NEDO-33864 Appendix B (NEDO-33834), NUMAC Systems Engineering Development Plan

Non-Proprietary

GEH Information – Class I (Public)

APPENDIX B

NUMAC SYSTEMS

ENGINEERING DEVELOPMENT PLAN

NEDO-33834, Revision 0

This attachment contains a copy of the stand-alone GEH Standard NUMAC Systems Engineering Development Plan that is applied to the HCGS NUMAC PRNM Retrofit Project; as such, it has not been reformatted for NEDO-33864.

HITACHI

GE Hitachi Nuclear Energy

NEDO-33834
Revision 0
April 2015

GEH Information – Class I (Public)

NUMAC SYSTEMS

ENGINEERING DEVELOPMENT PLAN

INFORMATION NOTICE

This is a non-proprietary version of the document NEDE-33834P, which has the proprietary information removed. Portions of the document that have been removed are indicated by a set of open and closed double square brackets as shown here [[ ]].

IMPORTANT NOTICE REGARDING CONTENTS OF THIS REPORT

Please Read Carefully

The design, engineering, and other information contained in this document is furnished for the purposes of supporting NUMAC digital instrumentation and control products in proceedings before the U.S. Nuclear Regulatory Commission. The only undertakings of GEH with respect to information in this document are contained in the contracts between GEH and its customers or participating utilities, and nothing contained in this document shall be construed as changing that contract. The use of this information by anyone for any purpose other than that for which it is intended is not authorized; and with respect to any unauthorized use, GEH makes no representation or warranty, and assumes no liability as to the completeness, accuracy, or usefulness of the information contained in this document.

No use of or right to copy any of this information contained in this document, other than by the NRC and its contractors in support of an application for a NUMAC digital instrumentation and control products, is authorized except by contract with GEH, as noted above. The information provided in this document is part of and dependent upon a larger set of knowledge, technology, and intellectual property rights pertaining to the design of standardized, nuclear powered, electric generating facilities. Without access and a GEH grant of rights to that larger set of knowledge, technology, and intellectual property rights, this document is not practically or rightfully usable by others, except by the NRC.

Revision History

Revision	Description of Changes
0	Initial revision

TABLE OF CONTENTS

1.0 Introduction

This NUMAC Systems Engineering Development Plan and its companion plans define a development program for NUMAC digital instrumentation and control products that is consistent with U.S. Nuclear Regulatory Commission (NRC) requirements for a high quality development process for software used in safety systems of nuclear power plants. NUREG 0800, Standard Review Plan, Branch Technical Position (BTP) 7-14, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems, provides acceptance criteria for process planning. This NUMAC Systems Engineering Development Plan, hereafter referred to as the NUMAC SyEDP, addresses process planning characteristics defined in BTP 7-14 Section B.3.1.2, Software Development Plan; BTP 7-14 Section B.3.1.4, Software Integration Plan; and BTP 7-14 Section B.3.1.11, Software Configuration Management Plan.

This NUMAC SyEDP is used in conjunction with the NUMAC Systems Independent Verification and Validation Plan, hereafter referred to as the NUMAC SyIVVP, and with the NUMAC Systems Quality Assurance Plan, hereafter referred to as the NUMAC SyQAP. The plans (NUMAC SyEDP, NUMAC SyIVVP, and NUMAC SyQAP) define activities that are specific to NUMAC digital I&C retrofit projects. These activities are performed in accordance with the applicable policies and procedures of the GE-Hitachi Nuclear Energy Quality Assurance Program described in NEDO-11209-A that meets the requirements of 10CFR50 Appendix B.

The GEH Quality Assurance Program encompasses design engineering related activities such as design process, verification, dedication, qualification of personnel performing design work, condition reporting, and archiving of quality records. The NUMAC SyEDP and its companion plans supplement the GEH Quality Assurance Program by defining project activities performed in a specific way, or in addition to activities governed by the GEH Quality Assurance Program.

1.1 Purpose and Scope

This NUMAC SyEDP establishes processes for design and development, integration, and configuration management of safety-related NUMAC products. The plan is designed to remain in effect throughout the entire product life cycle. This NUMAC SyEDP, or a subset thereof, may also be used for non-safety-related NUMAC products. The scope of this plan for such applications shall be determined during the project Concept Phase and documented in the project System Management Plan (SyMP) as described in Section 1.2 below.

1.2 Review and Applicability

For each specific application of this NUMAC SyEDP to the development of a NUMAC product, a review of this plan shall be conducted during the project Concept Phase (see Section 3.1.1). This review shall assure the suitability of the NUMAC SyEDP for the project. The results of this review shall be used in the preparation of the SyMP that shall formally document the application of this NUMAC SyEDP and its companion plans to the development of the NUMAC product.

1.3 Acronyms

BTP	Branch Technical Position
CCB	Change Control Board
ECO	Engineering Change Order
EPROM	Electrically Programmable Read-Only Memory
FDI	Field Disposition Instruction
FDDR	Field Deviation Disposition Request
FPGA	Field Programmable Gate Array
GEH	GE Hitachi Nuclear Energy
HMI	Human-Machine Interface
I&C	Instrumentation and Control
I/O	Input/Output
IPS	Instrument Performance Specification
NRC	Nuclear Regulatory Commission
NPR	NUMAC Problem Report
NUMAC	Nuclear Measurement Analysis and Control
O&M	Operation and Maintenance
PLD	Programmable Logic Device
PWP	Project Work Plan
SyCM	System Configuration Management
SyEDP	Systems Engineering Development Plan
SyIVVP	Systems Independent Verification and Validation Plan
SyMP	System Management Plan
SyQAP	Systems Quality Assurance Plan
V&V	Verification and Validation

1.4 References

1. NEDE-33835P, NUMAC Systems Independent Verification and Validation Plan.
2. NEDE-33836P, NUMAC Systems Quality Assurance Plan.
3. NEDO-11209-A, GE-Hitachi Nuclear Energy Quality Assurance Program Description
4. NUREG-0800, Branch Technical Position 7-14, Guidance on Software Reviews for

2.0 Implementation of the NUMAC SyEDP

This NUMAC SyEDP governs the design and development, product integration, and configuration management activities that are performed by the product design team.

2.1 Organization

The design team includes project engineers, system engineers, hardware engineers, and software engineers, as necessary, from the I&C Engineering organization. Managerial oversight of the design team activities that are executed in accordance with this plan is performed by I&C Engineering management. The NUMAC SyIVVP describes the provisions for organizational independence between the design team and the team performing the independent V&V activities. The NUMAC SyQAP describes the provisions for oversight of the process by the GEH Quality Assurance organization.

2.2 Responsibilities

2.2.1 Design Team

The design team responsibilities are to:

- Define project requirements and establish requirements traceability
- Create and document the design artifacts with traceability to the requirements
- Integrate and test the product, and document the test results
- Create and release manufacturing drawings, installation instructions, operation and maintenance instructions, user manuals, etc.
- Resolve any anomalies noted by the independent V&V team
- Support the factory acceptance test [[ ]]
- Prepare documentation to support licensing submittal
- Prepare for and participate in the Technical Design Review process (see Section 4.2)

2.2.2 System Configuration Management Engineer

The System Configuration Management Engineer, hereafter referred to as the SyCM Engineer, is a member of the design team. The SyCM Engineer responsibilities are to:

- Prepare the project configuration status accounting at each life cycle phase, including changes to a previously baselined configuration (see Section 4.4.1)
- Document performance of configuration management activities at each life cycle phase, including changes to the configuration, in the System Configuration Management (SyCM) Task Report (see Section 4.4.2)

- Prepare for and participate in the Baseline Review process (see Section 4.3)

3.0 NUMAC Digital I&C Development Life Cycle

The NUMAC Digital I&C Development Life Cycle follows a waterfall model approach that comprises the following five life cycle phases or baselines:

1. Concept Phase (Baseline 1)
2. Requirements Phase (Baseline 2)
3. Design Phase (Baseline 3)
4. Implementation Phase (Baseline 4)
5. Test Phase (Baseline 5)

The documentation produced within in a given life cycle phase must be technically adequate and sufficiently complete to formally begin the next life cycle phase (see Section 4.0). The documents developed throughout the life cycle may be baselined at any time even though some portion or portions of the design are incomplete or preliminary at that time. As the design process progresses, each baseline will address missing or preliminary information from earlier phases. At the completion of the design process the final version of each document will be complete and verified, with all open items closed, all changes incorporated, all comments resolved and will be in agreement with the final NUMAC product. Initial and interim versions of these documents may be released with deferred verification status in accordance with the applicable GEH policies and procedures in order to maintain configuration control.

3.1 Concept Phase (Baseline 1)

The Concept Phase of the development life cycle includes confirmation of applicability of the NUMAC planning documents via a project specific System Management Plan and development of a proposed design approach to fulfill the needs of the project. This phase of the life cycle is concluded with a technical design review (see Section 4.2) and a baseline review (see Section 4.3) to establish the Concept Phase baseline and authorize the project to proceed to the Requirements Phase. The configuration items required to be baselined at the completion of the Concept Phase are:

1. System Management Plan
2. NUMAC SyEDP (this plan)
3. NUMAC SyIVVP, Reference 2
4. NUMAC SyQAP, Reference 3
5. Project Work Plan
6. Concept Description

The documents identified above shall be released in the GEH document configuration management system in accordance with applicable GEH policies and procedures, and included in the project Concept Phase baseline review records (see Section 4.4).

3.1.1 Project Planning

3.1.1.1 System Management Plan

The System Management Plan (SyMP) is the master plan used by the project manager, in conjunction with the project schedule, to manage the NUMAC digital I&C retrofit project. The project SyMP addresses process planning characteristics defined in BTP 7-14 Section B.3.1.1, Software Management Plan. The project SyMP invokes the standard NUMAC Digital I&C Development Program for the project by referencing the NUMAC SyEDP, NUMAC SyIVVP, and NUMAC SyQAP, as discussed in the following sections.

3.1.1.2 NUMAC SyEDP

The NUMAC SyEDP (this plan) is reviewed for applicability to the project and is referenced in the Project SyMP in order to apply the plan to the project. The SyMP specifies applicability of the NUMAC SyEDP for the design and development, integration, and configuration management aspects of the digital I&C retrofit project.

3.1.1.3 NUMAC SyIVVP

The NUMAC SyIVVP is reviewed for applicability to the project and is referenced in the project SyMP in order to apply the plan to the project. The SyMP specifies applicability of the NUMAC SyIVVP for the safety analysis, verification and validation, and independent testing and qualification aspects of the digital I&C retrofit project.

3.1.1.4 NUMAC SyQAP

The NUMAC SyQAP is reviewed for applicability to the project and is referenced in the project SyMP in order to apply the plan to the project. The SyMP specifies applicability of the NUMAC SyQAP for the quality assurance oversight aspects of the digital I&C retrofit project.

3.1.1.5 Project Work Plan

The Project Work Plan (PWP) is required by GEH policies and procedures. The PWP contains personnel and commercial information, including project budgetary information that is classified as GEH Proprietary Class III (confidential). The PWP is created and maintained by the Project Manager to manage the commercial aspects of the project.

3.1.2 Concept Description

The concept description provides documentation of the proposed design approach to fulfill the needs of the project and is considered to be a technically focused extension of the project plans. The concept description is a vehicle for the independent review team to evaluate the proposed design approach and to provide feedback to the design team as part of the baseline process (see Section 4.0). In this way, the concept is refined to maximize opportunity for a successful project at the beginning of the product development life cycle. The concept description is not a design input itself, but it should discuss the strategy for establishing requirements traceability, and it should identify the technical design inputs for the project that will establish the starting point for

requirements traceability. The concept description may also describe [[

]]

3.2 Requirements Phase (Baseline 2)

The Requirements Phase of the development life cycle includes development of a top-level system requirements specification and an instrument performance specification for each NUMAC instrument in the system. The division between hardware and software is defined in the instrument performance specification. The associated hardware and software requirements are included [[ ]] in the instrument performance specification. Requirements for system and sub-system interfaces are also defined at this time. This phase of the life cycle is concluded with a technical design review (see Section 4.2) and a baseline review (see Section 4.3) to establish the Requirements Phase baseline and authorize the project to proceed to the Design Phase. The configuration items required to be baselined at the completion of the Requirements Phase are:

1. System Requirements Specification
2. NUMAC Instrument Performance Specification (includes hardware and software)

The documents identified above shall be released in the GEH document configuration management system in accordance with applicable GEH policies and procedures, and included in the project Requirements Phase baseline review records (see Section 4.4) as applicable.

3.2.1 System Requirements Specification

The system functional and design requirements are normally contained in the System Requirements Specification (and accompanying Data Sheet, if needed). Traceability of the system requirements to the project design inputs identified in the previous life cycle phase shall be established. The System Requirement Specification shall incorporate the requirements and the acceptance criteria for validation of the system. If there is no System Requirements Specification for the project, then some other document or documents must identify all of the requirements that are applicable to the NUMAC product design. The document or documents containing the system requirements shall be verified to confirm that the requirements of the customer contract or internal work authorization are captured and checked for completeness using the following checklist:

- [[
  -
  -
  -
  -
  -
-
-
-
-

-
-
-
-
-
-
-
-
-
-
-]]

Applicability of the above items is determined based on the needs of the project. The System Requirements Specification may include requirements beyond what is suggested in this list, depending on the needs of the project.

3.2.2 NUMAC Instrument Performance Specification

A NUMAC Instrument Performance Specification (IPS) shall be prepared for each NUMAC instrument. The IPS shall contain the hardware and software performance requirements for the NUMAC instrument, [[

]]. The IPS shall incorporate the requirements and the acceptance criteria for validation of the NUMAC instrument. Traceability of the IPS requirements to the applicable system requirements (see Section 3.2.1) and other design inputs identified in the previous life cycle phase, as applicable, shall be established.

3.2.2.1 Hardware Requirements

The NUMAC instrument performance specification shall include, as a minimum, the following hardware requirements:

- [[
-
-
-
-
-
-

]]

The above hardware requirements may be incorporated entirely within the IPS, or may be incorporated in the IPS by reference to another hardware specific document (e.g. hardware module performance specification), or a combination thereof.

3.2.2.2 Software Requirements

The NUMAC instrument performance specification shall include, as a minimum, the following software requirements:

- [[
-
-
-
-
-
-
-
-
-]]

The software requirements for a NUMAC instrument are typically contained entirely within the product IPS.

3.3 Design Phase (Baseline 3)

The Design Phase of the development life cycle includes definition of the system and sub-system architecture and interfaces, and high level hardware and software design. The hardware circuitry and programmable logic functions are defined at this phase. The software architecture and structure, and the general module functions, including the human-machine interface functions, are also defined at this phase. This phase of the life cycle is concluded with a technical design review (see Section 4.2) and a baseline review (see Section 4.3) to establish the Design Phase baseline and authorize the project to proceed to the Implementation Phase. The configuration items required to be baselined at the completion of the Design Phase are:

1. System Elementary Diagram
2. NUMAC Instrument Schematic
3. Hardware Design Documentation including:
    a. Hardware Module Design Specification
    b. Programmable Logic Device Design Specification
    c. Hardware Module Schematic
4. Software Design Documentation including:

a. Functional Controller Software Design Specification

b. Display Controller Software Design Specification

c. Human-Machine Interface Design Specification

d. Digital Signal Processor Software Design Specification

5. Communication Protocol Documentation including:

a. External Communication Protocol

b. Intra-System Communication Protocol

c. Inter-Computer Communication Protocol

The documents identified above shall be released in the GEH document configuration management system in accordance with applicable GEH policies and procedures, and included in the project Design Phase baseline review records (see Section 4.4) as applicable.

3.3.1 System Elementary Diagram

The System Elementary Diagram includes a [[

]] The System Elementary Diagram shall be traceable to the System Requirements Specification from the previous life cycle phase (see Section 3.2.1).

3.3.2 NUMAC Instrument Schematic

A NUMAC Instrument Schematic shall be prepared for each NUMAC instrument. The instrument schematic includes a [[

]] The NUMAC Instrument Schematic shall be traceable to the applicable NUMAC Instrument Performance Specification from the previous life cycle phase (see Section 3.2.2). T he NUMAC Instrument Schematic shall also be verified for consistency with the System Elementary Diagram (see Section 3.3.1).

3.3.3 Hardware Design Documentation

Hardware modules are, in most cases, developed as general purpose modules that may be used in multiple NUMAC applications (e.g. computer module). The performance requirements for a general purpose hardware module are typically captured in a hardware module performance specification that defines the functional and electrical characteristics of the module. The hardware module performance specification would then be included by reference in the IPS for

the NUMAC instrument where the module is used. The hardware design documentation discussed in the following sections shall be traceable to the applicable hardware module performance specification and/or to the applicable NUMAC Instrument Performance Specification from the previous life cycle phase (see Section 3.2.2).

3.3.3.1 Hardware Module Design Specification

The Hardware Module Design Specification provides [[
]]. Functions that are to be performed in a programmable logic device (e.g. PLD or FPGA) are identified, and the programmable logic device design is included by r eference to the applicable Programmable Logic Device Design Specification (see Section 3.3.3.2) or may be included entirely with the Hardware Module Design Specification. The Hardware Module Design Specification includes [[
]]

3.3.3.2 Programmable Logic Device Design Specification

The Programmable Logic Device Design Specification describes the [[
]]. This includes [[
]]

3.3.3.3 Hardware Module Schematic

The Hardware Module Schematic provides a [[

]] are shown. The information is arranged in a manner to aid in understanding the operation of the circuits and does not necessarily correspond to the physical layout of the hardware module.

3.3.4 Software Design Documentation

The software for each NUMAC product is developed uniquely for that product. For a mature product line [[
]]nevertheless, the software for every project is documented and tested specifically for that project. Most NUMAC projects involve some [[
]]. The software design documentation discussed in the following sections shall be traceable to the applicable NUMAC Instrument Performance Specification from the previous life cycle phase (see Section 3.2.2).

3.3.4.1 Functional Controller Software Design Specification

The Functional Controller Software Design Specification shall provide a [[

]] The Functional Controller Software Design Specification shall also contain sufficient detail to show which software procedures perform the functions defined in the applicable NUMAC Instrument Performance Specification from the previous life cycle phase (see Section 3.2.2), including input processing, algorithms, output processing, task timing, and task prioritization.

3.3.4.2 Display Controller Software Design Specification

The Display Controller Software Design Specification shall provide a [[

]] The Display Controller Software Design Specification shall also contain sufficient detail to show which software procedures perform the human-machine interface functions defined in the applicable NUMAC Instrument Performance Specification from the previous life cycle phase (see Section 3.2.2). The details of the human-machine interface are defined in the Human-Machine Interface Design Specification (see Section 3.3.4.3).

3.3.4.3 Human-Machine Interface Design Specification

The human-machine interface (HMI) design specification defines the critical characteristics and functionality of the user interface including but not limited to the following:

- [[
-
-
-
-]]

The HMI design specification may be issued as a separate design document or it may be incorporated within the Display Controller Software Design Specification (see Section 3.3.4.2).

3.3.4.4 Digital Signal Processor Software Design Specification

Some NUMAC applications use a digital signal processor module to perform pre-processing of certain signals. The digital signal processor exchanges data with the functional controller [[

]]. The Digital Signal Processor Software Design Specification shall provide a [[

]]. The Digital Signal Processor Software Design Specification shall also contain sufficient detail to show which functions defined in the applicable NUMAC Instrument Performance Specification from the previous life cycle phase (see Section 3.2.2) are performed in the digital signal processor.

3.3.5 Communication Protocol Documentation

The [[ ]] are defined in communication protocol specifications. Communication protocol specifications may apply at the system level, sub-system level, or component level as discussed in the following sections.

3.3.5.1 External Communication Protocol Specification

The External Communication Protocol Specification shall describe the [[ ]]. The External Communication Protocol Specification shall be traceable to the System Requirements Specification from the previous life cycle phase (see Section 3.2.1).

3.3.5.2 Intra-System Communication Protocol Specification

The Intra-System Communication Protocol Specification shall describe the [[ ]] The Intra-System Communication Protocol Specification shall be traceable to the applicable NUMAC Instrument Performance Specifications (see Section 3.2.2) and/or to the System Requirements Specification from the previous life cycle phase (see Section 3.2.1). The Intra-System Communication Protocol Specification shall be verified to be consistent with the External Communication Protocol Specification (see Section 3.3.5.1) to ensure that data exchange between the sub-systems supports the data exchange with external systems.

3.3.5.3 Inter-Computer Communication Protocol Specification

The Inter-Computer Communication Protocol Specification (also referred to as CommBlocks) shall describe the [[ ]] The Inter-Computer Communications Protocol shall be traceable to the applicable NUMAC Instrument Performance Specification from the previous life cycle phase (see Section 3.2.2). The Inter-Computer Communication Protocol Specification shall be verified to be consistent with the HMI Design Specification (see Section 3.3.4.3) to ensure that data exchange required to support the user interface has been accounted for.

3.4 Implementation Phase (Baseline 4)

The Implementation Phase of the development life cycle includes preparation of the hardware manufacturing drawings as well as detailed design of the software and programmable logic in source code. The design team performs testing of software and programmable logic at various levels to ensure that the individual modules and the integrated design are performing correctly. Testing performed by the design team is documented in a test item transmittal report prior to turnover to the independent V&V test team for independent testing (see Reference 1). The firmware is released as unverified, pending completion of independent testing in the next phase. This phase of the life cycle is concluded with a technical design review (see Section 4.2) and a

baseline review (see Section 4.3) to establish the Implementation Phase baseline and authorize the project to proceed to the Test Phase. The configuration items required to be baselined at the completion of the Implementation Phase are:

1. Hardware Manufacturing Drawings
2. Source Code
3. Code Review Report
4. Build Description
5. Test Item Transmittal Report
6. Firmware Conditional Release

The documents identified above shall be released in the GEH document configuration management system in accordance with applicable GEH policies and procedures, and included in the project Implementation Phase baseline review records (see Section 4.4) as applicable.

3.4.1 Hardware Manufacturing Drawings

Hardware manufacturing drawings may include items such as [[

]] In general, hardware manufacturing drawings are verified against and traceable to the applicable design documentation produced in the previous life cycle phase. In some cases, hardware manufacturing drawings will be released with deferred verification status, pending completion of equipment qualification and/or independent V&V testing activities. The conditional release of EPROM and/or PLD drawings is one specific example (see Section 3.4.6).

3.4.2 Source Code

Source code includes any program listing written in a programming language (e.g. C, Asm, Verilog, etc.) used to create the program for a digital part (e.g. microprocessor, digital signal processor, or programmable logic device). Source code is verified against and traceable to the applicable design documentation produced in the previous life cycle phase. Source code is verified through code review (see Section 3.4.3).

3.4.3 Code Review Report

Code review is required for all NUMAC source code. Code review is a design verification activity that confirms the source code (see Section 3.4.2) conforms with its applicable design specification, and to [[ ]]. The results of code review are documented in a code review report. The code review report may be a separate document, or it may be incorporated entirely within the applicable test item transmittal report (see Section 3.4.5). C ode review is performed by an individual from the design team other than the responsible designer to verify and release the applicable source code in the GEH configuration management system. The independent V&V team performs an independent code review on the released source code for all safety related source code (see Reference 1).

3.4.4 Build Description

The build description includes all of the information necessary to recreate the program for a digital part (e.g. microprocessor, digital signal processor, or programmable logic device) from the source code. The build description should also include a means of confirming a successful build, such as a program checksum. The build description may be a separate document, or it may be incorporated entirely within the applicable test item transmittal report (see Section 3.4.5) for the associated functional controller software, display controller software, digital signal processor software, or programmable logic device.

3.4.5 Test Item Transmittal Report

The test item transmittal report is the formal handoff from the design team to the independent V&V test team. A test item transmittal report identifies a test item or test items that are ready for independent testing by the independent V&V test team.

Test items may include [[
]], as well as the [[
]] The test item transmittal report documents the status of the test item being transmitted, including the location of source code in the configuration management system, results of code reviews performed, build instructions, and the results of unstructured testing performed by the design team. The results of code reviews may be included by reference to a separate code review report (see Section 3.4.3), or included entirely within the test item transmittal report. Likewise, the instructions for how to build the software or programmable logic may be included by reference to a separate build description (see Section 3.4.4), or included entirely within the test item transmittal report.

The test item transmittal report shall provide [[
]] to confirm that the design is complete and consistent with all applicable design documentation, and that the design is ready for independent testing by the independent V&V test team (see Reference 1).

3.4.5.1 Use of Previously Developed Software

Most NUMAC products developed today include [[
]] depending on the nature of the product. The more mature and standardized a product line is, the more likely [[ ]].
The test item transmittal report shall discuss the pedigree of any [[ ]] software used in the NUMAC product to justify the extent of testing performed by the design team (see Section 3.4.5.2) [[
]].

Whenever software from a previous NUMAC product is used as the starting point for a new NUMAC product, the software should be built according to the original build instructions and the resulting build checksum confirmed. This practice provides confirmation that the software used as the starting point, and the build environment, are as expected.

3.4.5.2 Unstructured Testing

Unstructured testing is testing performed by the design team without a formal test plan or procedure. The four types of unstructured testing are exploratory testing, software module (unit) testing, programmable logic module (unit) testing, and product integration testing. Software module testing, programmable logic module testing and product integration testing must meet specific testing requirements as discussed below.

3.4.5.2.1 Exploratory Testing

Exploratory testing is used by the designer to evaluate specific implementation ideas such as display arrangements or specific filtering logic. This type of testing is performed throughout development at the discretion of the designer and requires no specific documentation.

3.4.5.2.2 Software Module Testing

Software module (unit) testing is used to confirm the performance of individual software modules or a group of related modules in the functional and display controllers, and in the digital signal processor modules. Though module testing is unstructured, it does have specific requirements. Module testing shall evaluate the [[
]] Testing shall be conducted for [[
]] Module accuracy and processing time shall be tested if applicable.
Module tests [[
]]to exercise the module(s) under test. Individual test records shall be kept for each module or group of modules except where it can be demonstrated that simplicity or previous application can justify abbreviated testing or code review in lieu of testing. All modules in the software package shall be addressed.

The functional controller testing is performed on a NUMAC chassis [[

]] The functional controller module testing shall be traceable to the applicable Functional Controller Software Design Specification from the previous life cycle phase (see Section 3.3.4.1).

The display controller testing is performed on display test hardware [[ ]]. This testing may also be performed on a full NUMAC assembly. [[
]] The display controller module testing shall be traceable to the applicable Display Controller Software Design Specification from the previous life cycle phase (see Section 3.3.4.2) and also to the applicable HMI Design Specification from the previous life cycle phase (see Section 3.3.4.3).

The digital signal processor testing is performed to confirm the performance of the software modules under test. [[
]] The digital signal processor module testing shall be traceable to the applicable Digital Signal Processor Software Design Specification from the previous life cycle phase (see Section 3.3.4.4).

Results, methods, and extent of software module testing shall be recorded during the testing and shall be included in a test item transmittal report.

3.4.5.2.3 Programmable Logic Module Testing

Programmable logic module (unit) testing is used to confirm the performance of the logic synthesis that is to be programmed into a programmable logic device (PLD or FPGA) that is a component of a hardware module. This type of testing uses [[ ]]to evaluate and confirm the proper operation of the logic independent of the hardware. The device is then programmed and integrated into the hardware module that uses it. Once integrated into the hardware module, testing of the programmable logic device may be performed using conventional test methods and tools to stimulate inputs to the hardware module and monitor outputs from the hardware module. The programmable logic module testing shall be traceable to the applicable Programmable Logic Device Design Specification from the previous life cycle phase (see Section 3.3.3.2).

Results, methods, and extent of programmable logic module testing shall be recorded during the testing and shall be included in a test item transmittal report.

3.4.5.2.4 Integration Testing

Integration testing is performed on the target hardware, [[ ]]. Its purpose is to confirm that all instrument functions are working properly and that the hardware, programmable logic, functional software, display software, and digital signal processor software are properly integrated and perform correctly in the target hardware. This level of testing will typically involve the use of [[

]]

The scope of the integration testing shall include[[

]]. Integration testing shall evaluate each instrument function over its entire process range including bounding conditions and timing considerations. Integration testing employs a combination of [[

]] to test internal and interface aspects of the design. Integration testing is also used to confirm self-test [[

]]

Results, methods, and extent of integration testing shall be recorded during the testing and shall be included in a test item transmittal report.

3.4.6 Firmware Conditional Release

The EPROM and/or PLD drawings are issued with deferred verification status in the GEH configuration management system pending completion of the required independent V&V activities in the next phase, including independent testing (see Reference 1). The deferred verification status will be cleared only when all independent V&V activities have been

successfully completed and all open items have been resolved. If changes are required to resolve anomalies noted by the independent V&V test team, the verification status shall remain deferred until all independent V&V activities have been successfully completed.

3.5 Test Phase (Baseline 5)

The design team activities during the Test Phase of the development life cycle include: (1) resolution of any anomalies identified in the independent testing performed by the independent V&V test team (see Reference 1); (2) preparation of user documentation by the design team; and (3) final issuance of the verified firmware. This phase of the life cycle is concluded with a technical design review (see Section 4.2) and a baseline review (see Section 4.3) to establish the Test Phase baseline. At this phase of the project life cycle any remaining open items must be closed and all documentation released as complete and verified. The configuration items required to be baselined at the completion of the Test Phase are:

1. User Documentation
2. Installation instructions
3. Firmware Unconditional Release

The documents identified above shall be released in the GEH document configuration management system in accordance with applicable GEH policies and procedures, and included in the project Test Phase baseline review records (see Section 4.4) as applicable.

3.5.1 User Documentation

The user documentation provides instructions for how to safely operate and maintain the system once it is installed in the nuclear power plant. A user manual that defines the operation of the instrument front panel keypad and displays is included in the NUMAC instrument operation and maintenance (O&M) manual. The O&M manual also provides a description of the theory of operation of the NUMAC instrument, operating procedures for various modes of operation, installation and maintenance information such as required adjustments, troubleshooting guide, list of spare parts, etc.

3.5.2 Installation Instructions

The Field Disposition Instruction (FDI) provides instructions for installation of the equipment in the nuclear power plant. The FDI will reference the appropriate drawings and list materials and tools required to install and confirm proper operation of the equipment.

3.5.3 Firmware Unconditional Release

At the conclusion of the technical design review (see Section 4.2) for the Test Phase all independent V&V activities will be completed (see Reference 1), with all anomalies resolved, and all test reports released with no further open items. At this point the firmware is issued as final and verified, and the baseline review records are updated to reflect the final revision of the verified firmware (see Section 4.4).

4.0 Baseline Process

The baseline process described in the following sections is the method used to review and approve design artifacts for application to a NUMAC product. A baseline is established when [[

]]

Any changes to a previously baselined configuration must be justified and approved through the baseline process. When a baseline includes changes to a previously baselined configuration, the baseline review records will include an assessment of the change impact to ensure that effects of the change are fully evaluated as part of the review and approval process (see Section 4.4.2).

4.1 Design Team's Role in the Baseline Process

The design team initiates the baseline process by requesting a technical design review through the Chief Engineer's Office (see Section 4.2). In addition, the SyCM Engineer is a member of the baseline review team (see Section 4.3), and the SyCM engineer prepares the baseline configuration documentation that constitutes the design team's contribution to the baseline review records (see Section 4.4).

4.2 Technical Design Review

[[

]]

4.3 Baseline Review

[[

]]

4.4 Baseline Review Records

The state of the project may be determined at any time during the project life cycle through an audit of the baseline review records.

4.4.1 Configuration Status Accounting

The configuration status accounting sheet identifies the configuration items for the project by title, by the unique document identifier assigned by the configuration management system, and by revision. The revision is tracked for each life cycle phase such that a review of the configuration status accounting sheet will identify any previously baselined configuration items that have changed.

4.4.2 System Configuration Management Task Report

The SyCM Task Report provides objective evidence that the configuration management activities have been carried out in accordance with this plan. The SyCM Task Report is used to document the assessment of changes made to a previously baselined configuration. The reason for the change and the impact of the change are documented in the SyCM Task Report to

facilitate additional reviews of the previously baselined items that have been modified and to ensure that all affected items have been identified.

The SyCM Task Report is also used to track open items that may affect design artifacts later in the life cycle. For each open item, the status is tracked and reviewed during the baseline process, and as open items are closed the final resolution is documented in the report.

The SyCM Task Report may be provided to the U.S. NRC (or foreign regulatory agency, as applicable) as objective evidence of the configuration management activities for the project.

4.4.3 Other Baseline Documentation

The complete baseline review record comprises the Configuration Status Accounting and SyCM Task Report described above, and the following baseline documentation described in other plans:

- System Verification and Validation Task Report (see Reference 1)
- System Safety Analysis Task Report (see Reference 1)
- Functional Configuration Audit Checklist (see Reference 2)

4.5 Configuration Control

4.5.1 Change Initiation Process

The Change Initiation Process commences with the identification of a discrepancy or deficient condition detected in a previously baselined item. The discrepancy or deficient condition may be documented by any of the following forms:

1. NUMAC Problem Report (NPR)
2. Engineering Change Order (ECO)
3. Field Deviation Disposition Request (FDDR)

A NUMAC Problem Report (NPR) may be opened by anyone observing a problem with a NUMAC product (see Section 7.0). An ECO is used to process design changes during the normal course of development. A Field Deviation Disposition Request is used to initiate changes to resolve issues that are discovered post-shipment, typically during installation.

4.5.2 Change Control Process

Changes to the configuration are handled in accordance with the change control policies and procedures of the GEH Quality Assurance Program. In addition, changes to previously baselined items are evaluated during the technical design review (see Section 4.2) and during the baseline review (see Section 4.3) as described above.

4.5.3 Change Approval Process

When changes are made to a previously baselined configuration, the baseline review team performs a change control board (CCB) function to approve the changes (see Section 4.3) as part of the new baseline that is established at the end of the present life cycle phase.

5.0 Use of Development Tools

The use of development tools is necessary for the development of any digital system. Development tools that have the potential to introduce errors into the design shall be used in a manner such that defects that may be introduced by the use of the tool will be detected either through testing performed by the design team (see Section 3.4.4) or through independent V&V testing (see Reference 1). Regardless, a tool evaluation report documenting the capabilities and limitations of the development tool shall be prepared by the design team for every development tool. The baseline review team approves the use of development tools based on these tool evaluation reports as part of the baseline review process (see Section 4.3). Examples of development tools that require a tool evaluation report and approval for use by the baseline review team include [[
]]. The configuration status accounting for the project (see Section 4.4.1) shall include all applicable development tool evaluation reports for tools that are used on the project.

6.0 Secure Development and Operational Environment

Product integrity during development is maintained in accordance with GEH policies and procedures that contribute to a secure development environment. Access to the NUMAC development lab is controlled and monitored. P roduction equipment is segregated from prototype equipment used for development to further limit access. Scanning tools are used when appropriate to ensure that no malicious software is present. T amper proof seals are used to ensure the integrity of the equipment while it is in transit to the customer.

During software development, source code is maintained on a secure server in the NUMAC development lab. All documentation, including source code, is secured when it is released in the GEH configuration management system to prevent unauthorized modifications. Source code is reviewed to ensure that no unwanted or unused code is present in the design. The software for the microprocessor based controllers in a NUMAC [[
]] and it cannot be inadvertently or maliciously modified in the field.

Security features that contribute to a secure operational environment (e.g. keylock and password and access controls) are standard NUMAC features. Other security features may be incorporated into the design as required to mitigate identified vulnerabilities.

Finally, the independent review team performs a security analysis at every phase in the life cycle to ensure that identified vulnerabilities are being addressed (see Reference 1).

7.0 NUMAC Problem Reports

Any deviation from a baselined design may be recorded with a NUMAC Problem Report (NPR). An NPR may be generated by anyone identifying a design problem with a NUMAC product at any time during the product life cycle; however, most problems identified during product development are generally handled through an engineering change order (ECO) in accordance with the change control processes of the GEH Quality Assurance Program. Most NUMAC Problem Reports are associated with customer feedback reported to GEH following delivery and installation of the NUMAC product, typically to report undesirable or unexpected behavior of the product. Applicable NPRs shall be reviewed in the Concept Phase of the project development

life cycle (see Section 3.1.2) and corrective measures incorporated into new designs in order to promote continuous improvement of the NUMAC product line.