3. Feasibility of developing the missing software items.

4. Feasibility of developing or purchasing the missing hardware items.
5. Ease of operation and inaintenance.
6. Implemeentation constraints

[

]^{a,c}.

7.3. [ ]^{a,c} Software Design Activities

The [ ]^{a,c} Software Design Activities include Software Requirements Analysis, Software Architectural Design, Software Detailed Design, and Software Coding and Engineering Testing.

7.3.1. Software Requirements Analysis

The [ ]^{a,c} Software Requirements Analysis activity establishes and documents the software requirements for each software item identified in the System Design Specification.

Items to be considered include:

1. Functionality and capability requirements
2. Interfaces to other software items
3. Interfaces to hardware items
4. Safety requirements
5. Human factors requirements
6. Database requirements
7. Operation and inaintenance requirements
8. Design standards
9. Verification requirements

[

]^{a,c}.

7.3.2. Software Architectural Design

The Software Architectural Design activity establishes an architecture for each software item based on its Software Requirements Specification. The architecture describes the top-level strncture of the software items and identifies the software components required to implement the item. Each of the software item's requirements are refined and assigned to a software coinponent. The top-level interface between software components is defined.

If the software components identified in this activity require further decomposition, the Software Requirements Analysis activity and the Software Architectural Design Activity should be applied recursively.

[

]^{a,c}.

[

]a,c

7.3.3. Software Detailed Design

The developer shall establish a detailed design for each software component. The components shall be refined into lower level software units that can later be coded, compiled, and tested. Software requirements shall be allocated from the components to the units. Detailed interfaces shall be defined to external software, other software items, other software components, and other software units, as necessary.

[

]a,c.

[

]a,c

7.3.4. Software Coding and Engineering Testing

The developer shall write the code and otherwise complete the [ ]a,c modules in accordance with the appropriate language specific design and coding standards. [ ]a,c The developer shall compile the modules and test the software. [The testing performed at this stage also includes software integration testing]a,c. The developer shall combine the modules with other platform modules, application modules, and test modules. The test modules shall be designed to exercise the software in a configuration that is typical of its intended use.

[

]a,c.

[

]a,c.

7.4. [ ]a,c Hardware Design Activities

[

]a,c.

a,c

Figure 4: [ ]^{a,c} Hardware Design Process

7.4.1. Hardware Requirements Analysis

The Hardware Requirements Analysis activity establishes and documents the hardware requirements for each hardware item identified in the System Design Specification.

Items to be considered include:

1. Functional requirements
2. Interfaces to other hardware items
3. Interfaces to software items
4. Safety requirements
5. Human factors requirements
6. Qualification requirements
7. Operation and maintenance requirements
8. Design standards
9. Verification requirements

This information is documented in the Hardware Requirements Specification. [ ]^{a,c}.

Some hardware functions are sufficiently complex as to require additional decomposition into subordinate hardware items (not directly referenced by the System Design Specification). The Hardware Requirements Analysis Activity will produce individual hardware requirements for these subordinate hardware items.

7.4.2. Hardware Implementation Decision

The Hardware Implementation Decision activity determines the implementation path for each hardware item or component. Possible implementation paths include: Internal Design, Subcontract Desigu and Purchase of Commercial Product. This activity includes evaluation of Commercial Products against the hardware requirements.

7.4.3. Hardware Implementation

The Hardware Implementation activity takes one of three paths based on the Hardware Implementation Decision. The separate steps in each path are described below. The three design paths re-converge later in the process.

7.4.3.1. Internal Design Path

Items that have been identified to be designed in-house shall use the following steps.

7.4.3.1.1. Hardware Preliminary Design

The developer produces a preliminary design that establishes the basic functions, an explanation of operation, the performance characteristics, and the user operation or interface characteristics of the item. [

]^{a,c}.

7.4.3.1.2. Hardware Implementation and Engineering Testing

The developer produces a detailed design and tests the hardware. [

]^{a,c}.

7.4.3.2. Subcontractor Desigu Patb

Some items may be inore effectively produced by an outside design organization. Typically, these items represent customization of a vendors' standard product. Items that have been identified to be designed by outside vendors shall use the following steps.

7.4.3.2.1. Vendor Selection

The Hardware Requirements Document for the item is transmitted to potential vendors. Additional vendor requirements may be identified and transmitted to the vendor. Supply Management and Quality Assurance are involved in the process of defining additional vendor requirements. A vendor is selected based on the [ ]^{a,c}.

7.4.3.2.2. Design

The vendor produces a preliminary design that meets the basic functions defined in the Hardware Requirements Document. [

]^{a,c}. The results of the technical review are documented and transmitted to the vendor, and tracked for resolution.

7.4.3.2.3. Quality Assurance Vendor Commercial Survey

Quality Assurance performs a survey of the vendor in accordance with]^{a,c}. Engineering provides inputs to the requirements that are placed on the sub-contractor. At a minimum, the sub-contractor is evaluated for design control. Control of the design is necessary to form a [ ]^{a,c}.

7.4.3.3. Commercial Product Path

Some functions may be provided by existing commercially available standard products. The specific activities for these items are described below.

7.4.3.3.1. Vendor Selection

Item requirements are identified and transmitted to the vendor. Supply Management and Quality Assurance are involved in the process of defining any additional vendor requirements. A vendor is selected based on the [ ]^{a,c}.

7.4.3.3.2. Quality Assurance Vendor Commercial Survey

Quality assurance performs a survey of the vendor in accordance with[ ]^{a,c}. Engineering provides inputs to the requirements that are placed on the vendor. At a minimum, the vendor is evaluated for design control. Control of the design is necessary to form a [ ]^{a,c}.

7.4.4. Commercial Dedication Instruction

A commercial dedication instruction is developed or an [

]^{a,c}.

7.4.5. Final Documeutation Package

For each hardware item, whether internally designed, externally designed or purchased, a set of documentation will be produced. This may consist of [

]^{a,c}.

[ ]^{a,c}.

7.5. [ ]^{a,c} Integration Activity

The developers shall combine the software and hardware items with other product software and hardware and test equipment. The test setup shall be designed to exercise the system (or representative portions of the system) in configurations that are typical of its intended use. [

]^{a,c}.

8. [ ]^{a,c} VERIFICATION ACTIVITIES

The following sections define the various review types, the review techniques that can be employed, and the required platform verification effort.

8.1. Review Types

Reviews are used to perform verification of the design. Documentation produced by these reviews, either review comments, responses to comments, or reports, will become part of the records. The reviews may consist of any of the following:

- [ ]^{a,c}
- [ ]^{a,c}
- [ ]^{a,c}
- [ ]^{a,c}

8.1.1. [ ]^{a,c}

The [

]^{a,c}.

[

]^{a,c}.

[

]^{a,c}.

8.1.2. [ ]^{a,c}

[

]^{a,c}.

[

]^{a,c}.

8.1.3. [ ]^{a,c}

[

]^{a,c}.

[

]^{a,c}.

8.1.4. [ ]^{a,c}

[

]^{a,c}.

[

]^{a,c}.

[

]^{a,c}.

[ ]^{a,c}

8.2. Review Techniques

8.2.1. Inspection

Inspections consist of examining the entity being verified, either hardware or software. Typically, the item is (1) compared to a defined set of acceptance criteria, (2) compared to its requirements, and (3) examined for correctness.

8.2.2. Analysis

Analysis consists of a formally documented evaluation or calculation to confirm some aspect of the design. Analysis includes, but is not limited to, formal proofs, Petri Net and other graphical analysis methods, and related techniques. The analysis may be performed by the verifier, or the verifier may review an analysis performed by the designer.

8.2.3. Testing

Testing consists of operating the system or component, either hardware or software, under specified conditions, observing or recording the results, and making an evaluation of some aspect of the system or component based upon the results. Testing will be performed in a[

]^{a,c}.

8.2.4. Regression Aualysis and Testing

Regression analysis and testing are V&V techniques that are applicable to modifications of a previously verified item.

8.2.4.1. Regression Analysis

Regression analysis evaluates the differences between different releases of a controlled confignration item (e.g., documentation, hardware, software, or system) to determine the V&V actions required. The regression analysis should take account of the following when specifying the V&V technique:

- Type of change (e.g., Function, Confignration, Connection, etc.)
- Complexity of change
- Independence or modularity of the modification from the other parts of the system
- Impacts on interfacing systems

[

]^{a,c}.

8.2.4.2. Regression Tests

Regression tests are a selective retest of the system or component to verify the correctness of the modification. The regression analysis focuses the V&V test on the change. For the areas of the design that have not been changed, credit is taken for previously completed V&V actions. The regression tests should make use of existing test procedures when applicable.

8.3. [ ]^{a,c} Verification Effort

As the [ ]^{a,c} Design Activities proceed in a top-down fashion, the [ ]^{a,c} Verification Activities are performed in a stepwise fashion. As shown in Figure 3 and Figure 4, the following design products are checked for consistency and correctness:

1. System Design Products
   a) System Design Requirements -- [ ]^{a,c}.
   b) System Design Specification --[ ]^{a,c}.
2. Software Design Products
   a) Software Requirements Specifications -- [ ]^{a,c}.

b) Software Design Descriptions -- [ ]^{a,c}.

c) [ ]^{a,c}.

d) Commented Source Code and Object Modules -- [ ]^{a,c}.

3. Hardware Design Products

a) Hardware Requirements Specifications -- [ ]^{a,c}.

b) Draft Hardware Design Specifications -- [ ]^{a,c}.

c) Draft Documentation Package -- [ ]^{a,c}.

d) Final Documentation Package -- [ ]^{a,c}.

In addition to the reviews shown in these figures, one or more [

]^{a,c}.

[

]^{a,c}.

[

]^{a,c}.

9. [ ][a,c VALIDATION TEST AND EQUIPMENT QUALIFICATION TEST

9.1. [ ]a,c Validation Test

The [ ]a,c Validation Test confirms that the system meets the requirements specified in the platform System Desigu Requirements. The tests shall be conducted in accordance with a formal test plan and procedures. The required input signals, the anticipated output siguals, and the acceptance criteria shall be stated in the procedures.

[ ]a,c software items, platform hardware items, representative application software, and test equipment shall be arranged in configurations which represent the intended uses of the [ ]a,c . The configurations may represent entire systems, portions of systems (overlapping validation testing), or "thread paths" through a system.

The test plan should include tests which stress the system beyond its intended uses.

The [

]a,c. They shall prepare the test plan, prepare the test procedures, perform or supervise the tests, and document the test results. The test results will be recorded and retained. The system configuration (including hardware and software version information), the test procedures, and the results shall be documented at a level sufficient to allow the tests to be repeated. [

]a,c

[

]a,c.

9.2. Eqnipment Qualification

Modules must be shown to operate under the design basis for seismic, environmental and EMI conditions. Equipment may be qualified by type testing, analysis or some combination of the two. [

]a,c.

This activity shall be conducted in accordance with a formal equipment qualification plan and shall be documented by a qualification report that summarizes which testing or analysis covers the equipment.

10. [ ]^{a,c} DESIGN ACTIVITIES

The [ ]^{a,c} Desigu, Verification, and Validation Process is detailed in

Figure 5. This section will focus on the design activities (with indication of where verification is required). The figure shows the activities as purely sequential (similar to the classic "Waterfall" methodology). In actuality, [

]^{a,c}.

10.1. [ ]^{a,c} Definition Activity

The [ ]^{a,c} Definition Activity includes the following types of items:

1. Identification of the plant systems involved in the scope of the project.
2. Identification of the system desigu basis for the project.
3. Identification of the licensing basis for the project.
4. Documentation of the objective of the new system or modification.
5. An early evaluation of potential failure modes and impacts on the licensing evaluations.
6. Documentation of what other plant systems are affected.
7. Documentation of project specific methods and activities used in the design, development, documentation, verification, validation, etc.
8. Definition of particular options, features, and plant specific configurations.

This information shall become part of the [

]^{a,c}.

a,c

Figure 5: [ ]^{a,c} Design, Verification, and Validation
(Overview is shown in Figure 2)

10.2. Functional Requirements Capture Activity

The Functional Requirements Capture Activity establishes and documents the design basis for the project. This includes:

- Transfer Function Requirements
- Time Response Requirements
- Accuracy Requirements
- Reliability Requirements
- Availability Requirements
- External Interface Requirements
- Setpoints and Tuning Constants
- Environmental and Seismic Requirements
- Human Factors Requirements
- Response to Failures

This information is documented in the Functional Requirements document. This document may be supplemented or replaced by [ ]^{a,c}.

The effort associated with this activity varies with scope and format of information provided by the customer. The end result must be a complete set of functional requirements in a format usable for the remainder of the process.

[

]^{a,c}.

10.3. [ ]^{a,c} System Design Activities

The [ ]^{a,c} System Design Activities consist of two primary efforts: [

]^{a,c}.

10.3.1. [ ]^{a,c} Requirements Analysis

The [ ]^{a,c} Requirements Analysis determines and documents the system requirements based on the [ ]^{a,c}. The [ ]^{a,c} System Design Requirements are reviewed to determine the applicability of the platform requirements to the application requirements.

[

]^{a,c}.

10.3.2. [ ]^{a,c}

[

]^{a,c}.

[

]a,c.

[

]a,c.

[ ]a,c.

10.4. [ ]a,c

[

]a,c.

[

]a,c.

10.5. [ ]a,c Hardware Design Activities

The [ ]a,c Hardware Design Activity consists largely of configuring the standard hardware [ ]a,c for a specific application. The following sections describe the steps involved.

10.5.1. Hardware System Configuration

The project personnel configure the system according to the [ ]a,c System Design Requirements and the architecture outlined in the [ ]a,c System Design Specification. This is documented by the creation of [

]a,c.

10.5.2. Hardware Cabinet Configuration

Detailed configurations of the hardware and locations of hardware within cabinets are produced. This activity is documented by the creation of cabinet level configuration drawings. Typical information includes placement of cards, specific jumpering or keying of modules, definition of cable connection information, labeling of specific modules or cables, and identification of external termination points for field wiring. These drawings would typically refer to [standard platform drawings and only specify application specific customization. The drawings may be augmented or replaced by a database. [

]a,c.

10.5.3. Manufacturing

Manufacturing involves the production of hardware modules from components according to hardware assembly drawings. This activity may take place internally or at an external manufacturing site. It includes

inspection processes that are defined in manufacturing procedures. Assembled modules typically go through module level testing as part of the manufacturing process. The results of this testing must be recorded for traceability to the module level. Items requiring commercial dedication are dedicated at the module level by the criteria described in the commercial dedication instruction. The applicable instruction for each module must be identified by a drawing or other manufacturing tracking system. The dedication activity must be recorded for [ ]^{a,c}.

10.6. [ ]^{a,c} Integration Activity

The developers shall combine the application software and hardware items with [ ]^{a,c}, and test equipment. The test setup shall be designed to exercise the system (or portion of the system) in a configuration that is typical of its intended use. [

]^{a,c}.

11. [ ]^{a,c} VERIFICATION ACTIVITIES

As the [ ]^{a,c} Design Activities proceed in a [ ]^{a,c}.

The [ ]^{a,c} Verification Activities use the same definitions for review types and techniques as presented in Section 8.1 and Section 8.2, respectively.

As shown in 5, the following design products are checked for consistency and correctness:

1. Functional Requirements Capture Products
   a) Functional Requirements -- [ ]^{a,c}.
2. [ ]^{a,c}
   a) [ ]^{a,c}.
   b) [ ]^{a,c}.
3. [ ]^{a,c}
   a) [ ]^{a,c}.
4. Hardware Design Products
   a) System Level Documentation Package -- [ ]^{a,c}.
   b) Cabinet Level Documentation Package -- [ ]^{a,c}.

In addition to the reviews shown in these figures, [ ]^{a,c}.

[ ]^{a,c}.

[ ]^{a,c}.

The results of the software verification activities are documented in the Software Verification Report.

12. [ ]^{a,c} VALIDATION AND QUALIFICATION TESTS

12.1. [ ]^{a,c} Specific Qualification

An application specific qualification analysis is undertaken to show that the system will meet its design basis for seismic, environmental and EMI conditions. This analysis may confirm that the system has been qualified by previous analysis or testing. It may also indicate that further testing or analysis is needed.
[
]^{a,c}. They shall prepare the qualification plan, prepare any required procedures, perform or supervise any required tests, and document the analysis and/or test results in the Equipment Qualification Report.

12.2. Factory Acceptance Test

The Factory Acceptance Test (FAT) provides the formal validation of the system functionality as specified in the functional requirements. Additionally, the [

]^{a,c}. The required input signals, the anticipated output signals and the acceptance criteria shall be stated in the procedures.

[ ]^{a,c}.

- [ ]^{a,c}
- [ ]^{a,c}

  [ ]^{a,c}
-]^{a,c}
- [ ]^{a,c}

[

]^{a,c}.

[

]^{a,c}.

[

]^{a,c}.

[

]^{a,c}.

[ ]^{a,c}.

12.3. Site Acceptance Test

The Site Acceptance Test (SAT) is performed in the plant. Its purpose is to provide adequate confidence of the following:

1. No damage has occurred due to shipment or installation
2. The system is compatible with the plant
3. The interfaces to other plant systems are correct (especially interfaces which were simulated during the FAT).

[

]^{a,c}.

[

]^{a,c}.

13. SUMMARY OF DESIGN, VERIFICATION AND VALIDATION DOCUMENTS

The tables in this section summarize the documents that are produced in accordance to the design, verification and validation plans contained in this document.

a,c

Table 1: [[[a,c] Design, Verification, and Validation Documents

a,c

Table 2: [ ]^{a,c} Design, Verification, and Validation Documents

a,c

NRC FORM 199
(9-1999)
NRCMD 3.12

U.S. NUCLEAR REGULATORY COMMISSION

PROPRIETARY INFORMATION

NOTICE

THE ATTACHED DOCUMENT CONTAINS OR IS CLAIMED TO CONTAIN PROPRIETARY INFORMATION AND SHOULD BE HANDLED AS NRC SENSITIVE UNCLASSIFIED INFORMATION. IT SHOULD NOT BE DISCUSSED OR MADE AVAILABLE TO ANY PERSON NOT REQUIRING SUCH INFORMATION IN THE CONDUCT OF OFFICIAL BUSINESS AND SHOULD BE STORED, TRANSFERRED, AND DISPOSED OF BY EACH RECIPIENT IN A MANNER WHICH WILL ASSURE THAT ITS CONTENTS ARE NOT MADE AVAILABLE TO UNAUTHORIZED PERSONS.

COPY NO. _____

DOCKET NO. _____

CONTROL NO. _____

REPORT NO. _____

REC'D W/LTR DTD. _____

PROPRIETARY INFORMATION