



**HITACHI**

**GE Hitachi Nuclear Energy**

James C. Kinsey  
Vice President, ESBWR Licensing

PO Box 780 M/C A-55  
Wilmington, NC 28402-0780  
USA

T 910 675 5057  
F 910 362 5057  
jim.kinsey@ge.com

Proprietary Notice

*This letter forwards proprietary information in accordance with 10CFR2.390. Upon the removal of Enclosure 1, the balance of this letter may be considered non-proprietary.*

MFN 07-627

Docket No. 52-010

January 21, 2007

U.S. Nuclear Regulatory Commission  
Document Control Desk  
Washington, D.C. 20555-0001

**Subject: Submittal of DOORS Software Audit Presentation Materials and Slides for Support of ESBWR Design Certification Application – Human Factors Engineering**

The purpose of this letter is to submit a copy of presentation materials used during the NRC for audit of the Dynamic Object-Oriented Requirements System (DOORS) Software conducted November 13 through November 16, 2007.

This letter is to support NRC review of the GEH application for final design approval and standard design certification of the ESBWR standard plant design pursuant to 10 CFR Part 52 (Reference 1).

Enclosure 1 contains proprietary information of the type that GEH maintains in confidence and withholds from public disclosure. The information has been handled and classified as proprietary to GEH as indicated in the enclosed affidavit required by 10 CFR 2.390(b)(1) (Enclosure 5). GEH hereby requests that the information in Enclosure 1 be withheld from public disclosure in accordance with the provisions of 10 CFR 2.390 and 9.17. Enclosure 2 is the non-proprietary version of the presentation slides, which do not contain proprietary information and are suitable for public disclosure.

*D068*

*NRO*

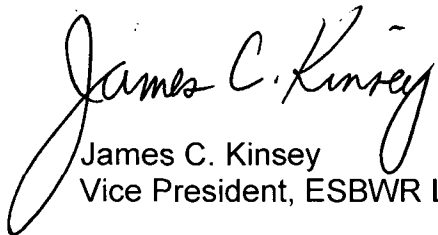
MFN 07-627

Page 2 of 3

Enclosure 3 contains non-Proprietary materials presented to NRC during the course of the DOORS Software Audit. Enclosure 4 contains additional information requested by NRC as a result of their reviews during the audit.

If you have any questions or require additional information, please contact me.

Sincerely,

  
James C. Kinsey  
Vice President, ESBWR Licensing

Reference:

1. MFN 05-084 - Letter from Steven A. Hucik, GE, to William D. Beckner, NRC, *General Electric Company Application for Final Design Approval and Design Certification of ESBWR Standard Plant Design*, dated August 24, 2005

Enclosures:

1. Presentation Materials Used During NRC Audit of DOORS Software (Proprietary version)
2. Presentation Materials Used During NRC Audit of DOORS Software (Non-Proprietary version)
3. Non-Proprietary Presentation Materials Used During NRC Audit of DOORS Software
4. Miscellaneous Supplemental Non- Proprietary Information Requested by NRC to Support NRC Audit of DOORS Software
5. Affidavit signed by David H. Hinds (GEH) dated January 21, 2008

cc: AE Cubbage            USNRC (with enclosures)  
RE Brown                GEH/Wilmington (with enclosures)  
GB Stramback            GEH/San Jose (with enclosures)

**Enclosure 2**

**MFN 07-627**

**Presentation Materials Used During NRC Audit of  
DOORS Software**

**(Non-Proprietary Version)**

The information in the documents in Enclosure 1 are essentially all marked proprietary. The non-proprietary versions would be cover sheets with blank pages. Based on this, no non-proprietary version will be supplied with this letter.

**Enclosure 3**

**MFN 07-627**

**Non- Proprietary Presentation Materials Used During  
NRC Audit of DOORS Software**

# DOORS Fundamentals



**HITACHI**

# What is “DOORS” anyway?

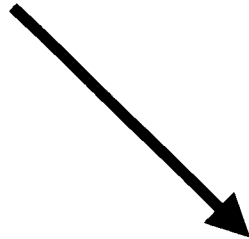
- DOORS is the world’s leading requirements management application that provides word processing and spreadsheet features combined within the same document.
- DOORS provides the ability to associate information between documents via links similar to hyperlinks as used in Word or on the WEB.
- DOORS provides revision history feature that allows you to track changes to information and to reconstruct or compare changes over time.
- DOORS provides a means to generate traceability reports and real time navigation for verification needs or for impact analysis.



**HITACHI**



# Starting and Logging In



guest1

guest2

guest3

A screenshot of a 'Login - DOORS' dialog box. It has a title bar with a close button (X). The dialog contains three input fields: 'Database:' with the value '36677@maspsa003.e', 'Username:' which is empty, and 'Password:' which is empty. At the bottom are 'OK' and 'Cancel' buttons.

Database: 36677@maspsa003.e

Username:

Password:

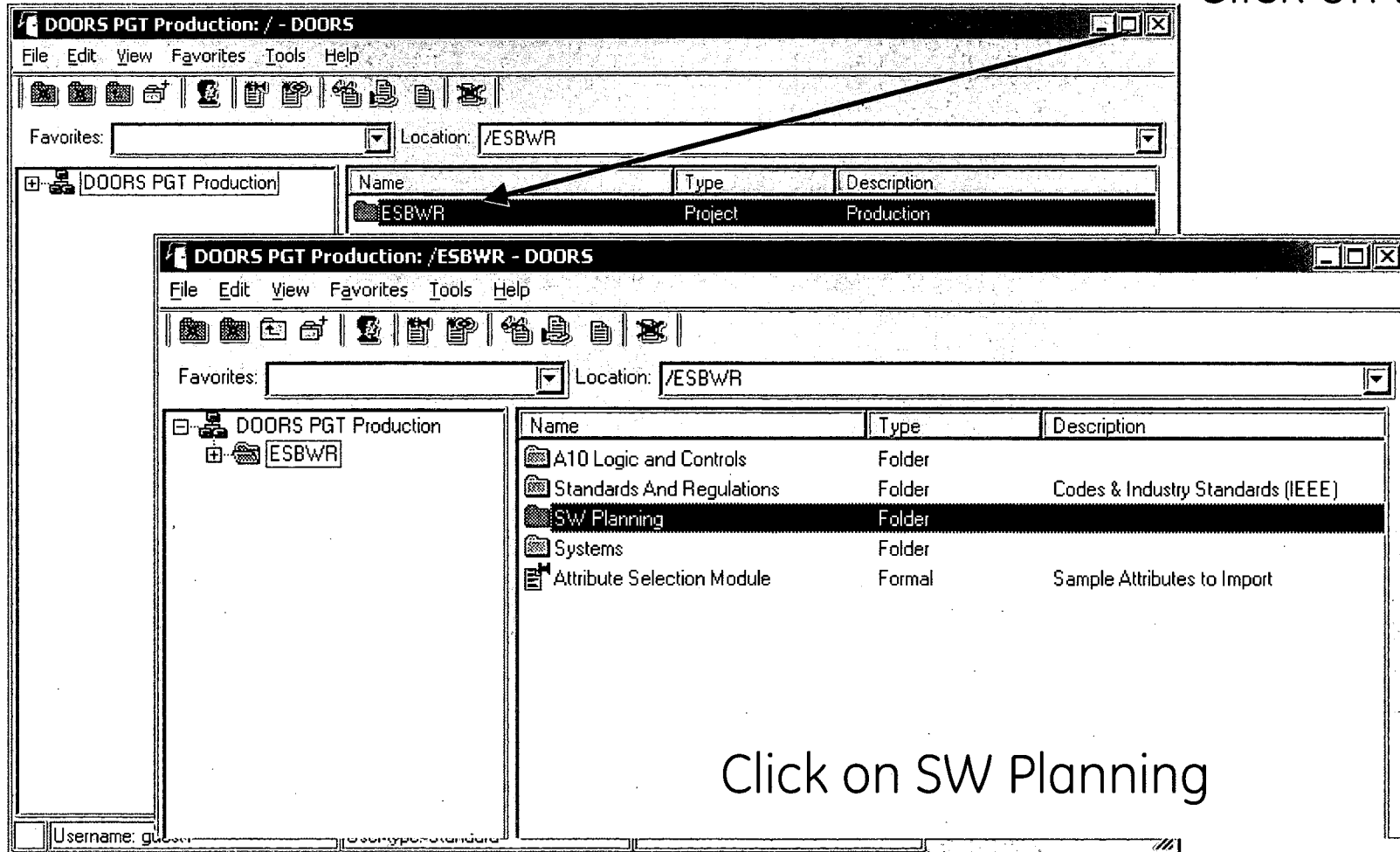
OK Cancel



HITACHI

# DOORS Explorer Window/Tree

Click on ESBWR



Icons help identify the type of object.



HITACHI



Folder



Project



Module

# SW Planning Folder

The screenshot shows the DOORS software interface. The main window is titled "DOORS PGT Production: /ESBWR/SW Planning - DOORS". The left pane shows a tree view of the project structure, with the "SW Planning" folder selected. The right pane displays a table of files:

| Name               | Type   | Description                             |
|--------------------|--------|---|
| SMP                | Formal | SOFTWARE MANAGEMENT PLAN (...)          |
| SQAP               | Formal | Software Quality Assurance Plan (SQ...) |
| Translation Matrix | Formal | Production                              |

Below the table, the text "When clicking on the above modules..." is displayed. An error dialog box titled "DOORS" is open, showing a warning icon and the message: "You have insufficient access rights to open this module for edit." The dialog box has two buttons: "Open Read Only" and "Cancel".

At the bottom of the window, the status bar shows "Username: guest1" and "User type: Standard".



HITACHI

# What You See When Opening a DOORS Document

The screenshot displays the DOORS software interface. The title bar reads "Formal module 'RPS Training/Standards And Regulations/IEEES/IEEE Std 1050 - 2004' current 0.0 - DOORS". The menu bar includes "File", "Edit", "View", "Insert", "Link", "Analysis", "Table", "Tools", "User", and "Help". A "Tool Bar" is located below the menu bar. The interface is divided into three main panes:

- Explorer Pane:** Located on the left, it shows a hierarchical tree structure of the document. The selected path is "4 Design considerations for electrical noise minimization". Other visible items include "IEEE Std 1050 - 2004", "IEEE Guide for Instrumentation and...", "IEEE Std 1050 - 2004 (Revision of IEEE Std 1050-1996)", "1 Overview", "2 Normative references", "3 Definitions and acronyms", "3.1 Definitions", "3.2 Acronyms", "5 I&C system grounding", "6 Signal cable shield grounding", and "7 Testing".
- Main Column:** The central pane displays a table of requirements. The table has two columns: "ID" and "Requirements".

| ID  | Requirements  |
|-----|---|
| 123 | <b>4 Design considerations for electrical noise minimization</b>  |
| 124 | <b>4.1 Typical noise sources and their characteristics</b>  |
| 125 | Noise sources can be divided into several categories:   |
| 126 | a) <i>Natural sources</i> - Those that happen independently of human activity; but their effects can be controlled.   |
| 128 | b) <i>Incidental sources</i> - Those caused by human activity; but they are not intentional.  |
| 130 | c) <i>Intentional sources</i> - These are emissions of potentially interfering energy produced for specific purposes unrelated to the equipment or systems under consideration.   |
| 132 | <b>4.1.1 Natural sources</b>  |
| 133 | Probably the most severe noise source to which any control system will be exposed is lightning. While most electronic control systems will probably fail under a direct lightning strike, even a remote power line strike can cause interference as the lightning-induced surge travels along power lines and is dissipated through leakage, radiation, and power loss in the distribution system. <span style="float: right;">▶ Yes</span>   |
| 134 | In addition to the currents created in the power system's conductors by a direct strike, lightning can also create similarly rapidly changing and high current flows through the earth and through numerous grounded metallic systems and items such as cable shields, equipment grounding conductors, building steel, metallic piping systems, conduits, raceways, and metallic equipment enclosures. <span style="float: right;">▶</span>   |
| 135 | Single-point grounding of the above metallic items does not prevent the indicated lightning current from flowing because of the distributed capacitance of the involved items, which completes the current path via stray reactive coupling. In addition, insulation of these items is not always a reliable protection for this problem since the large lightning induced voltages can often arc-over through six-feet of air. <span style="float: right;">▶</span>  |
| 136 | A typical lightning strike is composed of a downward-stepped leader stroke, usually negatively charged, a first upward positive return stroke, then two or more downward leader strokes, each followed by a positive return stroke. On average, subsequent strokes contain about 40% of the first stroke's amplitude. A continuing current is usually present between stroke sequences. There may be as many as twenty stroke sequences in a typical lightning flash. Characteristics of a typical lightning flash are as follows: <span style="float: right;">▶</span> |
- Applies:** A narrow pane on the right side of the Main Column, currently empty.

At the bottom of the window, the status bar shows "Username: 501503519" and "Exclusive edit mode".



HITACHI

# What You See When Opening a DOORS Document

The screenshot shows a DOORS software window titled "Formal module 'RPS Training/Standards And Regulations/IEEES/IEEE Std 1050 - 2004' current 0.0 - DOORS". The window displays a requirements document with the following content:

| ID  | Requirements   | Applies | Requirement Type | Safety Classification |
|-----|--|---------|------------------|-----------------------|
| 12  | <b>4 Design considerations for electrical noise minimization</b>   |         |                  |                       |
| 124 | <b>4.1 Typical noise sources and their characteristics</b>   |         |                  |                       |
| 125 | Noise sources can be divided into several categories:  |         |                  |                       |
| 126 | a) <i>Natural sources</i> - Those that happen independently of human activity; but their effects can be controlled.  |         |                  |                       |
| 128 | b) <i>Incidental sources</i> - Those caused by human activity; but they are not intentional.   |         |                  |                       |
| 130 | c) <i>Intentional sources</i> - These are emissions of potentially interfering energy produced for specific purposes unrelated to the equipment or systems under consideration.  |         |                  |                       |
| 132 | <b>4.1.1 Natural sources</b>   |         |                  |                       |
| 133 | Probably the most severe noise source to which any control system will be exposed is lightning. While most electronic control systems will probably fail under a direct lightning strike, even a remote power line strike can cause interference as the lightning-induced surge travels along power lines and is dissipated through leakage, radiation, and power loss in the distribution system.   | Yes     | Requirement      |                       |
| 134 | In addition to the currents created in the power system's conductors by a direct strike, lightning can also create similarly rapidly changing and high current flows through the earth and through numerous grounded metallic systems and items such as cable shields, equipment grounding conductors, building steel, metallic piping systems, conduits, raceways, and metallic equipment enclosures.   |         |                  |                       |
| 135 | Single-point grounding of the above metallic items does not prevent the indicated lightning current from flowing because of the distributed capacitance of the involved items, which completes the current path via stray reactive coupling. In addition, insulation of these items is not always a reliable protection for this problem since the large lightning induced voltages can often arc-over through six-feet of air.  |         |                  |                       |
| 136 | A typical lightning strike is composed of a downward-stepped leader stroke, usually negatively charged, a first upward positive return stroke, then two or more downward leader strokes, each followed by a positive return stroke. On average, subsequent strokes contain about 40% of the first stroke's amplitude. A continuing current is usually present between stroke sequences. There may be as many as twenty stroke sequences in a typical lightning flash. Characteristics of a typical lightning flash are as follows: |         |                  |                       |

Annotations on the left side of the screenshot:

- Section Number → points to the ID column.
- Each Row is an Object → points to the entire row structure.
- Each Object Has an ID → points to the ID column.
- Change Bar → points to the vertical bar on the left side of the document content.

Annotation on the right side of the screenshot:

- Link Indicator → points to the right-pointing triangle symbols in the Requirements column.

At the bottom of the window, the status bar shows "Username: 501503519" and "Exclusive edit mode".



HITACHI

# Document Navigation



imagination at work.

# Module Explorer

Explorer Toggle

Click on Explorer Section to Navigate

The screenshot displays a software application window titled "Formal module /ESBWR/Software Planning/Translation Matrix' current 0.0=DOORS". The interface includes a menu bar (File, Edit, View, Insert, Link, Analysis, Table, Tools, User, Help) and a toolbar with various icons. A "Standard view" dropdown and "All levels" filter are visible. On the left, a "Translation Matrix" tree lists items such as "1 IEEE Std 7.4.3.2 -Rev 2000" and "9 IEEE Std 1028 -Rev 1997". A text area below the tree lists roles: "a) Decision maker", "b) Review leader", "c) Recorder", "d) Management staff", "e) Technical staff".

The main window shows a table with columns "ID" and "Production". The selected entry is:

| ID       | Production  |
|----------|---|
| RTD-3119 | <b>12 RTM for IEEE Std 1074 - 1995</b>  |
| RTD-3820 | 12.1  |
| RTD-3828 | In 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," paragraph 55a(a) (1) requires, in part, that systems and components be designed, tested, and inspected to quality standards commensurate with the safety function to be performed. Criterion I, "Quality Standards and Records," of Appendix A, "General Design Criteria for Nuclear Power Plants," to 10 CFR Part 50 requires, in part, that a quality assurance program be established and implemented in order to provide adequate assurance that systems and components important to safety will satisfactorily perform their safety functions.   |
| RTD-3829 | Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," to 10 CFR Part 50 describes criteria that a quality assurance program for systems and components that prevent or mitigate the consequences of postulated accidents must meet.   |
| RTD-3907 | In particular, besides the systems and components that directly prevent or mitigate the consequences of postulated accidents, the criteria of Appendix B also apply to all activities affecting the safety-related functions of such systems and components as designing, purchasing, installing, testing, operating, maintaining, or modifying.  |
| RTD-3908 | A specific requirement is contained in 10 CFR 50.55a(h), which requires that reactor protection systems satisfy the criteria of IEEE Std 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations." Paragraph 4.3 of IEEE Std 279-1971 states that quality of components is to be achieved through the specification of requirements known to promote high quality, such as requirements for design, inspection, and testing.   |
| RTD-3909 | In Appendix B to 10 CFR Part 50, many of the criteria contain requirements closely related to software life cycle activities. Criterion I, "Organization," describes the establishment and execution of a quality assurance program. Criterion II, "Quality Assurance Program," states, in part, that activities affecting quality must be accomplished under suitably controlled conditions, which include assurance that all prerequisites for a given activity have been satisfied. This criterion also calls for taking into account the need for special controls and processes to attain the required quality. Criterion III, "Design Control," states, in part, that measures must be established for the identification and control of design interfaces and for coordination among participating design organizations. Criterion XV, "Nonconforming Materials, Parts, or Components," requires measures to be established to control materials, parts, or components that do not conform to requirements in order to prevent their inadvertent use or installation. Finally, Criteria VI, "Document Control," and XVII, "Quality Assurance Records," provide for the control of the issuance of documents, including changes thereto, that prescribe all activities affecting quality and provide for the maintenance of sufficient records to furnish evidence of activities affecting quality. |
| RTD-3830 | This regulatory guide endorses IEEE Std 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes, subject to the exceptions stated in the Regulatory Position. IEEE Std 1074-1995. <small>Herein a method acceptable to the NRC staff for complying with parts of the NRC's regulations</small>   |

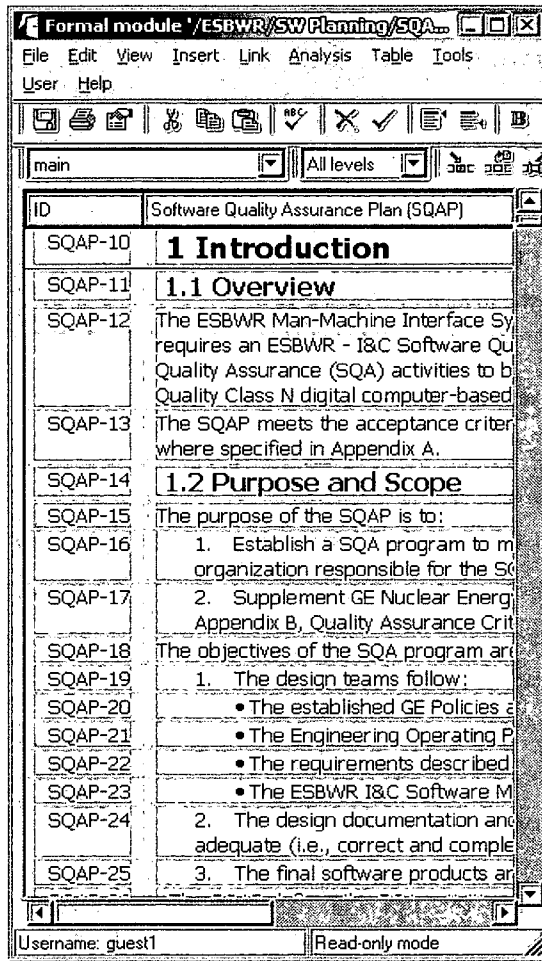
At the bottom of the window, the status bar shows "Username: 501431318" and "Shareable edit mode".



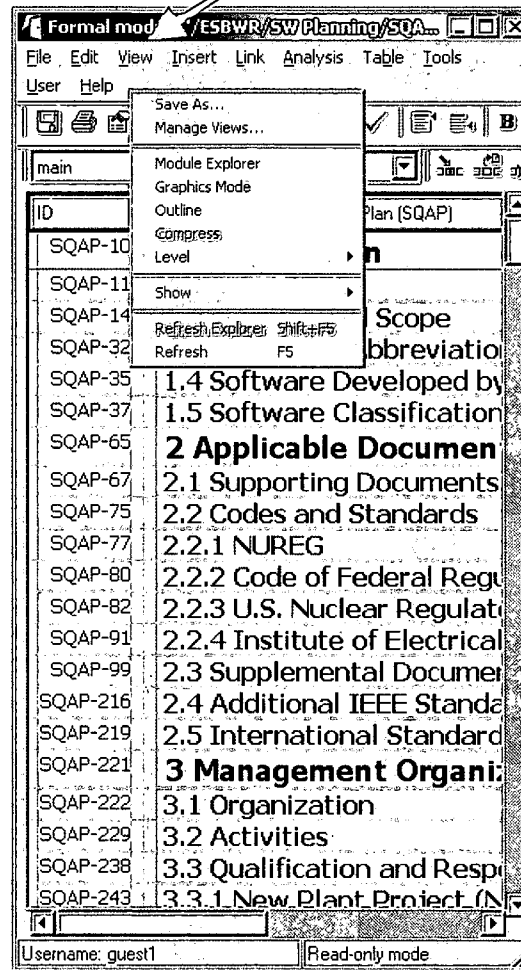
HITACHI

# Navigating a DOORS Module-Display Modes

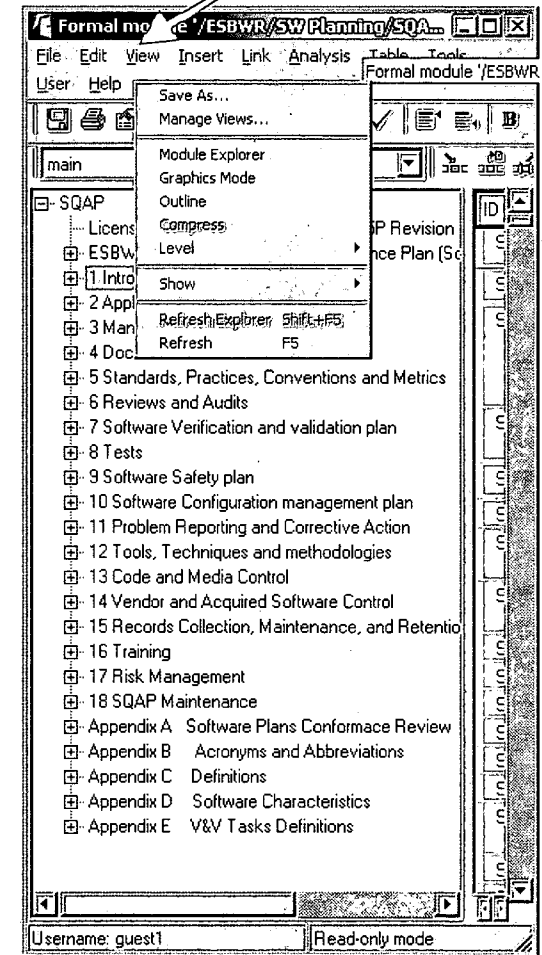
## Normal



## View - Outline



## View - Module Explorer



HITACHI



# Using Levels



Formal module '/JCwiklinski/IEEE 1074 1995' current 0.0 - DOORS

File Edit View Insert Link Analysis Table Tools User Help

main All levels

| ID   | Requirement  | Level    |
|------|--|----------|
| 4054 | IEEE Std 1   | Level 1  |
| 4055 | IEEE Stand   | Level 2  |
| 4056 | <b>1 Over</b>  | Level 3  |
| 4057 | <b>1.1 Sc</b>  | Level 4  |
| 4058 | This stand   | Level 5  |
|      | development and maintenance of software, whether stand-alone or part of a system.  | Level 6  |
|      | <b>This is a test comment.</b>   | Level 7  |
|      | <b>This is another test comment.</b>   | Level 8  |
| 5165 | (Non-software Activities, such as hardware development and purchasing, are outside of the scope of this standard.)   | Level 9  |
| 5166 | This standard also provides associated Input and Output Information.   | Level 10 |
| 4059 | For convenience, Activities are listed and described under specific Processes.   |          |
| 5167 | In practice, the Activities may be performed by persons whose organizational titles or job descriptions do not clearly convey that a Process is part of their job. |          |
| 5168 | The Process under which an Activity is listed in this standard may be transparent in practice.   |          |
| 4060 | This standard does not prescribe a specific software life cycle model (SLCM).  |          |
| 5169 | Each using organization must map the activities specified in the standard into its own software life cycle   |          |

Levels are very helpful in finding particular sections in very large documents. Select the level, then select a section. Select "All Levels" to see everything within the section.



HITACHI

# Searching and Sorting Modules

Searching and sorting are similar to the search found in Word and Excel and the sort found in Excel. These features allow you to look for specific information in a document or to look at information sorted by a value.



imagination at work

# Preferred Views of the Translation Matrix

Click on  
Drop Down  
Box to select  
your PV IEEE

The screenshot shows a software application window titled "Formal module /ESBWR/SW Planning/Translation Matrix" current 1.1 - DOORS. The window has a menu bar (File, Edit, View, Insert, Link, Analysis, Table, Tools, User, Help) and a toolbar. A dropdown menu is open on the left, showing "Standard view" selected. Below it are other options like "Out Links View", "PV 15 BTP14", "PV 7-4.3.2", "PV IEEE 1008", "PV IEEE 1012", "PV IEEE 1028", "PV IEEE 1042", "PV IEEE 1074", "PV IEEE 828", and "PV IEEE 829". The main area displays a table with two columns: "ID" and "Production". The table contains several rows of requirements, with the first row highlighted. An arrow points to the "Standard view" menu item.

| ID       | Production  |
|----------|---|
| RTD-109  | <b>5 IEEE Std 830 - 1993 - IEEE Recommended Practice for Software Requirements Specifications.</b>  |
| RTD-3995 | The (Software Safety) plan <b>should</b> include a requirement that a safety analysis be performed and documented on each of the principal design documents: requirements (being one of them).  |
| RTD-3998 | The (Software Safety) plan <b>should</b> require that appropriate safety requirements be included in the software requirements specification.   |
| RTD-4004 | Items to be controlled (by the Software Configuration Mgmt Process) <b>should</b> include: software requirements.   |
| RTD-4009 | Documentation <b>should</b> exist that shows that the safety analysis activities have been successfully accomplished for each life cycle activity group. In particular, the documentation <b>should</b> show that the system safety requirements have been adequately addressed for each activity group.  |
| RTD-4102 | (Documentation should show) that the software requirements that can affect safety <b>have been</b> identified; and that all other software requirements <b>will not</b> adversely affect safety.  |
| RTD-4011 | Documentation <b>should</b> exist that shows that the V&V tasks have been successfully accomplished for each life cycle activity group. In particular, the documentation <b>should</b> show that the requirements satisfy the appropriate software development functional and process characteristics (as described in Section B.3.3 of BTP 7-14).  |
| RTD-4015 | As part of the software V&V effort, a traceability matrix <b>should</b> be produced. This traceability matrix <b>should</b> clearly show the linkage between each requirement imposed on the software by the system requirements document and system design documents, and one or more requirements in the SRS. The final matrix <b>should</b> permit tracing from the system requirements and design through the software requirements, design, implementation, integration, validation, and installation. |

Username: guest1      Read-only mode



HITACHI

# Using Find Utility

Formal module: '/ESBWR/Software Planning/Translation Matrix' current 0.0 - DOORS

File Edit View Insert Link Analysis Table Tools User Help

Undo Ctrl+Z  
Cut Ctrl+X  
Copy  
Paste  
Paste Special...  
Clear  
Find... Ctrl+F  
Find Next F3  
Replace...  
Go To... Ctrl+G  
Columns...  
Attributes...  
Types...  
Object  
In-Place  
Purge All  
Section  
Edit Mode

Reference Location Requirement/Design Goal

3 IEEE Std 82 Signed Need 050907 (KM)

2 Software Configuration Management Plan

3.1 Software Configuration Management Plan

1) A document with the title "Software Configuration Management Plan" shall be embedded in another document.

2) This document shall contain information either by reference to other documents or by locations, such as other documents.

3) A format for this document shall be defined in Table 1 unless a different format is specified in the Introduction of the Plan.

The purpose shall be to provide a brief description of the intended audience and the scope shall address the assumptions. The following shall be included:

a) Overview description of the project.

b) Identification of the project.

IEEE 828

IEEE 828 2.1 Introduction

IEEE 828

IEEE 828

IEEE 828

IEEE 828

Find and Replace - DOORS

Find Replace Go To

Find what: SCM

Find Next

Find Previous

Match case

Use regular expression

Find in:

Attribute Name / Layout DXL

Last Modified By

Last Modified On

Object Heading

Object Identifier

Object Level

Object Number

Object Short Text

Object Text

RE Disposition

All in View

All

Advanced... Close Help

The 'Find' utility allows you to search specific attributes for key values.



HITACHI

# LINKS



imagination at work

# About Traceability

- DOORS lets you link together related information
- Links give you traceability
- Links can be followed in both directions
- Links allow us to manage change



**HITACHI**

# Navigating Links

To Trace the link.

*Right click and follow.....*

| Requirement/Design Goal   | Compliance  | Exception/Comment   |
|---|---|---|
| <b>7 IEEE Std 1012 - 1998 Software Verification and Validation</b>  |   |   |
| No "shall" requirements for S/W V&V   | B - Information Only                                    |   |
| No "shall" requirements for S/W V&V   | B - Information Only                                    |   |
| <b>Endorses IEEE 1012-1998 with exceptions:</b>   | B - Information Only                                    |   |
| a) Guidance for acceptance of pre-existing safety system software not verified during development to provisions of RG 1028 or equivalent, is <b>not endorsed</b> .  | A - Conforms - No Deviations                            | No Exceptions   |
| b) In addition to provisions of IEEE 1012, any V&V materials necessary for the verification of the effectiveness of V&V programs or necessary to furnish evidence of activities affecting quality <b>should</b> be maintained as quality assurance records.                 | A - Conforms - No Deviations<br>/ESBWR/SW Planning/SQAP | No Exceptions<br>1736: This SCMP establishes the SCM ...<br>1803: SCM Tools<br>1820: Configuration Identification |
| c) <b>Exception</b> is taken with regard to "optional" V&V tasks. Following are considered part of the minimum set of V&V activities for critical software: audits, regression analysis and testing, security assessment, test evaluation, and evaluation of documentation. | A - Conforms - No Deviations                            | No Exceptions   |
| No "shall" requirements for S/W V&V   | B - Information Only                                    |   |
| No "shall" requirements for S/W V&V   | B - Information Only                                    |   |

Links can be navigated using the link indicator. Select the Orange triangular Link Indicator using your RIGHT mouse button. A list of the links will appear. By navigating the list and moving to the right of each list entry you may use your RIGHT mouse button to open the document which is linked.



HITACHI

# Navigating Through

| Requirement/Design Goal   | Compliance                   | Exception/Comment |
|---|------------------------------|-------------------|
| <b>7 IEEE Std 1012 - 1998 Software Verification and Validation</b>  |                              |                   |
| No "shall" requirements for S/W V&V   | B - Information Only         |                   |
| No "shall" requirements for S/W V&V   | B - Information Only         |                   |
| <b>Endorses IEEE 1012-1998 with exceptions:</b>   | B - Information Only         |                   |
| a) Guidance for acceptance of pre-existing safety system software not verified during development to provisions of RG 1028 or equivalent, is <b>not endorsed.</b>   | A - Confirms - No Deviations | No Exceptions     |
| b) In addition to provisions of IEEE 1012, any V&V materials necessary for the verification of the effectiveness of V&V programs or necessary to furnish evidence of activities affecting quality <b>should</b> be maintained as quality assurance records. | A - Confirms - No Deviations | No Exceptions     |
| c) <b>Exception</b> is taken with regard to "optional" V&V tasks. Following are considered part of the minimum set of V&V activities for critical software:   | A - Confirms - No Deviations | No Exceptions     |

A - Confirms - No Deviations  
 /ESBWR/SW Planning/SQAP  
 1736: This SCMP establishes the SCM ...  
 1803: SCM Tools  
 1820: Configuration Identification

Formal module /ESBWR/SW Planning/SQAP current 1.1 - DOORS

File Edit View Insert Link Analysis Table Tools User Help

main All levels Underline

| ID        | Software Quality Assurance Plan (SQAP)   |
|-----------|--|
| SQAP-1735 | <b>10.1 Introduction</b>   |
| SQAP-1736 | This SCMP establishes the SCM activities for the design and development of the software products. This SCMP satisfies the requirements of RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants [2.2.3(2)], except where specified in Appendix A. RG 1.169 endorses IEEE Std. 828, IEEE Standard for SCM Plans [2.2.4(3)]. |
| SQAP-1737 | <b>10.1.1 Purpose</b>  |
| SQAP-1738 | The intent of this SCMP is to provide additional guidance and direction necessary to implement the SCM activities required during the software product design and development process. This SCMP supplements GEEN established configuration management procedures in system and hardware design. It establishes a formal set of standards and methodology used to                          |



HITACHI



# Decision Links

| ID       | Standard      | Reference Location | Requirement/Design Goal  | Compliance                   | Exception/Comment   |
|----------|---------------|--------------------|--|------------------------------|---|
| RTD-3119 | IEEE 1074     |                    | <b>12 IEEE Std 1074 - 1995 - Software Life Cycle Processes</b>   |                              |   |
| RTD-3820 | RG 1.173-1997 | A. Introduction    | 12.1   |                              |   |
| RTD-3830 | RG 1.173-1997 |                    | This regulatory guide endorses IEEE Std 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes, subject to the exceptions stated in the Regulatory Position. IEEE Std 1074-1995 describes a method acceptable to the NRC staff for complying with parts of the NRC's regulations for promoting high functional reliability and design quality in software used in safety systems". | A - Conforms - No Deviations | No Exceptions   |
| RTD-3906 | RG 1.173-1997 |                    | Decision Links: The following links were used as a basis for determining why this is a requirement.  | Z - Decision Link            | RG 1.173 Footnote 4 was also analyzed & included in determining this requirement. |
| RTD-3834 | RG 1.173-1997 | B. DISCUSSION      | 12.2   |                              |   |
| RTD-3831 | RG 1.173-1997 |                    | Therefore, the standard should be used in conjunction with guidance from other   | C - Conforms with Deviations | SQAP does not reference IEEE 1074 in Section                                      |

- In the RTM, there are two types of links in the Requirement/Design Goal Column (orange & red).
- The Decision Link is clearly identified by the drop down selection in the Compliance column.
- Additionally, the Exception/Comment field can also be used to further clarify an analyst's position (as shown).



HITACHI

# Decision Links

| Requirement/Design Goal  | Compliance                   | Exception/Comment  |
|--|------------------------------|--|
| <b>12 IEEE Std 1074 - 1995 - Software Life Cycle Processes</b>   |                              |  |
| <b>12.1</b><br>This regulatory guide <b>endorses</b> IEEE Std 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes, subject to the exceptions stated in the Regulatory Position. IEEE Std 1074-1995 <b>describes a method acceptable</b> to the NRC staff for complying with parts of the NRC's regulations for promoting high functional reliability and design quality in software used in safety systems <sup>4</sup> .<br><br>↳ <b>Decision Links:</b> The following links were used as a basis for determining why this is a requirement. | A - Conforms - No Deviations | No Exceptions  |
| <b>12.2</b><br>Therefore, the standard <b>should</b> be used in appropriate regulatory guides, standards, and IEEE Std 1074-1995 <b>can be used</b> as a basis for developing specific software life cycle processes that are consistent with regulatory requirements, as applied to software, for <b>controlling and coordinating the design of safety system software</b> .<br><br>↳ <b>Decision Links:</b> The following links were used as a basis for determining why this is a requirement.  | C - Conforms with Deviations | SQAP does not reference IEEE 1074 in Section 2.2.4.  |
| IEEE Std 1074-1995 <b>describes</b> a complete set of software life cycle processes; however, its system-level view is a generic view from a software perspective.<br>↳ <b>Decision Links:</b> The following links were used as a basis for determining why this is a requirement.   | Z - Decision Link            | Information Only   |
|  | C - Conforms with Deviations | SQAP does not reference IEEE 1074 in Section 2.2.4.  |
|  | Z - Decision Link            | SMP 2.2.4 statement preceding IEEE list (DOORS SMP ID# SMP-63) was analyzed and included in this requirement decision. |
| <b>12.3</b>  |                              |  |

Then, by right click (mouse) on the Decision Link outbound arrow, one can view all decision links associated with determination of this particular requirement.



HITACHI

# Decision Links Cont.

- What is the basis? Decision Links were devised to assist the RTM analysis effort in capturing the analyst's thoughts on a particular decision regarding a requirement. Such as:
  - Is a particular statement a requirement? The RTM Compliance column reflects this decision. Yes or No, the Decision Link object is used to clarify that position. (A "No" answer normally means exclusion from the RTM. But in certain cases, Information Only analyzed statements are included in the RTM, with Decision Links, for clarification)
  - Is not enough information available? Then, additional research is required with corresponding Decision Links. The RTM Compliance column also reflects this decision.
- Linking back to the Standard and/or Regulation, through the Decision Link, allows the RTM to remain simple, yet all information is just a mouse click away.
- Works efficiently with the DOORS Filtering or Report process. No difference than any other DOORS feature.
- Enhances the overall GEH ESBWR RTM analysis effort.



**HITACHI**

The End



HITACHI

**Enclosure 4**

**MFN 07-627**

**Miscellaneous Supplemental Non- Proprietary  
Information Requested by NRC to Support NRC Audit of  
DOORS Software**

| # | Affected Doc | Section     | Comment  | Recommended Resolution | Identifier | Date     | DOORs ID# |
|---|--------------|-------------|--|------------------------|------------|----------|-----------|
| 1 | SQAP         | General     | <p>Formatting of Headers 1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3 2.4, 2.5,... are Cap letter followed by small letters while all other headers are all capitalized.</p> <p><b>1.0 INTRODUCTION</b></p> <p><b>1.1 Overview</b></p> <p><b>2:2.2 CODE OF FEDERAL REGULATIONS (CFR)</b></p> <p><b>3.3.5.1 SPE MANAGER</b></p> |                        | JMH        | 7/7/2007 |           |
| 2 | SQAP         | Table 1.5-1 | Should include personal injury in accident discussion.   |                        | JMH        | 7/7/2007 |           |
| 3 | SQAP         | 2.3         | Supplemental document table should start on same page. (Formatting)  |                        | JMH        | 7/7/2007 |           |
| 4 | SQAP         | 2.3         | Supplemental document table – correct alignment for Nuclear Energy policies (Formatting)   |                        | JMH        | 7/7/2007 |           |
| 5 | SQAP         | 4.0         | Correct "This SMP [2.3(1)]" to "This SQAP [2.3(1)].<br>Incorrect document referenced.  |                        | JMH        | 7/7/2007 |           |

| # | Affected Doc | Section | Comment   | Recommended Resolution | Identifier | Date       | DOORS ID# |
|---|--------------|---------|---|------------------------|------------|------------|-----------|
| 6 | SQAP         | 7.1.2   | <p>The first sentence</p> <p>“This SVVP outlines the formal set of standards and procedures necessary to comprehensively verify and Software Class Q and Software Class N3 and N2 software products during all phases of the software life cycle. The software life cycle phases in the SVVP correspond with those defined in the SMP [2.3(1)].</p> <p>Should read:</p> <p>“This <u>SQAP</u> outlines the formal set of standards and procedures necessary to comprehensively verify and <u>validate Class Q, N3 and N2 software</u> products during all phases of the software life cycle. The software life cycle phases in the <u>SQAP</u> correspond with those defined in the SMP [2.3(1)].”</p> |                        | JMH        | 7/7/2007   |           |
| 7 | SQAP         | 7.4.7   | <p>Include summary to describe the basis for the selected Software Integrity Level (SIL).</p> <p>This a requirement of IEEE-1012 Section 4.1.5</p>  |                        | JMH        | 7/7/2007   |           |
| 8 | SQAP         | 1.2.1   | Needs to specifically state "...per 10CFR 50 Appendix A" just like 1.2.2 does for 10CFR50 Appendix B.   |                        | JCC        | 08/01/2007 |           |
| 9 | SQAP         | 2.2.4   | <p>SQAP that I am working with in DOORS is missing references to some IEEE standards, including 1074. These would be listed in Section 2.2.4 (Institute of Electrical and Electronic Engineers (IEEE) Standards). When compared to the SMP Section 2.2.4, it appears that 1074, 7-4.3.2-2003, 1008-1987, and 830-1993 are not included in the SQAP. Currently I link to the Section SQAP header, rather than specific verbiage.</p>   |                        | JCC        | 08/01/2007 |           |

| #  | Affected Doc | Section | Comment  | Recommended Resolution   | Identifier | Date       | DOORS ID# |
|----|--------------|---------|--|--|------------|------------|-----------|
| 10 | SQAP         | 2.4     | DOORS SQAP Section 2.4 (Additional IEEE Guidance), the SQAP lists 1228-1994, only, whereas the SMP Section 2.4 lists an additional 6 IEEE Standards.   |  | JCC        | 08/01/2007 |           |
| 11 | SQAP         | 1.5     | The decision tree for software classification should include a decision block that asks "Is the software going to reside on a Safety related platform?" if so, then the Software Classification shall be Safety Related. |  | JMH        | 9-19-2007  |           |
| 12 | SQAP         | 1.5     | The last paragraph in this section is lost on a page after the Software Classification Decision Tree. It can easily be overlooked.   | Move paragraph to before decision tree.  | JMH        | 9/19/2007  |           |
| 13 | SQAP         | 7.3.4.7 | V&V Output sub paragraph should be labeled "a." for consistency.   |  | JMH        | 9/19/2007  |           |
| 14 | SQAP         | 7.3.7.4 | Sub paragraph 3. V&V Outputs: Sub paragraph "a." and "c." should be labeled "a" and "b".   |  | JMH        | 9/19/2007  |           |
| 15 | SQAP         | 7.3.7.6 | Sub paragraph 2. V&V Tasks sub paragraph "e." should be labeled "d".   |  | JMH        | 9/19/2007  |           |
| 16 | SQAP         | 8.0     | Section "8.0 Tests" has two sub paragraphs 1, 2, 3, and 4.   |  | JMH        | 9/19/2007  |           |
| 17 | SQAP         | 8.0     | Section "8.0 Tests" second sub paragraph 2 has two sub paragraph "ii." One for "Interface" and one for "Regression test".  |  | JMH        | 9/19/2007  |           |
| 18 | SQAP         | 9.3.1.1 | 9.3.1.1 sub paragraph "bb." and "cc." Should be sub paragraph "b." and "c."  |  | JMH        | 9/19/2007  |           |
| 19 | SQAP         | 9.3.3.1 | 9.3.3.1 sub paragraph "3 SSA Output" sub paragraph should be labeled "a." for consistency.   |  | JMH        | 9/19/2007  |           |
| 20 | SQAP         | 9.3.3.2 | 9.3.3.2 sub paragraph "3 SSA Output" sub paragraph should be labeled "a." for consistency.   |  | JMH        | 9/19/2007  |           |
| 21 | SQAP         | 14.0    | Section 14.1 Vendor Control has three sub sections labeled 1 and 2.  |  | JMH        | 9/19/2007  |           |
| 22 | SQAP         | Table 2 | Formatting is inconsistent across pages. Headers are in the middle of the page rather than the top in many cases.  |  | JMH        | 9/19/2007  |           |
| 23 | SQAP         | Table 2 | The heading "Test" only includes software classification "Q". The "Installation" heading has "N2, N2, Q, N3, and N2"   | Move related information from Part of "Installation N2 & N3" under the "Test" heading. | JMH        | 9/19/2007  |           |



| #  | Affected Doc | Section           | Comment  | Recommended Resolution  | Identifier | Date      | DOORs ID#  |
|----|--------------|-------------------|--|---|------------|-----------|--|
| 24 | SQAP         | Table of Contents | "Section 7.0 Software Validation and verification."<br>The word verification needs to be capitalized.  |   | JMH        | 9/19/2007 |  |
| 25 | SQAP         | Table of Contents | Some headings are all capitol letters while others are not.  | Correct for consistency.  | JMH        | 9/19/2007 |  |
| 26 | SQAP         | 1.5               | Software classification does not discuss risk due to personal injury.  |   | JMH        | 9/19/2007 |  |
| 27 | SQAP         | 6.2               | Section 6.2 "Managerial Review" does not have correct numbering. Number 6.2 is missing.  |   | JMH        | 9/19/2007 |  |
| 28 | SQAP         | 7.1.2             | The wording for the first sentence needs to be corrected.<br><br>"The SVVP outlines the formal set of standards and procedures necessary..." should read – "The SQAP SVVP outlines the formal set of standards and processes necessary..."             |   | JMH        | 9/19/2007 |  |
| 29 | SQAP         | 7.3.1             | The third paragraph is very wordy and needs to be edited.  |   | JMH        | 9/19/2007 |  |
| 30 | SQAP         | 7.3.2             | There are two sub paragraphs numbered 2. "V&V Tasks" and "Verify that the SDS...."   | Eliminate second number "2" heading and put this verbiage under "2. V&V Tasks".   | JMH        | 9/19/2007 |  |
| 31 | SQAP         |                   | Does not comply with IEEE-1012 Section 5.2.1, Acquisition support V&V. Includes Sections 5.2.1.1, 5.2.1.2, 5.2.1.3   |   | JMH        | 10-10-07  | RTD 2913 - 2916  |
| 32 | SQAP         | Appendix C        | The definition of the word interface needs to include all four variations as defined in IEEE 610 and as requested by RG 1.172 and MPR review. The definition should be modified to include the additional NRC interpretation found in Reg Guide 1.172. | See requirement in translation matrix.  | ST         | 10/24     | RTD-115  |
| 33 | SQAP         | Appendix A        | Since we classify requirements as safety or non-safety, we meet the requirement that "requirements be ranked by importance". IEEE comments on stability and necessity are suggestions and not requirements.  | Remove exception noted in Appendix A of the SMP for IEEE 830-1993.  | ST         | 10/26     | RTD-129<br>RTD-169<br>RTD-171                              |
| 34 | SQAP         | Various           | Nowhere in the document is the requirement to verify the SRS for modifiability and style.  | Each time the SQAP talks about verifying consistency with the SRS, it should also mention to verify modifiability and style. The links in the translation matrix for consistency will help you. | ST         | 10/28     | RTD-4041<br>RTD-4042<br>RTD-133<br>RTD-173<br>thru RTD-176 |

| #  | Affected Doc | Section              | Comment  | Recommended Resolution  | Identifier | Date    | DOORS ID#                                |
|----|--------------|----------------------|--|---|------------|---------|--|
| 35 | SQAP         | 7 – IV&V Plan        | The contents of section 5.4.7 of the SMP, Deferred Verification, is not discussed in the SQAP IV&V Plan  | Discuss what must be done during IV&V for incomplete requirements. Also discuss what information must be included until the TBD condition is resolved.                                | ST         | 10/29   | RTD-137<br>RTD-164<br>RTD-165<br>RTD-166 |
| 36 | SQAP         | 7 – IV&V Plan        | When the plan discusses checking for completeness, it does not mention how to handle requirements labeled TBD, To Be Determined.   | Any SRS that uses the phrase "to be determined" (TBD) is not a complete SRS.  | ST         | 10/29   | RTD-164                                  |
| 37 | SQAP         | 7.3.7.6              | The statement that you will validate safety requirements during the Installation Configuration Audit seems out of place. It should not be there.   | The statement needs to be removed or rewritten so that it concerns itself with installation configuration activities only.  | ST         | 11/1    | RTD-1084                                 |
| 38 | SQAP         | Various              | SMP and SQAP talk about cyber security but they do not classify the security threats according to impact on safety and likelihood of occurrence..  | Add the requirement that identified security threats need to be classified according to their impact on safety and likelihood of occurrence. Use DOORS links to find needed sections. | ST         | 11/1    | RTD-141<br>RTD-4029                      |
| 39 |              | General              | There are spelling errors throughout the RTM.  |   | JMH        | 11/2/07 |  |
| 40 |              | General              | Many of the IEEE 1012 requirements have been identified as being "below commitment level to the NRC. The CTS will be written to be ensure the ESBWR Work Instructions adequately evaluate this detail."<br><br>It is unclear if the issues have been identified in the Commitment Tracking System (CTS). |   | JMH        | 11/2/07 |  |
| 41 |              | RG 1.152             | RTM does not clearly state the traceability to RG 1.152 or the NRC's endorsement of IEEE Std 7-4.3.2-2003 for software quality, Security, or the software life cycle.  |   | JMH        | 11/2/07 |  |
| 42 |              | RG 1.168             | RTM does not clearly state that the NRC's endorsement of IEEE 1012 is for Safety Related software only and thereby being traceable to 10CFR50 Appendix B.  |   | JMH        | 11/2/07 |  |
| 43 |              | RTM / RG1.152 Item 4 | The SW classification process does not take residence of software fully in to account.   | Modify process and figure to ensure that NSR software that resides on SR computers is re-classified as SR per requirement.  | JMH        | 11/2/07 |  |

| #  | Affected Doc | Section                            | Comment   | Recommended Resolution | Identifier | Date    | DOORS ID# |
|----|--------------|------------------------------------|---|------------------------|------------|---------|-----------|
| 44 |              | RG 1.168<br>C. Regulatory Position | RTM states:<br>“Endorses IEEE 1012-1998 with exceptions:”<br>However, all of the NRC’s exceptions are not listed in the RTM.<br><br>Note: These exceptions only apply to Safety Related software and tools used to develop that software.<br><br>i.e. RG 1.168 Critical Software – “Software used in nuclear power plant safety systems should be assigned integrity level 4 or equivalent, as demonstrated by a mapping between the applicants or licensee approach and integrity level 4 as defined in IEEE Std 1012-1998.” |                        | JMH        | 11/2/07 |           |
| 45 |              | General                            | The RTM does not clearly map requirements from IEE Std 1012 using page and paragraph number. This makes it difficult to locate the delineated requirement to the source document.   |                        | JMH        | 11/2/07 |           |
| 46 |              | RTM Item 14                        | Software Integrity Levels (IEEE-1012 4.1.5 pg 9).<br>“The basis for assigning software integrity levels to software components shall be documented in a V&V Task report and V&V Final Report.”<br>Requirement not addressed.  |                        | JMH        | 11/2/07 |           |
| 47 |              | RTM Item 31                        | Acquisition Support V&V (IEEE-1012 5.2.1 pg 11)<br>“The V&V effort shall perform, as appropriate for the selected software integrity level, the minimum V&V tasks for Acquisition Support V&V from the following list:”<br>No Acquisition support requirements addressed see No.’s 10, 11, and 12 below.  |                        | JMH        | 11/2/07 |           |
| 48 |              | RTM Item 32                        | Acquisition Support V&V (IEEE-1012 5.2.1.1 pg 11)<br>“a) Scoping the V&V Effort”<br>Requirement not addressed.  |                        | JMH        | 11/2/07 |           |
| 49 |              | RTM Item 33                        | Acquisition Support V&V (IEEE-1012 5.2.1.2 pg 11)<br>“ b) Planning the interface between the V&V Effort and Supplier”<br>Requirement not addressed.   |                        | JMH        | 11/2/07 |           |

| #  | Affected Doc | Section      | Comment  | Recommended Resolution | Identifier | Date    | DOORS ID# |
|----|--------------|--------------|--|------------------------|------------|---------|-----------|
| 50 |              | RTM Item 34  | Acquisition Support V&V (IEEE-1012 5.2.1.3 pg 11)<br>“c) System Requirements Review.”<br>Requirement not addressed.  |                        | JMH        | 11/2/07 |           |
| 51 |              | RTM Item 50  | Requirements V&V (IEEE-1012 5.4.2.5 pg 12)<br>“e) System V&V Test Plan Generation and Verification.”<br>Requirement not addressed.   |                        | JMH        | 11/2/07 |           |
| 52 |              | RTM Item 51  | Requirements V&V (IEEE-1012 5.4.2.6 pg 12)<br>“f) Acceptance V&V Test Plan Generation and Verification”<br>Requirement not addressed.  |                        | JMH        | 11/2/07 |           |
| 53 |              | RTM Item 62  | Design V&V (IEEE-1012 5.4.3.7 pg 12)<br>“h) V&V Test Design Generation and Verification”<br>Requirement not addressed.   |                        | JMH        | 11/2/07 |           |
| 54 |              | RTM Item 71  | Implementation V&V (IEEE-1012 5.4.4.6 pg 13)<br>“V&V Test Procedure Generation and Verification”<br>Requirement not addressed.   |                        | JMH        | 11/2/07 |           |
| 55 |              | RTM Item 72  | Implementation V&V (IEEE-1012 5.4.4.7 pg 13)<br>“Component V&V Test Execution and Verification”<br>Requirement not addressed.  |                        | JMH        | 11/2/07 |           |
| 56 |              | RTM Item 96  | Operation V&V (IEEE-1012 5.5.1.3 pg 15)<br>“Operating Procedures Evaluation”<br>Requirement not addressed.   |                        | JMH        | 11/2/07 |           |
| 57 |              | RTM Item 99  | Process: Maintenance (IEEE-1012 5.6 pg 15)<br>“Modifications of the software shall be treated as development processes and shall be verified and validated as described in 5.1(Management Process) and 5.4(Development Process) of this standard.”<br>Requirement not addressed. |                        | JMH        | 11/2/07 |           |
| 58 |              | RTM Item 101 | Process: Maintenance (IEEE-1012 5.6 pg 15)<br>“The software integrity level assignments shall be revised as appropriate to reflect the requirements of the maintenance process.”<br>Requirement not addressed.   |                        | JMH        | 11/2/07 |           |

| #  | Affected Doc | Section         | Comment  | Recommended Resolution | Identifier | Date    | DOORS ID# |
|----|--------------|-----------------|--|------------------------|------------|---------|-----------|
| 59 |              | RTM<br>Item 102 | Maintenance V&V (IEEE-1012 5.6.1 pg 15)<br>“For migrating software, the V&V effort shall verify that the migrated software meets the requirements of 5.4(Development process) through 5.5(Operation process).”<br>Requirement not addressed.   |                        | JMH        | 11/2/07 |           |
| 60 |              | RTM<br>Item 103 | Maintenance V&V (IEEE-1012 5.6.1 pg 15)<br>“If the software was verified under this standard, the standard shall continue to be followed in the maintenance process.”<br>Requirement not addressed.  |                        | JMH        | 11/2/07 |           |
| 61 |              | RTM<br>Item 104 | Maintenance V&V (IEEE-1012 5.6.1 pg 15)<br>“If the software was not verified under this standard and appropriate documentation is not available or adequate, the V&V effort shall determine whether the missing or incomplete documentation should be generated.”<br>Requirement not addressed.                                      |                        | JMH        | 11/2/07 |           |
| 62 |              | RTM<br>Item 117 | V&V Reporting (IEEE-1012 6.1 pg 16)<br>“The V&V reports shall consist of required V&V reports (i.e., V&V Task Reports, V&V Activity Summary Reports, V&V Anomaly Reports, and V&V Final Report.)”<br>Does not address V&V Task Reports or Activity Summary Reports.  |                        | JMH        | 11/2/07 |           |
| 63 |              | RTM<br>Item 136 | SVVP Definitions (IEEE-1012 7.2 pg 18)<br>“The SVVP shall define or reference all terms used in the SVVP, including the criteria for classifying an anomaly as a critical anomaly.”<br><br>Does not contain requirement for referenced terms in the SVVP. Should probably reference an EOP for document development. In Section 7.2. |                        | JMH        | 11/2/07 |           |
| 64 |              | RTM<br>Item 137 | SVVP Definitions (IEEE-1012 7.2 pg 18)<br>“All abbreviations and notations used in the SVVP shall be described.”<br>Does not contain requirement for abbreviations and notations in the SVVP. Should probably reference an EOP for document development in Section 7.2.  |                        | JMH        | 11/2/07 |           |

| #  | Affected Doc | Section      | Comment   | Recommended Resolution | Identifier | Date    | DOORS ID# |
|----|--------------|--------------|---|------------------------|------------|---------|-----------|
| 65 |              | RTM Item 148 | Software Integrity Level Scheme (IEEE 1012 7.4.3 pg 18)<br>“SVVP shall document the assignment of software integrity levels to individual components where there are differing software integrity levels assigned within the program.”<br>Requirement not addressed.  |                        | JMH        | 11/2/07 |           |
| 66 |              | RTM Item 149 | Software Integrity Level Scheme (IEEE 1012 7.4.3 pg 18)<br>“For each SVVP update, the assignment of software integrity levels shall be reassessed to reflect changes that may occur in the integrity levels as a result of architecture selection, detailed design choices, code construction usage, or other development activities.”<br>Although sections 7.3.1, 7.3.1.1 refer to SVVP generation and update, reassessment of software integrity levels in not addressed. |                        | JMH        | 11/2/07 |           |
| 67 |              | RTM Item 150 | Resource Summary (IEEE 1012 7.4.4 pg 19)<br>“SVVP shall summarize the V&V resources, including staffing, facilities, tools, finances, and special procedural requirements.”<br><br>SQAP 7.2.4 summarizes and refers to resources for IVVT and BRT. However, there is no similar reference for the Design Team. Also facilities, finances and special procedural requirements are not addressed.   |                        | JMH        | 11/2/07 |           |
| 68 |              | RTM Item 151 | Responsibilities (IEEE 1012 7.4.5 pg 19)<br>“SVVP shall identify an overview of the organizational element(s) and responsibilities for V&V tasks.”<br>References to IVVT and SQA Manager are not correct. There is no similar reference to DT. What is meant by "The project letter" is not clear.  |                        | JMH        | 11/2/07 |           |
| 69 |              | RTM Item 154 | Tools, techniques, and methods (IEEE 1012 7.4.6 pg 19)<br>“Tools that insert code into the software shall be verified and validated to the same rigor as the highest software integrity level of the software.”<br>Requirement not addressed.   |                        | JMH        | 11/2/07 |           |

| #  | Affected Doc | Section      | Comment   | Recommended Resolution | Identifier | Date    | DOORS ID# |
|----|--------------|--------------|---|------------------------|------------|---------|-----------|
| 70 |              | RTM Item 155 | Tools, techniques, and methods (IEEE 1012 7.4.6 pg 19)<br>“Tools that do not insert code shall be verified and validated to assure that they meet their operational requirements.”<br>Requirement not addressed.  |                        | JMH        | 11/2/07 |           |
| 71 |              | RTM Item 156 | Tools, techniques, and methods (IEEE 1012 7.4.6 pg 19)<br>“If partitioning of tool functions can be demonstrated, only those functions that are used in the V&V processes shall be verified to demonstrate that they perform correctly for their intended use.”<br>Requirement not addressed.   |                        | JMH        | 11/2/07 |           |
| 72 |              | RTM Item 159 | Software Life Cycle (IEEE 1012 7.5.1 pg 19)<br>“SVVP shall include sections 5.1 through 5.6 for V&V activities and tasks as shown in SVVP Outline (boxed text).”<br>Not all IEEE processes are mapped directly. Operations and maintenance have been combined in SQAP section 7.3.8. Some are missing including acquisition.  |                        | JMH        | 11/2/07 |           |
| 73 |              | RTM Item 162 | Software Life Cycle (IEEE 1012 7.5.1 pg 19)<br>“The SVVP shall describe the methods and procedures for each task, including on-line access, and conditions for observation/evaluation of development processes.”<br>Online access is not described except through the use of EOPs that require use of ematrix; the methods are deferred to other reports or standards, but are not discussed in the SQAP document on a task by task basis. Observation of the development process is not addressed in the SQAP. |                        | JMH        | 11/2/07 |           |
| 74 |              | RTM Item 163 | Software Life Cycle (IEEE 1012 7.5.1.2 pg 20)<br>“SVVP shall define the criteria for evaluating the task results.”<br>Not specifically defined. May be done in the test plans but should be mentioned in SQAP.  |                        | JMH        | 11/2/07 |           |
| 75 |              | RTM Item 169 | Software Life Cycle (IEEE 1012 7.5.1.5 pg 21)<br>“SVVP shall describe the schedule for the V&V task.”<br>Requirement not addressed.   |                        | JMH        | 11/2/07 |           |

| #  | Affected Doc | Section   | Comment   | Recommended Resolution | Identifier | Date    | DOORs ID# |
|----|--------------|---|---|------------------------|------------|---------|-----------|
| 76 |              | RTM Item 170                                    | Software Life Cycle (IEEE 1012 7.5.1.5 pg 21)<br>“SVVP shall establish specific milestones for initiating and completing each task, for the receipt and criteria of each input, and for the delivery of each output.”<br>Requirement not addressed. |                        | JMH        | 11/2/07 |           |
| 77 |              | RTM Item 172                                    | Software Life Cycle (IEEE 1012 7.5.1.6 pg 21)<br>“SVVP shall specify resources by category. (e.g., staffing, equipment, facilities, travel, and training.)”<br>Requirement not fully addressed.   |                        | JMH        | 11/2/07 |           |
| 78 |              | RTM Item 174                                    | Software Life Cycle (IEEE 1012 7.5.1.7 pg 21)<br>“SVVP shall provide recommendations to eliminate, reduce, or mitigate risks.”<br>Process for mitigating risk not addressed.  |                        | JMH        | 11/2/07 |           |
| 79 |              | General   | The abbreviations “SMP” and “SCMP” are used interchangeably throughout NEDE-33226 & NEDE-33245 to refer to NEDE-33226. All uses of “SCMP” to refer to NEDE-33226 should be changed to “SMP”.  |                        | JMH        | 11/2/07 |           |
| 80 |              | NEDE-33245 section 7.3.4.2.2                    | Letters in subsection are out of sequence and need to be corrected / re-ordered in sequence.  |                        | JMH        | 11/2/07 |           |
| 81 |              | NEDE-33245 sections 7.3.4.8.1.e and 7.3.5.2.1.d | The term “Software Coding and Conventions Guideline Document” is missing the word “Coding”. This term should be made consistent with its use in corollary procedure NEDE-33226.   |                        | JMH        | 11/2/07 |           |
| 82 |              | NEDE-33245 section 3.3.1 and 3.3.3              | SQAP sections 3.3.1 and 3.3.3 both refer to responsibilities of the NPP Quality manager. While they say different things, the specified duties overlap. These two sections should be edited and merged into one section.                            |                        | JMH        | 11/2/07 |           |



| #  | Affected Doc | Section  | Comment   | Recommended Resolution | Identifier | Date    | DOORS ID# |
|----|--------------|--|---|------------------------|------------|---------|-----------|
| 83 |              | NEDE-33245 sections 7.3.1 thru 7.3.8                       | These sections are very wordy in describing V&V lifecycle activities. An enhancement may be in order. See example tables to replace these sections. These tables are located in a WORD file call < Life Cycle V&V Activities.doc > at < M:\ESBWR_Gen_Desc\ESBWR Requirements Traceability Matrix Project for IEEE to SMP and SQAP\Comments\Revision 3 >.  |                        | JMH        | 11/2/07 |           |
| 84 |              | NEDE-33245 section 8.0 step 2 subsections b.i through b.vi | Subsections b.i through b.vi should be subsections b.i through b.vii. The number “ii” is repeated twice for two different things: interface test and regression test.   |                        | JMH        | 11/2/07 |           |
| 85 |              | NEDE-33245 section 8.4                                     | <p>The last sentence in section 8.4 of NEDE-33245 says:</p> <p><u>Test documentation requirements described in Section 8.2 shall be used in preparing SAT test documents</u></p> <p><u>This should say:</u></p> <p><u>Test documentation requirements described in Section 8.5 shall be used in preparing SAT test documents</u></p> <p>Section 8.2 is on the SFAT, not SAT test documentation.</p> |                        | JMH        | 11/2/07 |           |

| #  | Affected Doc | Section                     | Comment  | Recommended Resolution   | Identifier | Date     | DOORS ID# |
|----|--------------|-----------------------------|--|--|------------|----------|-----------|
| 86 |              | NEDE-33245<br>Section 8.1   | <p>Section 8.1 in NEDE-33245 SQAP says in part:<br/><u>The IVVT is responsible for the preparation of the Validation Test Plan, Test Procedure, and Test Cases Specification</u></p> <p>This section makes no differentiation with regard to software class.</p> <p>Shouldn't the Design Team be responsible for these with regard to class N3 &amp; N2 software? Why have the IVVT do N3 preps of an SVT plan? It's a waste of resources.</p> |  | JMH        | 11/2/07  |           |
| 87 |              | NEDE-33245<br>Section 8.5.1 | <p>The test plan shall be independently verified as defined in Section 7.0, SVVP and placed under the CM control as described in Section 10.0, SCMP.</p> <p>Shouldn't this be just for Class Q software?</p>   |  | JMH        | 11/2/07  |           |
| 88 | SQAP         | 7.5.3                       | <p><b>Training feedback:</b> if deviation is allowed from the SQAP, shouldn't it be revised? Also, I see that that NUREG-0800 disallowed any deviation.</p>  |  | Greg Droba | 11/26/07 |           |
| 89 | SQAP         | 7.4.5                       | <p><b>Training feedback:</b> I believe duplication of the same document in two different DRFs is a violation of the EOPs. If one is updated, the other may not be.</p>   |  | Greg Droba | 11/26/07 |           |
| 90 | SQAP         | 9.3.1.1                     | <p><b>Training feedback:</b> Items 1(b) and 1(c) have typos.</p>   |  | Greg Droba | 11/26/07 |           |
| 91 | SQAP         | Appendix Table 1            | <p><b>Training feedback:</b> For each test activity / task, test results should be the output of test execution; then the test reporting should be a separate task where test results are an input.</p>  |  | Greg Droba | 11/26/07 |           |
| 92 | SQAP         | 11.2                        | <p><b>Training feedback:</b> Last paragraph, CQA should be CAQ.</p>  |  | Greg Droba | 11/26/07 |           |
| 93 | SQAP         | 7.3.3                       | <p>Why isn't the system requirement specification listed as one of the documents that must be V&amp;V during the requirement phase.</p>  | <p>Verified that every document listed in the SMP is V&amp;V at the proper time.</p> | ST         | 11/3     |           |

| #  | Affected Doc | Section    | Comment  | Recommended Resolution  | Identifier | Date | DOORs ID#  |
|----|--------------|------------|--|---|------------|------|--|
| 94 | SQAP         | 6.4.1      | The functional audit recommends that the audit be performed for class N3 and N2 systems. Good software development demands that the audit be performed on all software regardless of class. The BRT need not do this but somebody should. Since N3 impacts safety, should this at least be mandated.   |   | ST         | 11/3 |  |
| 95 | SQAP         | Appendix A | For RG 1.170 and IEEE 829, add the following exception. Two entries in the table needs to be updated.  | The sequence order of sections for each document found in IEEE 829 will not be followed. The justification for this is: Modern Tools and Techniques do not always allow themselves to follow the outline found in IEEE 829. When that is the case, the required information will be captured and displayed in a readable and understandable manor that is best for the tool/technique and the reader/users. | ST         | 11/5 |  |
| 96 | SQAP         | Various    | When the test documentation layout is discussed, add the following statement to that paragraph. See the RTD ID# for list of locations  | RG 1.170 and IEEE 829 shall be followed ... as amended by the exception in Appendix A ... Modern Tools and Techniques do not always allow themselves to follow the outline found in IEEE 829. When that is the case, the required information will be captured and displayed in a readable and understandable manor that is best for the tool/technique and the reader/users.                               | ST         | 11/5 | SQAP-1405<br>SQAP-1438<br>SQAP-1464<br>SQAP-1480<br><br>RTD-618<br>RTD-625<br>RTD-634<br>RTD-640<br>RTD-647<br>RTD-652<br>RTD-658<br>RTD-668 |
| 97 | SQAP         | Various    | We need an implementing procedure for test documentation.  | Write an implementing procedure to cover the parts of RG 1.170 and IEEE 829 not covered in the SMP and SQAP. Update SMP and SQAP to reference the implementing procedure.   | ST         | 11/5 |  |
| 98 | SQAP         | 1.5        | When we talk about software classification, we do not explicitly state that we will not have software which the NRC classification, Level 4 (malfunction causes death). Our process for classifying software does not check to see if the submitted software meets the definition of NRC Level 4. If we check the software and it meets the definition of NRC Level 4, then we need to reject that design. |   | ST         | 11/6 |  |

| #  | Affected Doc | Section        | Comment   | Recommended Resolution   | Identifier | Date | DOORs ID# |
|----|--------------|----------------|---|--|------------|------|-----------|
| 99 | SQAP         | 8.5 thru 8.5.3 | These sections will have to be modified to account for the fact that we will write an implementing procedure for IEEE 829 and RG 1.170. | Note: To keep the heading structure, change the names of the sub sections. Then all that will be necessary is to modify the contents of each section to compliment the implementing procedures.<br><br>8.5.1 Test Planning<br>8.5.2 Test Specification and Execution<br>8.5.3 Test Reporting | ST         | 11/7 |           |

| # | Affected Doc | Section                        | Comment  | Recommended Resolution   | Identifier | Date    | DOORs ID# |
|---|--------------|--------------------------------|--|--|------------|---------|-----------|
| 1 | SMP          | Proprietary Information Notice | <p>Broken sentence – The “except as specified above” clause is in the wrong place. Do you want the phase to apply to patented inventions as well?</p> <p>This document contains proprietary information of the General Electric Company (GE) and is furnished in confidence solely for the purpose(s) stated in the transmittal letter. No other use, direct or indirect, of the document or the information it contains is authorized. Furnishing this document does not convey any license, express or implied, to use any patented invention or <b>except as specified above</b>, any proprietary information of GE disclosed herein or any right to publish or make copies of the document without prior written permission of GE. The header of each page in this document carries the notation “GE Proprietary Information.”</p> | Suggested improvement – Place the phrase “except as specified above” after the word implied or at the beginning of the sentence. | ST         | 9/10/07 |           |
| 2 | SMP          | Proprietary Information Notice | <p>New Sentence – The word “figures” should be capitalized.</p> <p>GE proprietary information is identified by a dotted underline inside double square brackets. The electronic version includes a red font inside the brackets. For black-grayscale printed copies, the red font and dotted underline appears similar to normal text. [[This sentence is an example.<sup>{3}</sup>]] <b>figures and large</b> equation objects are identified with double square brackets before and after the object. In each case, the superscript notation <sup>{3}</sup> refers to Paragraph (2) of the enclosed affidavit, which provides the basis for the proprietary determination. Specific information that is not so marked is not GE proprietary.</p>   |  | ST         | 9/10/07 |           |

| # | Affected Doc | Section                        | Comment  | Recommended Resolution | Identifier | Date    | DOORS ID# |
|---|--------------|--------------------------------|--|------------------------|------------|---------|-----------|
| 3 | SMP          | Proprietary Information Notice | <p>The stated purpose appears to be very limited. Section 1.1, Overview seems more complete. Create a separate sentence about the ABWR supporting reference. Is the ESBWR supporting the ABWR or is the ABWR supporting the ESBWR? Can the ABWR and ESBWR support each other (both direction and not just a one way flow of information)?</p> <p>The information contained in this document is furnished <b>for the purpose of supporting the NRC review of the certification of the ESBWR</b>, with the information here being used as ABWR supporting reference.</p> |                        | ST         | 9/10/07 |           |
| 4 | SMP          | Table of Contents              | Table of Contents is missing from DOORS version.   |                        | ST         | 9/10/07 |           |
| 5 | SMP          | Table of Contents              | 5.4 Methods and Tools is in Bold. It is not in other sections of the Table of Contents. "and Tools" should be removed since 5.5 covers Tools   |                        | ST         | 9/10/07 |           |
| 6 | SMP          | Table of Contents              | 5.5 Tools is in Bold. It is not in other sections of the Table of Contents.  |                        | ST         | 9/10/07 |           |
| 7 | SMP          | Table of Contents              | 5.6 {{ Planning Phase. Remove double brackets. The double brackets appears in other places of the Table of Contents (e.g. 6.4.2, 6.5.1, 8.5.0, Appendix A  |                        | ST         | 9/10/07 |           |
| 8 | SMP          | Table of Contents              | Section 5 parts on the Software Development Lifecycle appears to be inconsistent in what order you discuss the individual phases. It appears that you are trying to discuss the parts that make up each phase as follows (1) Inputs (2) Outputs (3) Activities (4) Each Deliverable (can be more than one). (5) Baseline Review Record. When you look at each phase, the order varies, what is capitalized varies, which subsection title includes the phase in the title name varies. Not all phases discuss all 5 items.   |                        | ST         | 9/10/07 |           |
| 9 | SMP          | Table of Contents              | 5.11.7 is repeated twice.. Should the operation and training manuals be part of section 5.12? Training is not covered as a separate activity in section 5.   |                        | ST         | 9/10/07 |           |

| #  | Affected Doc | Section           | Comment   | Recommended Resolution | Identifier | Date    | DOORs ID# |
|----|--------------|-------------------|---|------------------------|------------|---------|-----------|
| 10 | SMP          | Table of Contents | Material in section 6.1 does not follow the same format in sections 5, 7, 8, and 9. Section 6.1 has no title.   |                        | ST         | 9/10/07 |           |
| 11 | SMP          | Table of Contents | Section 6 – There is no discussion of Tools used in the Integration Plan.   |                        | ST         | 9/10/07 |           |
| 12 | SMP          | Table of Contents | Section 6.5 does not discuss Problem Reporting as a separate sub section.   |                        | ST         | 9/10/07 |           |
| 13 | SMP          | General           | The SMP and each plan needs to discuss problem reporting and change control. Tools exist to help manage this.   |                        | ST         | 9/10/07 |           |
| 14 | SMP          | General           | Meetings and Emails have a tendency to change scope and requirements during the software development lifecycle. How will this be managed? How will the changes be documented, approved, and implemented? What will be done if an approved change or fix goes to a previous phase that has already been completed? |                        | ST         | 9/10/07 |           |
| 15 | SMP          | Table of Contents | 7.6.1 should be rolled into 7.6   |                        | ST         | 9/10/07 |           |
| 16 | SMP          | Table of Contents | No separate section 7.x for the Operation and Maintenance Manuals   |                        | ST         | 9/10/07 |           |
| 17 | SMP          | Table of Contents | There appears to be two 7.9 sections  |                        | ST         | 9/10/07 |           |
| 18 | SMP          | Table of Contents | Word has features to automatically create the Table of Contents for you.  |                        | ST         | 9/10/07 |           |
| 19 | SMP          | Table of Contents | Section 7, Software Installation Plan does not discuss the use of tools to help in this activity.   |                        | ST         | 9/10/07 |           |
| 20 | SMP          | General           | Tools exist for all activities involving software. We need to discuss if and how we are going to use them.  |                        | ST         | 9/10/07 |           |
| 21 | SMP          | General           | Documentation Control, Source Control, and Problem Documentation, Reporting, Resolution, and Implementation needs to be addressed in the SMP and in each plan of the SMP.   |                        | ST         | 9/10/07 |           |
| 22 | SMP          | Table of Contents | Spacing for Section 7.10 and above is different from the initial sections (2 spaces instead of 1 between the number and the title).   |                        | ST         | 9/10/07 |           |

| #  | Affected Doc | Section           | Comment   | Recommended Resolution  | Identifier | Date      | DOORS ID# |
|----|--------------|-------------------|---|---|------------|-----------|-----------|
| 23 | SMP          | Table of Contents | I don't understand why we have the section 7.11, Software Archive Retrieval. How will version control of software and documents be handled?   |   | ST         | 9/10/07   |           |
| 24 | SMP          | Table of Contents | Section 8.5.0 title is missing. All other parts of the SMP start with x.1 not x.0.<br><br>This is a typo in the SMP training course handout. I did not see this in the DOORS version.   |   | ST         | 9/10/07   | SMP-1635  |
| 25 | SMP          | Table of Contents | Section 8.5.1 You have Software Operations Maintenance Manuals. Did you mean Software Operation and Maintenance Manuals?  |   | ST         | 9/10/07   |           |
| 26 | SMP          | General           | Should the SMP say more about the Retirement Phase of the Software Development Lifecycle?   |   | ST         | 9/10/07   |           |
| 27 | SMP          | Table of Contents | For consistency, should section 9.7 Metrics be Measurement and Metrics.   |   | ST         | 9/10/07   |           |
| 28 | SMP          | Table of Contents | The use of dots in the Table of Contents conflicts with the dots we use to indicate GE proprietary Information  |   | ST         | 9/10/07   |           |
| 29 | SMP          | Appendix B        | The definitions for the three Software Classes are not in Alphabetical Order. They come after the P.. and before the R... definitions.  |   | ST         | 9/10/07   |           |
| 30 | SMP          | General           | When software is updated with a newer version, is the older version of the software covered by maintenance or is it considered retired software. How and where is it covered in the SMP.  |   | ST         | 9/10/07   |           |
| 31 | SMP          | 6                 | Would Software Integration Test Plan or Software Test Plan be a more appropriate title? Unit testing should be covered somewhere in the SMP? Does it matter if unit testing is done here at GE or by a vendor? Will the requirements of the SMP apply to vendors as well? |   | ST         | 9/10/07   |           |
| 32 | SMP          | 4.4.2 Tools       | Wording for first sentence "The Project manager shall specify approve which tools.."  | Should read "The Project manager shall approve which tools...". The PM may not necessarily specify the tools, but does have the responsibility to approve the use of the tools. | JMH        | 9-18-2007 |           |
| 33 | SMP          | Table 5.8-1       | Software Safety Analysis is entered twice in the table.   | Eliminate entry number 7 in Table 5.8-1   | JMH        | 9-18-2007 |           |



| #  | Affected Doc | Section                            | Comment   | Recommended Resolution   | Identifier          | Date       | DOORs ID# |
|----|--------------|------------------------------------|---|--|---------------------|------------|-----------|
| 34 | SMP          | Table 5.9-1                        | Table incorrectly lists "Requirements Baseline Review Record".  | Table entry should read 'Implementation Baseline Review Record'.   | JMH                 | 9-18-2007  |           |
| 35 | SMP          | Table 5.10-1                       | Item 1 – "Software Validation Test Report of N Class Software"  | Entry should read "Software Validation Test (SVT) Report of N Class Software"  | JMH                 | 9-18-2007  |           |
| 36 | SMP          | 6.1.1 Overview                     | Software Integration Plan acronym is entered as (SIP).  | The correct acronym is (SIntP).  | JMH                 | 9-18-2007  |           |
| 37 | SMP          | Figure 5-3 and all of section 5.7  | Figure 5-3 begins with the HSS, goes to the SyRS and SRS, then onwards. But the requirements section (5.7.4) begins at software tools and COTS which is in the middle of the requirements phase.  | Reorder ALL of section 5.7 to be consistent with figure 5-3. Follow the flow diagram.  | PWP                 | 9-19-2007  |           |
| 38 | SMP          | Figure 5-4 and all of section 5.8  | Figure 5-4 covers a lot more than what section 5.8 covers for the design phase of the software life cycle. SAT, MFAT and SFAT plans are missing from the discussion. So are supplemental documentation package for PDS and support S/W tool doc package                               | Cover each block in figure 5-4 within section 5.8 in the order that the figure flow, not just SVT plans, Intraystem comm. Protocol specs, SDDs and software coding & conventions guidelines. | PWP                 | 9-19-2007  |           |
| 39 | SMP          | Figure 5-5 and all of section 5.9  | Figure 5-5 has SSA after the SFT Report and SVT Plans, but section 5.9 discusses these right after coding and before discussing the process for code review and SFT. Section 5.9 additionally skips software release for validation testing shown on figure 5-5 to be before the BRR. | Cover each block within figure 5-5 in the order that it is shown, and ensure ALL blocks are covered.   | PWP                 | 9-19-2007  |           |
| 40 | SMP          | Figure 5-6 and all of section 5.10 | The SQA audit after the SVT Report is not discussed. Instead, the section jumps directly to production release & the SBD. The HFE V&V is also not covered in section 5.10   | Cover each block within figure 5-6 in the order that it is shown, and ensure ALL blocks are covered  | PWP                 | 9-19-2007  |           |
| 41 | SMP          | Figure 5-7 and all of section 5.11 | The HFE ISV, V&V RSR Results Summary Report are not discussed in section 5.11 even though they are shown on figure 5-7.   | Cover each block within figure 5-7 in the order that it is shown, and ensure ALL blocks are covered  | PWP                 | 9-19-2007  |           |
| 42 | SMP          | Figure 5-8 and all of section 5.11 | I agree with not covering SOM and Trng manuals in section 5.11 since they are covered at length later on. But no mention is made in section 5.11 of the SAA, Installation Checkout and HFE Design Implementation Results Summary Report that figure 5-8 shows.                        | Except for SOM and Trng manuals, cover each block within figure 5-7 in the order that it is shown, and ensure ALL blocks are covered   | PWP                 | 9-19-2007  |           |
| 43 | SMP          | Table 5.8-1                        | Table repeats Software Safety Analysis Report twice as items 5 and 7.   | Delete item 7; renumber remaining items accordingly.   | PWP for Tim Everitt | 09-24-2007 |           |

| #  | Affected Doc | Section         | Comment  | Recommended Resolution   | Identifier          | Date       | DOORS ID# |
|----|--------------|-----------------|--|--|---------------------|------------|-----------|
| 44 | SMP          | Section 5.8.3.3 | "...section from Section 5.8.3.3, I believe that the Software Validation Test Plan, Procedures, and Test Case Specification are intended to meet the "software requirements" instead of the "system requirements" which requires integration with the hardware system later in FAT phases. The entire software design phase is dedicated to the implementation of the software requirements. Slide 89 reinforces this by requiring traceability to the SRS, HSS, and UIS." | Change 1 <sup>st</sup> sentence in 5.8.3.3 to read: <u>"The Software Validation Test Plan, Procedures, and Test Case Specifications including acceptance criteria, define how the individual test cases will ensure that the completed, integrated software package meets the system software requirements</u> | PWP for Tim Everitt | 09-24-2007 |           |
| 45 | SMP          | Table 5.9-1     | Item 8 is incorrectly identified as Requirements Baseline Review Record instead of Implementation Baseline.....  | Change to Implementation Baseline Review Record  | PWP for Tim Everitt | 09-24-2007 |           |
| 46 | SMP          | Section 6.1.1   | Grammatical error: This Software Integration Plan (SIntP) consists of three major phases; integrating the various software modules together for form single programs, integrating the result of this the hardware and instrumentation and testing the resulting integrated product.  | Change to: This Software Integration Plan (SIntP) consists of three major phases; integrating the various software modules together for form single programs, integrating the result of this <u>with</u> the hardware and instrumentation and testing the resulting integrated product                         | PWP for Tim Everitt | 09-24-2007 |           |
| 47 | SMP          | 6.1.2           | Error is 6.1.2: "The purpose of this SMP is to:" should read "The purpose of this SintP is to:"  | Change to "The purpose of this SintP is to:"   | PWP for Tim Everitt | 09-24-2007 |           |
| 48 | SMP          | 6.2.2           | The DOORS version does not have "Software Functional Test Engineer" marked as an object header. DOORS item SMP-1257.<br><br>Reason: Difference between printed copy in SMP class and DOORS.  | Change line to an object header line. It should read "6.2 Software Functional Test Engineer (RTE)." The object header number for Test Personnel Qualifications should be 6.2.3   | ST                  | 10/2/07    | SMP-1257  |
| 49 | SMP          | Appendix C      | The definition of the word interface needs to include all four variations as defined in IEEE 610 and as requested by RG 1.172 and MPR review. The definition should be modified to include the additional NRC interpretation found in Reg Guide 1.172.   | See requirement in translation matrix.   | ST                  | 10/24      | RTD-115   |

| #  | Affected Doc | Section    | Comment   | Recommended Resolution  | Identifier | Date  | DOORs ID#  |
|----|--------------|------------|---|---|------------|-------|--|
| 50 | SMP          | 5.7.8      | More needs to be said about safety requirements than the one sentence in the last paragraph of section 5.7.8.   | Follow the links from the translation matrix to the SQAP for more information. Consideration should be given to writing an implementation procedure that expands on what needs to be in a software requirement specification document.      | ST         | 10/26 | RTD-169  |
| 51 | SMP          | Appendix A | Since we classify requirements as safety or non-safety, we meet the requirement that "requirements be ranked by importance". IEEE comments on stability and necessity are suggestions and not requirements. | Remove exception noted in Appendix A of the SMP for IEEE 830-1993   | ST         | 10/26 | RTD-129<br>RTD-169<br>RTD-171  |
| 52 | SMP          | 2.2.1      | You have two standards listed. They are both the same document.   | The two reference statements need to be combined into one reference.  | ST         | 10/28 | SMP-48<br>SMP-49   |
| 53 | SMP          | 5.7.8      | Nowhere in the document is the requirement to verify the SRS for modifiability and style.   | Add to section 5.7.8 a paragraph that cover all characteristics.  | ST         | 10/28 | SMP-686<br>RTD-4041<br>RTD-4042<br>RTD-133<br>RTD-173<br>thru RTD-176                    |
| 54 | SMP          | 5.7.8      | A glossary of definitions either inside the SRS or as a separate stand alone document is needed.  | A list of precise definitions of technical terms is needed. Include terms that may have multiple meanings so it is clear which definition is being used.  | ST         | 10/28 | RTD-4041<br>RTD-133<br>RTD-159<br>RTD-162<br>RTD-168<br>RTD-4038<br>RTD-4042<br>RTD-4147 |
| 55 | SMP          | 5.7.8      | The NRC input (RG 1.172) as to what information is needed for incomplete requirements (TBD's) is not enough.  | Use information from the IEEE to expand the discussion of incomplete requirements.  | ST         | 10/29 | RTD-165<br>RTD-166   |
| 56 | SMP          | 5.8.2      | <del>Software Safety Analysis Report is mentioned twice in the design output table.</del>   | Remove one of the entries   | ST         | 11/1  | SMP-778  |
| 57 | SMP          | 5.7.8      | We need an implementing procedure for the software requirement specification document.  | Use the implementing procedure to cover the "should" requirements found in the translation matrix. The requirements cover BTP 7-14, RG 1.172, and IEEE 830. Columns where the reviewer initials are ST2 and ST3 will go into this document. | ST         | 11/1  | RTD-109  |

| #  | Affected Doc | Section     | Comment  | Recommended Resolution  | Identifier | Date  | DOORS ID#                       |
|----|--------------|-------------|--|---|------------|-------|---------------------------------|
| 58 | SMP          | 5.7.7 5.7.8 | When requirements discuss functionality of the software, it is not made clear that each mode of operation must be covered  | Add statement "for each mode of operation" to the SMP. See RTD entries for links.   | ST         | 11/1  | RTD-161<br>RTD-4023<br>RTD-4034 |
| 59 | SMP          | Various     | SMP and SQAP talk about cyber security but they do not classify the security threats according to impact on safety and likelihood of occurrence.   | Add the requirement that identified security threats need to be classified according to their impact on safety and likelihood of occurrence. Use DOORS links to find needed sections. | ST         | 11/1  | RTD-141<br>RTD-4029             |
| 60 | SMP          | General     | The abbreviations "SMP" and "SCMP" are used interchangeably throughout NEDE-33226 & NEDE-33245 to refer to NEDE-33226. All uses of "SCMP" to refer to NEDE-33226 should be changed to "SMP".   |   | JMH        | 11/1  |                                 |
| 61 | SMP          | 5.7.8       | The section on SRS does not talk about the fact that the System Requirement Specification is one of the documents that drive the SRS document.   | Whenever HSS is mentioned, mention the SyRS. The list of documents that feed into the SRS should also include the Output documents from the planning phase.                           | ST         | 11/2  | RTD-160                         |
| 62 | SMP          | 5.9.3.4     | <b>Training feedback:</b> code reviews should specify Class Q is required IVVT review  |   | Greg Droba | 11/26 |                                 |
| 63 | SMP          | General     | <b>Training feedback:</b> SMP validation makes sure we are building the thing to the requirements specified, but there are no words or such to consider if we are building the right thing. This is an important part of validation. |   | Greg Droba | 11/26 |                                 |
| 64 | SMP          | General     | <b>Training feedback:</b> SBD in Test Phase should be Release Description. Not the same as SBD in Implementation Phase.  |   | Ty Rogers  | 11/26 |                                 |
| 65 | SMP          | General     | <b>Training feedback:</b> Evaluate COTS in implementation phase, NOT requirements phase  |   | Ty Rogers  | 11/26 |                                 |
| 66 | SMP          | General     | <b>Training feedback:</b> Update implementation phase to show loopback from code review & SFT to Coding. Code review and SFT should not be parallel activities, but series with Code Review 1 <sup>st</sup> .                        |   | Ty Rogers  | 11/26 |                                 |
| 67 | SMP          | 5.9.3.4     | <b>Training feedback:</b> Should allow use of automated tools for code review - also in SintP  |   | Ty Rogers  | 11/26 |                                 |

| #  | Affected Doc | Section           | Comment   | Recommended Resolution  | Identifier | Date  | DOORs ID# |
|----|--------------|-------------------|---|---|------------|-------|-----------|
| 68 | SMP          | 5.9.3.5           | <b>Training feedback:</b> Should allow use of automated tools for unit test & integration test (i.e., LDRA) – also in SintP   |   | Ty Rogers  | 11/26 |           |
| 69 | SMP          | General           | <b>Training feedback:</b> Deferred verification per EOP only applies to docs issued by RMCN. [Can't do SQA deferred design verifications.]  |   | Ty Rogers  | 11/26 |           |
| 70 | SMP          | General           | <b>Training feedback:</b> Suggest to change “target environment” to “installed environment” or “deployment environment” or other to describe site installation. [Target environment has a special meaning in software development that differs from the way in which it's used in the SMP.]             |   | Ty Rogers  | 11/26 |           |
| 71 | SMP          | 5.7.8 section 4.d | This comment on minimizing the use of assembly language needs to be removed. Whatever programming language that is appropriate to the application should be used regardless of people's personal attitude. IEEE 830 clearly states that design decisions be left out of the requirement specifications. | Remove all of part 4.d  | ST         | 11/3  |           |
| 72 | SMP          | 5.7.8             | BTP 7-14 states that Correctness <b>requires</b> that no other requirements be stated. This is not mentioned in the SMP.  | Add a statement to the SMP that the SRS not contain requirements that belong in other documents.  | ST         | 11/3  | RTD-4039  |
| 73 | SMP          | 5.7.8             | The IEEE states that a SRS is correct if, and only if, every requirement stated therein is one that the software shall meet. This really isn't mentioned in the SMP or SQAP.  | Add a statement to the SMP that every requirement in the SRS is one that can be met and shall be met.   | ST         | 11/3  | RTD-157   |
| 74 | SMP          | Appendix A        | For RG 1.170 and IEEE 829, add the following exception. Two entries in the table needs to be updated.   | The sequence order of sections for each document found in IEEE 829 will not be followed. The justification for this is: Modern Tools and Techniques do not always allow themselves to follow the outline found in IEEE 829. When that is the case, the required information will be captured and displayed in a readable and understandable manor that is best for the tool/technique and the reader/users. | ST         | 11/5  |           |

| #  | Affected Doc | Section          | Comment  | Recommended Resolution  | Identifier | Date  | DOORS ID#  |
|----|--------------|------------------|--|---|------------|-------|--|
| 75 | SMP          | Various          | When the test documentation layout is discussed, add the following statement to that paragraph. See the RTD ID# for list of locations        | RG 1.170 and IEEE 829 shall be followed ... as amended by the exception in Appendix A ... Modern Tools and Techniques do not always allow themselves to follow the outline found in IEEE 829. When that is the case, the required information will be captured and displayed in a readable and understandable manor that is best for the tool/technique and the reader/users. | ST         | 11/5  | SMP-1267<br>RTD-618<br>RTD-625<br>RTD-634<br>RTD-640<br>RTD-647<br>RTD-652<br>RTD-658<br>RTD-668 |
| 76 | SMP          | Various          | We need an implementing procedure for test documentation.  | Write an implementing procedure to cover the parts of RG 1.170 and IEEE 829 not covered in the SMP and SQAP. Update SMP and SQAP to reference the implementing procedure.   | ST         | 11/5  |  |
| 77 | SMP          | 6.5 thru 6.5.1.3 | These sections will have to be modified to account for the fact that we will write an implementing procedure for IEEE 829 and RG 1.170.      |   | ST         | 11/7  |  |
| 78 | SMP          | Section 5.0      | GE needs to state that the project will use a Waterfall type Software Development Model for all of the ESBWR software development processes. |   | RJS        | 11/16 |  |

## **Doors Audit - List of GEH Attendees and Titles**

|                   |  |
|-------------------|--|
| Lloyd Heckle      | SQA Manager  |
| Richard Stattel   | SPE Lead Engineer  |
| Rajeev Kohli      | Sr. Engineer I&C   |
| Mike Herron       | SPE Sr. Engineer   |
| Paul Primavera    | SPE Training Engineer (Granite)                          |
| Melissa Crownover | SPE Software Engineer (Granite)                          |
| Wayne Glidden     | SPE Software Engineer (Granite) New Hire                 |
| Sam Thompson      | SPE Software Engineer (Granite) On phone from Wilmington |
| Tim Everitt       | Software Quality Control Manager Salem Va.               |
| Don Lewis         | Regulatory Affairs Engineer                              |

Tuesday 11/13/07

NRC Software Audit Meeting Attendance (Wednesday 11/14/07)

| Name              | Company    | Phone          | EMail                    |
|-------------------|------------|----------------|--------------------------|
| Rich Stattel      | GE         | (910)602-4593  | Richard.stattel@ge.com   |
| Joe Ashcraft      | NRC        | (301)415-3177  | jma3@nrc.gov             |
| Lloyd Heckle      | GE         | (910)233-0675  | Lloyd.Heckle@ge.com      |
| Paul Primavera    | Granite    | (910)508-0481  |                          |
| Melissa Crowmover | GRANITE    | (404)610-5846  | MELISSA.CROWMOVER@ge.com |
| Royce Beacom      | NRC        | 3014152781     | rdby@nrc.gov             |
| Debra Herrmann    | NRC        | 301.415.7314   | dsh2@NRC.gov             |
| Tim Everitt       | GE Salem   | 540-387-7037   | timothy.everitt@ge.com   |
| KIMBERLEY CORP    | NRC        | 301-415-1091   | karl@nrc.gov             |
| Lenny Hardin      | NRC        | 301-415-6315   | LAH3@NRC.GOV             |
| Rajeev Kohli      | GE-H       | (910)-602-4944 | Rajeev.Kohli@GE.com      |
| John M. Herrow    | GE-H       | 410-610-4098   | john.M.herrow@GE.com     |
| Dennis Galrin     | NRC        | 301-415-6256   | djg3@nrc.gov             |
| Hulbert Li        | NRC        | 301415-2846    | HCL@NRC.GOV              |
| Ian Jung          | NRC        | 301 415 2969   | IxJ@NRC.GOV              |
| Don Lewis         | GE         | 910-675-6887   | don.lewis@ge.com         |
| JOSE MARCH-LEUBA  | ORNL       | 865 574 5571   | MARCHLEUBAJA@ORNL.GOV    |
| Andrew Loebi      | ORNL       | 8655745966     | Loebias@ORNL.GOV         |
| Wayne Glidden     | GE Granite | 404 610-4499   | wayne.glidden@ge.com     |
|                   |            |                |                          |





NRC Software Audit Meeting Attendance (Friday 11/16/07)

| Name           | Company | Phone                                   | EMail                  |
|----------------|---------|---|------------------------|
| Rich Stattel   | GE      | (910)602-4593                           | Richard.stattel@ge.com |
| Dor Lewis      | GE      | (910)675-6789                           | dor.lewis@ge.com       |
| Dennis Galvin  | NRC     | 301-415-6256<br><del>301-415-6256</del> | djg3@nrc.gov           |
| Andrew Loebl   | ORNL    | 865 574 5966                            | LoeblAS@ORNL.gov       |
| Mike Herrod    | GE      | 410-610-4098                            | John M. Herrod@GE.com  |
| LEROY HAZARDIN | NRC     | 301-415-6515                            | LAH3@NRC.GOV           |
| Lloyd Heckle   | GE      | 910-233-0675                            | Lloyd.Heckle@GE.Com    |
| Rich Stattel   | GE      |   |                        |
| Ian Jung       | NRC     | 301-415-2969                            | IXJ@NRC.GOV            |
|                |         |   |                        |
|                |         |   |                        |
|                |         |   |                        |
|                |         |   |                        |
|                |         |   |                        |
|                |         |   |                        |
|                |         |   |                        |
|                |         |   |                        |
|                |         |   |                        |
|                |         |   |                        |
|                |         |   |                        |

**Enclosure 5**

**MFN 07-627**

**Affidavit**

# GE Hitachi Nuclear Energy

## AFFIDAVIT

I, **David H. Hinds**, state as follows:

- (1) I am General Manager, New Units Engineering, GE Hitachi Nuclear Energy ("GEH"), have been delegated the function of reviewing the information described in paragraph (2) which is sought to be withheld, and have been authorized to apply for its withholding.
- (2) The information sought to be withheld is contained in Enclosure 1 of GEH letter MFN 07-627, Mr. James C. Kinsey to U.S. Nuclear Regulatory Commission, entitled *Submittal of DOORS Software Audit Presentation Slides for Support of ESBWR Design Certification Application – Human Factors Engineering*, dated January 21, 2007. The proprietary information in Enclosure 1, *Presentation Materials Used During NRC Audit of DOORS (Proprietary)*, is delineated by a [[underline inside double square brackets<sup>131</sup>]]. Figures and large equation objects are identified with double square brackets before and after the object. In each case, the superscript notation {3} refers to Paragraph (3) of this affidavit, which provides the basis for the proprietary determination.
- (3) In making this application for withholding of proprietary information of which it is the owner, GEH relies upon the exemption from disclosure set forth in the Freedom of Information Act ("FOIA"), 5 USC Sec. 552(b)(4), and the Trade Secrets Act, 18 USC Sec. 1905, and NRC regulations 10 CFR 9.17(a)(4), and 2.790(a)(4) for "trade secrets" (Exemption 4). The material for which exemption from disclosure is here sought also qualify under the narrower definition of "trade secret", within the meanings assigned to those terms for purposes of FOIA Exemption 4 in, respectively, Critical Mass Energy Project v. Nuclear Regulatory Commission, 975F2d871 (DC Cir. 1992), and Public Citizen Health Research Group v. FDA, 704F2d1280 (DC Cir. 1983).
- (4) Some examples of categories of information which fit into the definition of proprietary information are:
  - a. Information that discloses a process, method, or apparatus, including supporting data and analyses, where prevention of its use by GEH's competitors without license from GEH constitutes a competitive economic advantage over other companies;
  - b. Information which, if used by a competitor, would reduce his expenditure of resources or improve his competitive position in the design, manufacture, shipment, installation, assurance of quality, or licensing of a similar product;
  - c. Information which reveals aspects of past, present, or future GEH customer-funded development plans and programs, resulting in potential products to GEH;

- d. Information which discloses patentable subject matter for which it may be desirable to obtain patent protection.

The information sought to be withheld is considered to be proprietary for the reasons set forth in paragraphs (4)a, and (4)b, above.

- (5) To address 10 CFR 2.390 (b) (4), the information sought to be withheld is being submitted to NRC in confidence. The information is of a sort customarily held in confidence by GEH, and is in fact so held. The information sought to be withheld has, to the best of my knowledge and belief, consistently been held in confidence by GEH, no public disclosure has been made, and it is not available in public sources. All disclosures to third parties including any required transmittals to NRC, have been made, or must be made, pursuant to regulatory provisions or proprietary agreements which provide for maintenance of the information in confidence. Its initial designation as proprietary information, and the subsequent steps taken to prevent its unauthorized disclosure, are as set forth in paragraphs (6) and (7) following.
- (6) Initial approval of proprietary treatment of a document is made by the manager of the originating component, the person most likely to be acquainted with the value and sensitivity of the information in relation to industry knowledge. Access to such documents within GEH is limited on a "need to know" basis.
- (7) The procedure for approval of external release of such a document typically requires review by the staff manager, project manager, principal scientist or other equivalent authority, by the manager of the cognizant marketing function (or his delegate), and by the Legal Operation, for technical content, competitive effect, and determination of the accuracy of the proprietary designation. Disclosures outside GEH are limited to regulatory bodies, customers, and potential customers, and their agents, suppliers, and licensees, and others with a legitimate need for the information, and then only in accordance with appropriate regulatory provisions or proprietary agreements.
- (8) The information identified in paragraph (2), above, is classified as proprietary because it identifies detailed GEH ESBWR methods, techniques, information, procedures and assumptions related to its Human Factors Engineering technology. Development of these methods, techniques, information, procedures and assumptions and their application for the design, modification, and analyses methodologies and processes for Human Factors Engineering and Software Management was achieved at a significant cost to GEH and would result in a significant economic and competitive advantage to a competitor.

The development of the evaluation process along with the interpretation and application of the analytical results is derived from the extensive experience database that constitutes a major GEH asset.

- (9) Public disclosure of the information sought to be withheld is likely to cause substantial harm to GEH's competitive position and foreclose or reduce the availability of profit-making opportunities. The information is part of GEH's comprehensive BWR safety and technology base, and its commercial value extends beyond the original development cost. The value of the technology base goes beyond the extensive physical database and analytical methodology and includes development of the expertise to determine and apply the appropriate evaluation process. In addition, the technology base includes the value derived from providing analyses done with NRC-approved methods.

The research, development, engineering, analytical and NRC review costs comprise a substantial investment of time and money by GEH.

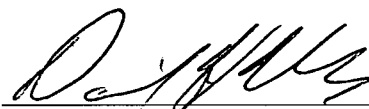
The precise value of the expertise to devise an evaluation process and apply the correct analytical methodology is difficult to quantify, but it clearly is substantial.

GEH's competitive advantage will be lost if its competitors are able to use the results of the GEH experience to normalize or verify their own process or if they are able to claim an equivalent understanding by demonstrating that they can arrive at the same or similar conclusions.

The value of this information to GEH would be lost if the information were disclosed to the public. Making such information available to competitors without their having been required to undertake a similar expenditure of resources would unfairly provide competitors with a windfall, and deprive GEH of the opportunity to exercise its competitive advantage to seek an adequate return on its large investment in developing these very valuable analytical tools.

I declare under penalty of perjury that the foregoing affidavit and the matters stated therein are true and correct to the best of my knowledge, information, and belief.

Executed on this 21<sup>st</sup> day of January 2008.



---

David H. Hinds  
GE Hitachi Nuclear Energy