



HITACHI

GE Hitachi Nuclear Energy

Richard E. Kingston
Vice President, ESBWR Licensing

PO Box 780
3901 Castle Hayne Road, M/C A-55
Wilmington, NC 28402-0780 USA

T 910.819.6192
F 910.362.6192
rick.kingston@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 08-920, Supplement 3

Docket No. 52-010

December 17, 2008

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

Subject: **Response to Portion of NRC Request for Additional Information Letter No. 257 Related to ESBWR Design Certification Application - Instrumentation & Control Systems - RAI Numbers 7.1-127, 7.1-128, 7.1-129, and 7.1-130**

The purpose of this letter is to submit the GE Hitachi Nuclear Energy (GEH) response to the U.S. Nuclear Regulatory Commission (NRC) Request for Additional Information (RAI) sent by NRC letter dated September 14, 2008. GEH response to RAI Numbers 7.1-127, 7.1-128, 7.1-129, 7.1-130 is addressed in Enclosures 1, 2, and 3.

Enclosure 2 contains GEH proprietary information. GEH customarily maintains this information in confidence and withholds it from public disclosure. A non-proprietary version is provided in Enclosure 3.

The affidavit contained in Enclosure 4 identifies that the information contained in Enclosure 2 has been handled and classified as proprietary to GEH. GEH hereby requests that the information of Enclosure 2 be withheld from public disclosure in accordance with the provisions of 10 CFR 2.390 and 9.17.

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

Sincerely,

Richard E. Kingston
Vice President, ESBWR Licensing

DO68
NRO

Reference:

1. MFN 08-687, Letter from U.S. Nuclear Regulatory Commission to Robert E. Brown, *Request For Additional Information Letter No. 257 Related To ESBWR Design Certification Application*, dated September 14, 2008

Enclosures:

1. Response to Portion of NRC Request for Additional Information Letter No. 257 Related to ESBWR Design Certification Application - Instrumentation & Control Systems - RAI Numbers 7.1-127, 7.1-128, 7.1-129, and 7.1-130
2. Response to Portion of NRC Request for Additional Information Letter No. 257 Related to ESBWR Design Certification Application - Instrumentation & Control Systems - Licensing Topical Report Markups for RAI Numbers 7.1-127, 7.1-128, and 7.1-129 - GEH Proprietary Information
3. Response to Portion of NRC Request for Additional Information Letter No. 257 Related to ESBWR Design Certification Application - Instrumentation & Control Systems - Licensing Topical Report Markups for RAI Numbers 7.1-127, 7.1-128, and 7.1-129 - Non-Proprietary Version
4. Affidavit – David H. Hinds

cc:

AE Cabbage	USNRC (with enclosure)
RE Brown	GEH/Wilmington (with enclosure)
DH Hinds	GEH/Wilmington (with enclosures)
eDRF Section:	0000-0093-6337 (RAI 7.1-127)
	0000-0093-8467 (RAI 7.1-128)
	0000-0093-9109 (RAI 7.1-129)
	0000-0093-9132 (RAI 7.1-130)

MFN 08-920, Supplement 3

Enclosure 1

**Response to Portion of NRC Request for
Additional Information Letter No. 257
Related to ESBWR Design Certification Application**

Instrumentation & Control Systems

RAI Numbers 7.1-127, 7.1-128, 7.1-129, and 7.1-130

NRC RAI 7.1-127

The staff found multiple issues in the software LTRs NEDE-33226P and NEDE-33245P where the internal procedure reference was not correct. Please correct all references in these documents. One possible solution would be to use the same reference list in both documents – as appears to be the case for the Software Conformance Review – Appendix A – contained in both LTR's.

For example the procedure, "Reporting of Defects and Noncompliance Under 10 CFR Part 21" is referenced as 3.g on numbered page 9 of NEDE-33226P, Rev 3. However, on numbered page 22, this procedure is footnoted as 2.g. Likewise, the procedure "Deferred Design Verification," is referenced as 2.g on numbered page 6 of NEDE-33226P, Rev 3. However, on numbered page 28, this procedure is footnoted as 2.q. "Design Review" has a similar problem. It is referenced as 2.c on numbered page 6 of NEDE-33226P, Rev 3, but footnoted as 2.e throughout the document. 2.e also refers to "Material Request." 2.c does not appear as a footnote anywhere in the document. In NEDE-33245P, 2.e refers to "Design Review."

GEH Response

Licensing Topical Reports (LTRs) NEDE-33226P, ESBWR Software Management Program Manual, Revision 3, and NEDE-33245P, ESBWR Software Quality Assurance Program Manual, Revision 3, were reviewed for incorrect references to internal procedures. Multiple incorrect references were found in NEDE-33226P and corrected. None were found in NEDE-33245P.

A common reference list (Section 2.3 of each LTR) would not be beneficial as the LTRs emphasize different aspects of software management and quality, resulting in divergent procedure references.

DCD/LTR Impact

No DCD changes will be made in response to this RAI.

LTR NEDE-33226, Revision 3 will be revised as described above for this RAI. Example changes are provided on the enclosed markup pages. No changes are required for NEDE-33245 for this RAI.

NRC RAI 7.1-128

LTR NEDE-33226P, Section 2.3 lists several documents which are identified as subject to revision to remain current with GEH internal procedures, and do not require the NEDE-33226P to be updated when they are revised. The staff has identified several documents that are not subject to revision as described in NEDE-33226P:

NEDE-33245P; NEDE-33295P, "ESBWR Cyber Security Program Plan"; and NEDO-33275, "ESBWR HFE Training Development Implementation Plan" are incorporated by reference into the DCD and subject to specific controls.

IEEE 610.12-1990 and EPRI TR-106439 are not GEH documents.

Clarify the GEH documents that may be revised as described in NEDE-33226P, Section 2.3.

GEH Response

The subject Licensing Topical Reports (LTRs) were reviewed and the following changes made to correct the identified deficiencies.

LTR NEDE-33226, ESBWR Software Management Program Manual, Revision 3, (SMPM)

1. *In Section 2.3, removed the following sentences:*

"These documents are subject to revision to remain current with GEH internal procedures, and do not require the SMPM to be updated when they are revised. Requirements which are being met by these documents shall be maintained via the Requirements Traceability Matrix (RTM)."

Removal of this statement makes the LTR NEDE-33226 (SMPM) consistent with LTR NEDE-33245, ESBWR Software Quality Assurance Program Manual, Revision 3, (SQAPM) and removes any confusion about document revisions.

2. In order to clarify document references, the following changes were made:
 - a. Old reference 2.3(1) "Software Quality Assurance Program Manual" was renumbered to 2.3(1.a)
 - b. Old reference 2.3(4) "Cyber Security Program Plan" was moved to new section 2.3(1.b)
 - c. Old reference 2.3(5) "HFE Training Development" was moved to new section 2.3(1.c).
 - d. Old reference 2.3(6) "IEEE Standard Glossary" was moved to Section 2.4 with the other IEEE standard guidance documents.

- e. Old reference 2.3(7) "EPRI TR-106439" was renumbered to 2.3(4).
- f. Old reference 2.3(8) "Cyber Security Program Manual" was deleted. References to and statements addressing the Cyber Security Program Manual were revised to point to and to clarify implementation of the Cyber Security Program Plan, 2.3(1.b).
- g. All references in the SMPM affected by the above changes were revised to reflect the new reference number.

LTR NEDE-33245 (SQAPM)

1. No change is needed to LTR NEDE-33245 to clarify document revisions as only LTR NEDE-33226 had a statement addressing this topic.
2. In order to clarify document references, the following changes were made:
 - a. Old reference 2.3(1) "SMPM" was renumbered to 2.3(1.a).
 - b. Old reference 2.3(4) "IEEE Standard Glossary of Software Engineering Terminology" was moved to 2.4.
 - c. Old reference 2.3(5) "Commercial Grade Digital Equipment" was renumbered to 2.3(4)
 - d. Old reference 2.3(6) "Cyber Security Program Plan" was moved to new section 2.3(1.b).
 - e. All references in the SQAPM affected by the above changes were revised to reflect the new reference number.
3. Because of a change in numbering of references from earlier revisions of the document, some reference numbers in the text were incorrect (e.g., R.G. 1.173 was referenced as 2.2.3(6), when the original (6) had been converted to a bullet format). To assure correct references in conformance with the RAI, these references were also corrected.

DCD/LTR Impact

No DCD changes will be made in response to this RAI.

LTRs NEDE-33226, Revision 3 and NEDE-33245, Revision 3 will be revised as described above. NEDE-33226, Section 2 and NEDE-33245, Section 2 changes as described above are enclosed. Changes to correct text to the new reference numbers throughout the remainder of the documents are editorial in nature and are not attached.

NRC RAI 7.1-129

NEDE-33245P, Rev. 3, Figure 2, the first footnote says:

"This represents the organization at the time of SMPM and SQAPM development to reflect the independence of the I&C, SPE and SQA organizations. The organization is subject to change. However, independence of these functions shall be maintained."

In a teleconference, GEH informed the staff that Figure 2 is already obsolete. NRC expects GEH to make NEDE-33245P Tier 2 and accordingly Figure 2 should be revised and presented at a level that will have minimal changes over time while showing the independence of software development, verification and validation, and quality assurance functions. GEH should also identify the criteria it will use to maintain appropriate independence in future organizational changes.*

GEH Response

GEH agrees with the NRC Staff that the existing I&C, Software Project Engineering (SPE), and Software Quality Assurance (SQA) organizational structures do not match those as shown in Figure 3-1 of NEDE-33226P, ESBWR Software Management Program Manual, Revision 3 (SMPM) and Figure 2 of NEDE-33245P, ESBWR Software Quality Assurance Program Manual, Revision 3 (SQAPM). In order to remove obsolescence issues with SMPM Figure 3-1 and SQAPM Figure 2, GEH will eliminate the figures as they add no real value and the organization is expected to change over time. GEH also agrees to clarify the criteria used for ensuring independence between the I&C Design group, the SPE organization, and the SQA organization.

GEH will designate the SMPM and SQAPM as Tier 2* within the DCD as will be addressed in the response to RAI 14.3-420.

DCD/LTR Impact

No DCD changes will be made in response to this RAI.

NEDE-33226, ESBWR Software Management Program Manual and NEDE 33245, ESBWR Software Quality Assurance Program Manual will be revised as shown on the enclosed mark-ups.

NRC RAI 7.1-130

NEDE-33226P, Rev. 2 provides a discussion of the retirement phase of software but does not identify whether replacement (updating/upgrading) software can be run concurrent with existing software such that there is a period of dual operation using both systems. Clarify the methods by which dual operations will take place during the retirement phase (5.13).

The TR does not clearly show the process by which the installation of software on installed systems in operating plants is performed. Affected functions should be declared inoperable according to the plant's technical specifications before proceeding with installation, and appropriate return-to-service testing should be conducted before declaring the new/upgraded/replacement software operable. In general, there is an overall concern over risks during maintenance activities, especially those risks that may compromise safety.

Please provide further details on how these maintenance/upgrade activities, both during the retirement phase and/or operation and maintenance phase are managed in a manner that minimizes risks to the safety systems.

GEH Response

GEH concurs with the request for clarification. For clarification of the NRC staff's concerns regarding software upgrades and maintenance/retirement activities refer to the following sections of NEDE-33245P, Rev. 3, Software Quality Assurance Program Manual, and NEDE-33226P, Rev. 3, Software Management Program Manual.

The process that describes parallel operation of the old and new system and by which installation of the software on installed systems in operating plants is performed as described in NEDE-33245P, Rev. 3. Section 4.4.2.2 states, in part:

The Startup Procedure shall address the requirements for safely starting the new system and, if an old system is to be replaced, for making a safe transition from the old system to the new system. At a minimum, the following shall be addressed:

- Fallback modes for the new system
- Startup of backup components and subsystems
- Startup of the new system
- Parallel operation with backups
- Parallel operation of the old system and the new system
- Subsystem vs. full system operation

- Switchover to full system operation
- Validation of results from the new system
- Cross validation of results between the old system and the new system
- Fallback in the case of failure of the new system, including fallback to an old system if one exists

Further details on how these maintenance/upgrade activities, both during the retirement phase and/or operation and maintenance phase are managed in a manner that minimizes risks to the safety systems is described in NEDE-33226P, Rev. 3. Section 7.5.1 states, in part:

As a separate document or as a part of the O&M manual, the initial installation procedure for each individual software package and for each/or system or logical group of systems shall be defined for each plant software systems. The installation procedure shall include:

- A checklist or sequence of steps that can be used to confirm that correct software is installed in the specific systems in accordance with the system design documents. The following is a sample list of items to be considered as part of the checklist:
- Affected functions are inoperable and in a safe condition according to the plant's technical specifications before proceeding with installation.
- The computer system is functional.
- The sensors and actuators are functional.
- All cards are present and installed in the correct slots.
- The communication system is correctly installed.
- The correct software versions are installed on the correct computers.
- Appropriate return-to-service testing has been successfully conducted before declaring the modified function operable.
- Installation configuration tables are complete.
- Environmental conditions (e.g., temperature, humidity, vibration, and rack space) are considered and provided for.
- Special tools, methods, or techniques used to accomplish the installation function shall be identified.

- Installation tools shall be qualified with a degree of rigor and level of detail appropriate to the safety significance of the software utilizing the installation tools.
- Security provisions have been satisfied.
- Precautions to ensure personnel and plant safety have been identified.

DCD/LTR Impact

No DCD changes will be made in response to this RAI.

No changes to the subject LTRs will be made in response to this RAI.

MFN 08-920, Supplement 3

Enclosure 3

**Response to Portion of NRC Request for
Additional Information Letter No. 257
Related to ESBWR Design Certification Application**

Instrumentation & Control Systems

**Licensing Topical Report Markups for
RAI Numbers 7.1-127, 7.1-128, and 7.1-129**

Non-Proprietary Version

NON-PROPRIETARY INFORMATION NOTICE

These are non-proprietary versions of the documents NEDE-33226P and NEDE-33245P, from which the proprietary information has been removed. Portions of the document that have been removed are identified by white space within double square brackets, as shown here [[]].

**Markups for
RAI 7.1-127**

[[

]]

If a change to the SMPM is warranted, one of the SQA activities shall determine if NRC notification is required and shall track the notification process as defined by the MMIS HFE IP [2.1].

Changes to the SMPM require approvals of the following managers or designated appointees: I&C Manager, SPE Manager, and the SQA Manager.

[[



]]

If changes to the SMPM are made, the I&C Manager must document an evaluation indicating that previously completed projects do not have to be reopened to implement the SMPM changes. When changes are made to the SMPM, requirements traceability will be maintained and verified.

3.6 PROJECT MANAGEMENT PRIORITIES, MONITORING, AND CONTROL

The objective of project management is to coordinate the development of project deliverables and to ensure that the deliverables meet the Licensee expectations for nuclear safety, quality, cost, and schedule. The key elements for a successful project delivery by project management are:

- Integrity - Integrity for all aspects of project performance is practiced at all times
- Quality - Compliance with the software development and quality assurance process defined in the SMPM, the SQAPM [2.3 (1)], and the applicable industry codes and standards
- Occupational Safety - Safe work habits are practiced at all times
- Outputs - Deliverables meet the quality, schedule, and budget requirements as specified by the project work plans

[[

]]

The key management processes are:

- Project Initiation
- Project Planning and Scheduling

]]

5.8.3.4 Software Support Tool Documentation Package

The Software developer shall evaluate the use of software tools in the new design and document the intended use consistent with the Software Requirements Specification and Software Design Description.

5.8.3.5 Application of Previously Developed Software

]]



Appendix A - Software Plans Conformance Review								
Item	Reg Guide	IEEE Stand.	Related Software Plan			Deviation	Conform. Code	Justification
			SMPM	SQAPM	None			

**Markups for
RAI 7.1-128**

2.2.3 U.S. Nuclear Regulatory Commission (NRC) Regulatory Guides (RG)

- RG 1.152-2006 - Criteria for Use of Computers in Safety Systems of Nuclear Power Plants
- RG 1.168-2004 - Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
- RG 1.169-1997 - Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
- RG-1.170-1997- Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
- RG-1.171-1997 - Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
- RG 1.172-1997 - Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
- RG 1.173-1997 - Developing Software Life cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

2.2.4 Institute of Electrical and Electronic Engineers (IEEE) Standards

The following standards are applicable to the activities specified within the SMPM. The SMPM conforms to planning requirements of these standards except as explicitly noted in Appendix A.

The IEEE Standards provide recommended implementation techniques and methods. The SMPM makes specific commitments only to those requirements restated in this document. The ESBWR Project Work Plans shall capture the detailed implementation attributes in accordance with Work Planning and Scheduling [2.3(2.a)]. Future exceptions or deviations from the recommendations specified in the IEEE standards shall require management approval as defined in the SQAPM [2.3(1.2.3(1.a))] and the SMPM, and are potentially subject to NRC notification in accordance with the MMIS/HFE Implementation Plan [2.1].

- IEEE 7-4.3.2-2003 IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations
- IEEE 1012-1998 IEEE Standard for Software Verification and Validation
- IEEE 1028-1997 IEEE Standard for Software Reviews Description
- IEEE 828-1990 IEEE Standard for Software Configuration Management Plans
- IEEE-1042-1987 IEEE Guide to Software Configuration Management Description
- IEEE-829-1983 IEEE Standard for Software Test Documentation

- IEEE-1008-1987 IEEE Standard for Software Unit Testing
- IEEE-830-1993 IEEE Recommended Practice for Software Requirements Specifications
- IEEE-1074-1995 IEEE Standard for Developing Software Life cycle Processes
- IEEE 603-1991 and correction sheet dated January 30, 1995 - IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations. This IEEE standard is applicable to the design of safety-related instrumentation and control systems of which software is a part.

2.3 SUPPLEMENTAL DOCUMENTS

The following supplemental documents are used in conjunction with the SMPM and enable the performance of the activities stated in Appendix A. ~~These documents are subject to revision to remain current with GEH internal procedures, and do not require the SMPM to be updated when they are revised. Requirements which are being met by these documents shall be maintained via the Requirements Traceability Matrix (RTM).~~

Reference Number	Document
1.a	GE Hitachi Nuclear Energy, "ESBWR - Software Quality Assurance Program Manual," NEDE-33245P, Class III (Proprietary), and NEDO-33245, Class I (Non-Proprietary)
1.b	GE Hitachi Nuclear Energy, "ESBWR Cyber Security Program Plan," NEDE-33295P, Class III (Proprietary), and NEDO-33295, Class I (Non-Proprietary)
1.c	GE Hitachi Nuclear Energy, "ESBWR HFE Training Development Implementation Plan," NEDO-33275, Class I (Non-Proprietary)

GE Hitachi Nuclear Energy Procedures and Policies		
Reference Number	Document Title	Abstract
2.a	Work Planning and Scheduling	<p>Defines the process and responsibilities for developing and documenting work plans and schedules for customer-contracted design work and authorized projects.</p> <p>Four key purposes of a Project Work Plan are to define project scope, develop a schedule, monitor progress, and control resources.</p>

Reference Number	Document
4.	GE Hitachi Nuclear Energy, "ESBWR Cyber Security Program Plan," NEDE-33295P, Class III (Proprietary), and NEDO-33295, Class I (Non-Proprietary)
5.	GE Hitachi Nuclear Energy, "ESBWR HFE Training Development Implementation Plan," NEDO-33275, Class I (Non-Proprietary)
6.	Institute of Electrical and Electronic Engineers (IEEE), "Standard Glossary of Software Engineering Terminology," IEEE-610.12-1990
74.	Electric Power Research Institute (EPRI), "Guidelines on Evaluation and Acceptance of Commercial Grade Digital Equipment in Nuclear Safety Applications," EPRI TR-106439
8	GE Hitachi Nuclear Energy, "ESBWR Cyber Security Program Manual," NEDE-33399P, Class III (Proprietary), and NEDO-33399P, Class I (Non-Proprietary)

2.4 ADDITIONAL IEEE STANDARD GUIDANCE

The following IEEE Standards provide additional guidance for the implementation activities. Conformance of the SMPM to these activities has been evaluated. Selected sections/topics from these IEEE Standards are excluded from commitment because they either provide conflicting requirements with other Standards or the level of detail is not appropriate for the SMPM. Clarifications and justifications for such exclusions are provided in Appendix A.

- IEEE-730-2002 - IEEE Standard for Software Quality Assurance Plans

<ul style="list-style-type: none"> • <u>IEEE-610.12-1990 - IEEE Standard Glossary of Software Engineering Terminology</u>
--

- IEEE-1016-1998 - IEEE Recommended Practice for Software Design Descriptions
- IEEE-1058.1-1987 - IEEE Standard for Software Project Management Plans
- IEEE 1219-1998 - IEEE Standard for Software Maintenance
- IEEE 1228-1994 - IEEE Standard for Software Safety Plans
- IEEE 12207-1996 - IEEE/EIA Standard for Software Life Cycle Processes

2.2.3 U.S. Nuclear Regulatory Commission Regulatory Guides

The following codes and standards are applicable to the activities specified within this plan. This Plan conforms to planning requirements of these codes and standards except as explicitly noted in Appendix A.

- RG 1.168-2004, Verification, Validation, Reviews, and Audits For Digital Computer Software Used in Safety Systems of Nuclear Power Plants
- RG 1.169-1997, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
- RG 1.170-1997, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
- RG 1.171-1997, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
- RG 1.172-1997, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
- RG 1.173-1997, Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
- RG 1.152-2006, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants

2.2.4 Institute of Electrical and Electronics Engineers

The following codes and standards are applicable to the activities specified within this plan. This plan conforms to planning requirements of these codes and standards except as explicitly noted in Appendix A.

Where these Institute of Electrical and Electronics Engineers (IEEE) Standards provide recommended implementation techniques and methods, this program makes specific commitments only to those requirements restated hereafter. The ESBWR Project Work Plans shall capture the detailed implementation attributes in accordance with GEH Work Planning and Scheduling [2.3(2a)]. Future exceptions or deviations from the recommendations specified in the IEEE standards shall require management approval as defined in the SMPM [2.3(1)2.3(1.a)] and this SQAPM, and are potentially subject to NRC notification. The NRC notification process is addressed in the MMIS/HFE Implementation Plan [2.1(1)].

- IEEE 7-4.3.2-2003, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations
- IEEE 603-1991 including correction sheet dated January 30, 1995, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations
- IEEE 828-1990, Standard for Software Configuration Management Plans

2.3 SUPPLEMENTAL DOCUMENTS

The following supplemental documents are used in conjunction with the SQAPM and enable the performance of the activities stated in Appendix A.

Reference Number	Document Title	Document Number
1.a	ESBWR Software Management Program Manual (SMPM)	NEDO-33226
1.b	<u>ESBWR Cyber Security Program Plan</u>	<u>NEDO-33295</u>
GE-Hitachi Nuclear Energy Procedures and Policies		
Reference Number	Document Title	Abstract
2.a	Work Planning and Scheduling	Defines the process and responsibilities for developing and documenting work plans and schedules for customer-contracted design work and authorized projects. Four key purposes of a Project Work Plan are to define project scope, develop a schedule, monitor progress, and control resources.
2.b	Product Data Management System (PDMS)	PDMS is the computer-based data system that stores, retrieves, and reports data relevant to the engineering definition of products and services offered and provided to customers. It provides current listings of the engineering documents under formal GEH change control (i.e., engineering controlled documents) that have been approved for issue or application to specific standard, requisition, fuel, and operating plant projects.
2.c	Supplier Design Services Document Review	Defines responsibilities and procedural requirements for review, approval, and control of documentation from suppliers for design services. Supplier submitted documents are entered as elements of the design basis in the Product Data Management System as engineering controlled documents or Design Record Files.
2.d	Engineering Test	Defines the process for specifying, performing, evaluating, and documenting engineering tests.
2.e	Design Review	Defines responsibilities and procedural requirements for conducting formal, design adequacy evaluations. Design Reviews are used to verify that product designs meet customer, functional, contractual, safety, health, environmental, regulatory, industry codes and standards, and corporate requirements.

3.a	Project Risk Management Procedure	Implements the project risk management requirements of GEH Policy. Provides a controlled process for risk management to maintain positive control of work situations, especially during critical tasks or activities.
3.b	Project Management Policy	Provides requirements for the single Project Management process across all GEH. The process components include project initiation, planning, scheduling, execution, controls, and post-delivery closeout.
3.c	Quality Policy and Quality System Requirements	Establishes the requirements of the GEH business quality system. Defines requirements necessary to implement the quality policy and to demonstrate, by performance both inside and outside GEH, total dedication to the attainment of quality leadership and customer satisfaction.
3.d	Nuclear Energy Quality Assurance Audit Requirements	Establishes the requirements and processes for a comprehensive audit program to verify the implementation and effectiveness of the GEH Quality System. The audit program requirements apply to hardware, software and service products and to all personnel who perform quality-related activities on them.
3.e	Reporting of Defects and Noncompliance Under 10 CFR Part 21	Defines the requirements and responsibilities within GEH for ensuring compliance with the requirements of 10 CFR 21, "Reporting of Defects and Noncompliance."

Reference Number	Document Title	Document Number
------------------	----------------	-----------------

4.	IEEE Standard Glossary of Software Engineering Terminology	IEEE 610.12-1990
45.	Guidelines on Evaluation and Acceptance of Commercial Grade Digital Equipment in Nuclear Safety Applications	EPRI TR-106439
6.	ESBWR Cyber Security Program Plan	NEDO-33295

2.4 ADDITIONAL IEEE STANDARD GUIDANCE

The following IEEE Standards provide additional guidance for the implementation activities. Conformance of this plan to these activities has been evaluated. Selected sections/topics from these IEEE Standards are excluded from commitment because either they provide conflicting requirements with other Standards or the level of detail is not appropriate for this plan. Clarifications and justifications for such exclusions are provided in Appendix A.

- IEEE 610.12-1990, IEEE Standard Glossary of Software Engineering Terminology
- IEEE 730-2002, IEEE Standard for Software Quality Assurance Plans
- IEEE 1016-1998, IEEE Recommended Practice for Software Design Descriptions
- IEEE 1058.1-1987, IEEE Standard for Software Project Management Plans
- IEEE 1219-1998, IEEE Standard for Software Maintenance
- IEEE 1228-1994, IEEE Standard for Software Safety Plans
- IEEE 12207-1996, IEEE/Electronic Industries Alliance (EIA) Standard for Software Life Cycle Processes

2.5 INTERNATIONAL STANDARDS

- International Standards Organization (ISO) 9001:2000, Quality Management Systems - Requirements

**Markups for
RAI 7.1-129**

3.0 SOFTWARE MANAGEMENT PLAN

3.1 PURPOSE AND SCOPE

The purpose of the Software Management Plan (SMP) is to establish the managerial process and technical direction for the design and development activities of the Digital Computer-Based I&C Software within the scope of the MMIS/HFE IP [2.1].

3.2 ORGANIZATION

The organization is established to address the control of software management and to ensure independence is maintained between the design organization and the quality assurance, software safety, and Verification and Validation (V&V) organizations. ~~The organization is shown in Figure 3-1.~~

This section describes the following ESBWR organization functions:

1. I&C and Electrical Systems Engineering (I&C/ESE)
2. Software Project Engineering (SPE)
3. Configuration Management Manager (CMM)
4. Software Quality Assurance Manager (SQA Manager)
5. Project Management Team (PMT) (i.e. Project Control)
6. Training

3.2.1 I&C and Electrical Systems Engineering

The I&C software development organization comprises the GEH I&C and Electrical Systems Engineering, the Cyber Security organization and the (GEH and non-GEH) software products vendor organization. The GEH I&C and Electrical System Engineering (I&C/ESE) Organization comprises the I&C and Electrical Systems Engineering Manager (I&C Manager), the platform Technical Project Engineers (TPEs), the Responsible I&C/ESE Engineers and the Cyber Security Team (CyST). This organization implements the activities defined in the SMPM.

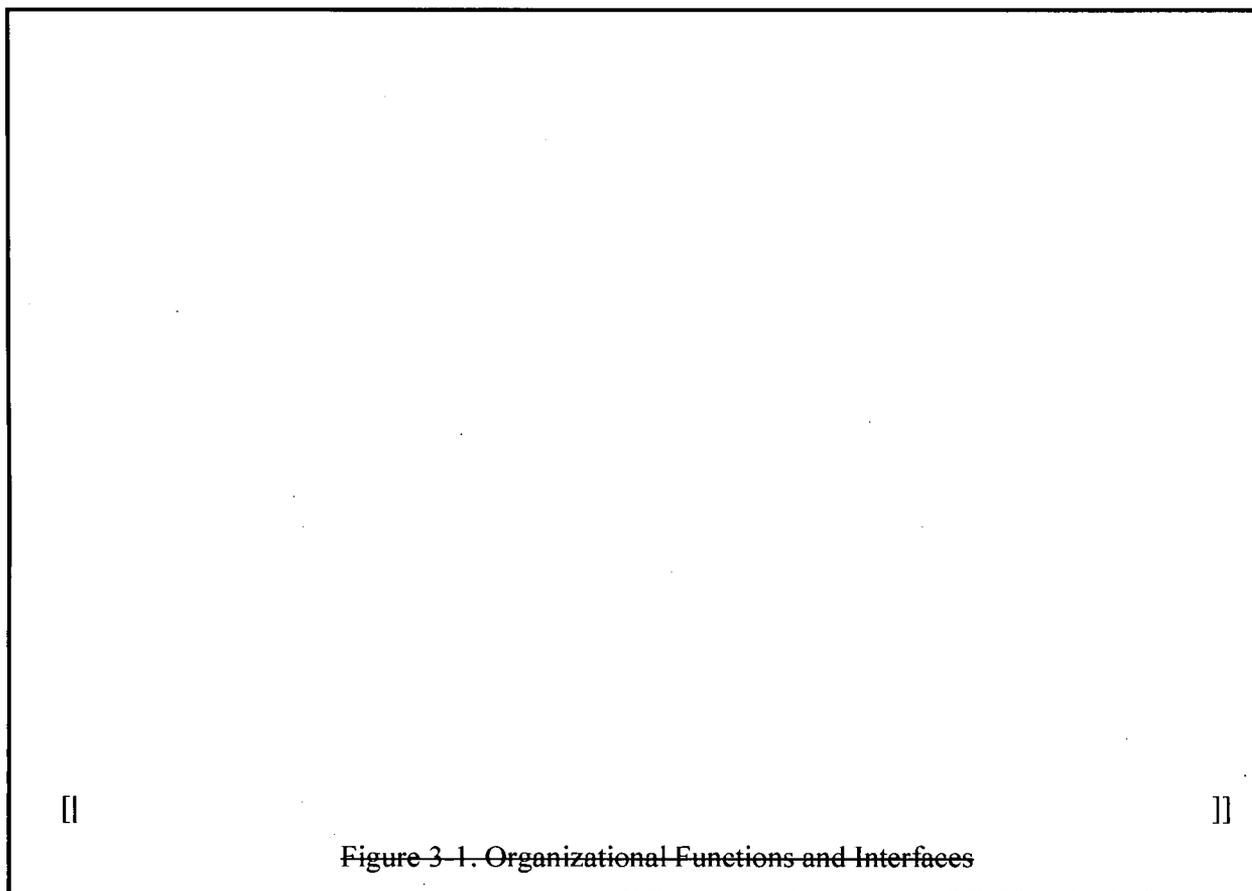
The I&C Manager is responsible for overall performance and schedule of the software development effort, including work flow to the system TPEs, system engineers, and software products vendors. The platform TPEs are responsible for day-to-day management, coordination, and scheduling of the system design and software development effort. They are responsible for interfacing with the system engineers and software product vendors. The platform TPEs are also responsible for providing status reports to the I&C Manager.

The I&C/ESE Engineer is responsible for the design and development of the software products. The I&C/ESE Engineer is responsible for reviewing and confirming that the design

documentation and outputs produced by the software products vendors meet the technical requirements specified in the contract/purchase order.

The software product vendors shall produce the software described in the SMPM. The vendors may be internal or external to GEH and shall be organized such that a single Point of Contact (POC) is assigned the responsibility of interfacing with the TPE. Alternative POCs shall be assigned to take over the duties when the Primary POC is unavailable. The Primary POC and alternative POCs shall be determined by the hardware/software vendor organization and may be any individual within the organization who is qualified to act as the organization's agent. Software developed by the vendors shall be in accordance with the SMPM and the SQAPM [2.3(1)].

The Cyber Security Team (CyST) is responsible for ensuring cyber security of the design, development and evaluation of the Software products throughout the product lifecycle. The CyST is responsible to provide methods to satisfy the cyber security design requirements, methods to assess and validate the actual digital configuration, aid in determining cyber security risks based on the validated configuration and ensure that all necessary cyber security issues are addressed programmatically within the GEH Policy and Procedures to achieve a reasonable level of risk at each ESBWR site for both safety-related and nonsafety-related systems.



9.0 SOFTWARE TRAINING PLAN

9.1 INTRODUCTION

The Software Training Plan (STrngP) describes the software training activities to be carried out before and during the operation of software products for the plant. Software training is performed prior to delivery of the software (System startup and post turn over) and during the O&M phase of the software life cycle. The STrngP addresses the management, implementation and resource characteristics as addressed in BTP-14 [2.2.1]. The STrngP also adheres to the HFE requirements for training as outlined in the HFE/MMIS IP [2.1].

9.1.1 Purpose

The purpose of the STrngP is to define:

- The requirements and methods used in developing the training manual.
- The training needs of appropriate plant staff, including operators, I&C engineers, and technicians.
- A general description of the training facilities.
- The organization supporting the training effort including interfaces and responsibilities.

9.1.2 Scope

The scope of this STrngP is to address the training requirements and documentation for each system or logical group of systems needed to ensure proper operation and use of the software within the overall system. The training requirements include proper usage (e.g., personal safety, system security) of the equipment for the users, operators, maintenance personnel, and management personnel. The SMPM describes the approach for identifying training requirements for use in developing the related training documents.

9.2 ESBWR-TRAINING ORGANIZATION

This section provides a description of the ESBWR Training organization supporting the software product training effort as well as organizational interfaces and responsibilities. **Figure 3-1 shows the relationship of the training organization which reports to GEH Nuclear Services.** The organizational responsibilities are identified in Subsection 3.4. The TSL is a functional position responsible for assignment of personnel to support training for the software products. The Training Services Lead (TSL) is responsible for ensuring the training requirements are accomplished. The training requirements are established based on Licensee needs to generate and maintain the software products. The TSL augments the training staff to support the required training based on the Licensee needs.

3. SOFTWARE QUALITY ASSURANCE PLAN

3.1 PURPOSE AND SCOPE

The purpose of this Software Quality Assurance Plan (SQAP) is to define the management organization, techniques, procedures, and methodologies used to assure the delivery of software which meets specified requirements for the ESBWR I&C Systems. The use of this plan will help assure the following:

- That software development, evaluation and acceptance standards, are implemented, documented, and followed.
- That the results of software quality reviews and audits will be given to appropriate management within the scope of the SQAPM. This provides feedback as to how the development effort is conforming to development standards.
- That test results adhere to acceptance standards.

3.2 MANAGEMENT ORGANIZATION

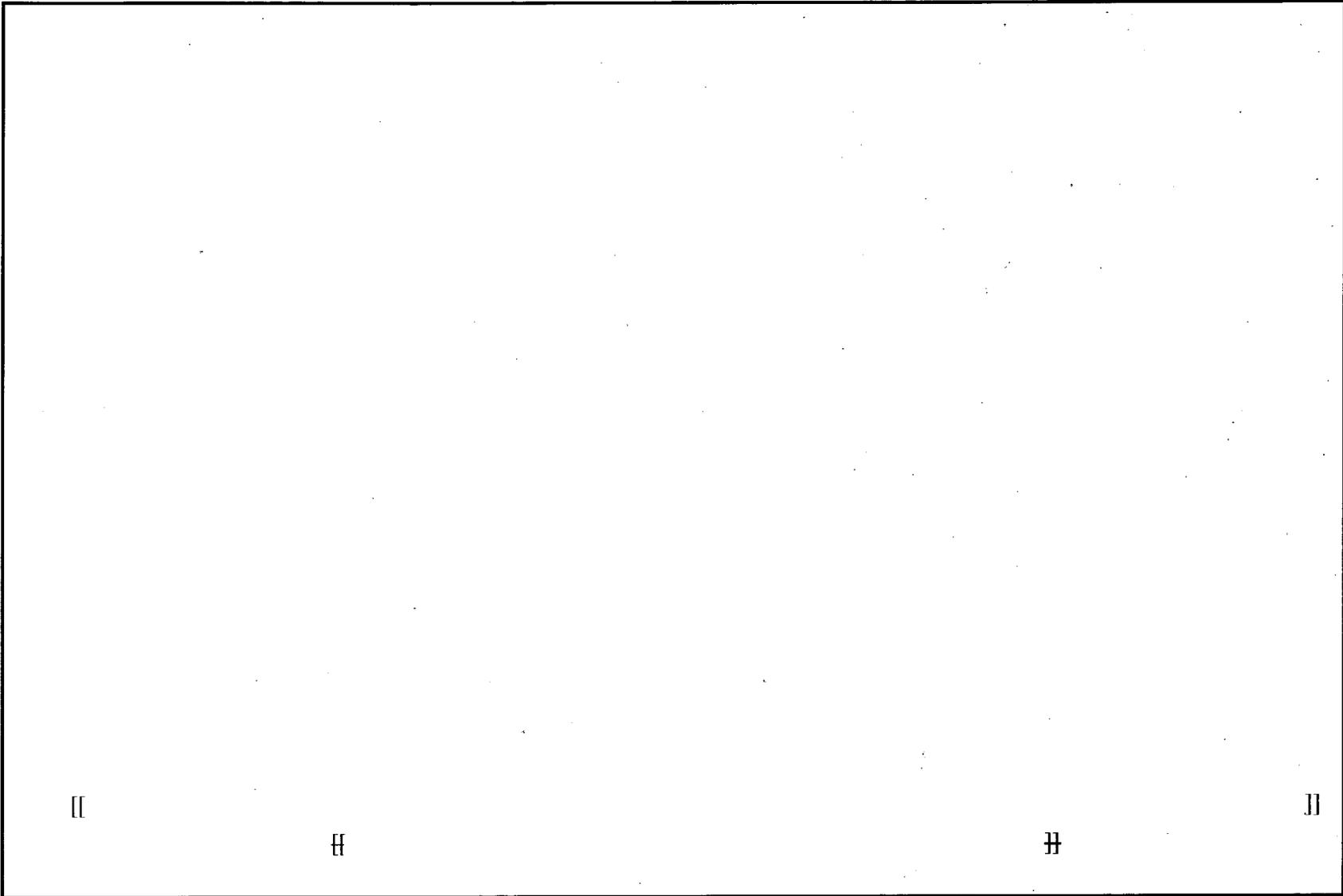
3.2.1 Organization

This section defines the functional responsibilities and authorities of the ESBWR Project organizations that are responsible for the quality of the software products. ~~The organization of the ESBWR Project is shown in Figure 2.~~

The Quality organization is responsible for GEH Quality Assurance (QA) program. The Quality Organization is a managerially and financially independent organization. The Quality Manager, who reports to the President and CEO of GEH, provides leadership for development and overall coordination of the QA program objectives, including the software quality assurance program. The SQA organization has the overall responsibility for developing and maintaining the SQA program with support from the Software Project Engineering (SPE) organization. The SPE organization is responsible for executing the technical aspects of the SQA program, which includes the following SQA tasks (hereafter referred to as Quality tasks):

- Independent Verification and Validation (IV&V) of Software Class Q software
- Software Safety Analysis (SSA)
- Software Configuration Management (SCM)

The SPE organization is technically, managerially, and financially independent from the software products design organization, in conformance with RG 1.168 [2.2.3].



3.2.3.1 Software Quality Assurance Manager

The SQA Manager, who interfaces with the SPE Manager, has the overall responsibility and authority of the SQA Program. The SQA Manager is responsible for:

- Approving this SQAPM
- Approving or rejecting the validated software
- Issuing stop work order if the audit or assessment findings indicate violation of the quality and/or safety requirements
- Organizing the software auditing activities and maintaining the software audit plan
- Participating in baseline reviews
- Scheduling and coordinating software audits (both internally and externally) with the New Plant Project (NPP) Quality Team and/or the Nuclear Quality Assurance Team to ensure effectiveness of the audit being conducted
- Reporting audit results to the responsible project leadership (e.g., SPE Manager, Engineering Manager, Project Management Team) and the Quality Manager

3.2.3.2 New Plant Project Quality Manager

The New Plant Project (NPP) Quality Manager has the overall responsibility and authority of the Quality Program for the ESBWR Project. The NPP Quality Manager shall coordinate with the SQA Manager concerning the audit of the software products. The NPP Quality Manager is responsible for:

- Quality assurance requirements for the design and production of the software products. This includes but is not limited to:
 - Hardware production
 - Hardware qualification
 - Shipping and packaging
 - Final product quality certification
 - Release for shipping approval
- Organization of the auditing activities and maintenance of the audit plan

- | |
|--|
| <ul style="list-style-type: none">• <u>Ensuring independence of the SQA and SPE Organizations from the Design Organization</u> |
|--|

MFN 08-920, Supplement 3

Enclosure 4

Affidavit

GE Hitachi Nuclear Energy Americas LLC

AFFIDAVIT

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

- (1) I am the General Manager, New Units Engineering, GE Hitachi Nuclear Energy ("GEH") and 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 2 of GEH letter MFN 08-920, Supplement 3, Mr. Richard E. Kingston to U.S. Nuclear Regulatory Commission, "Response to Portion of NRC Request for Additional Information Letter No. 257 Related to ESBWR Design Certification Application - Instrumentation & Control Systems - RAI Numbers 7.1-127, 7.1-128, 7.1-129, and 7.1-130," dated December 17, 2008. GEH Proprietary Information is identified in Enclosure 2, "Response to Portion of NRC Request for Additional Information Letter No. 257 Related to ESBWR Design Certification Application - Instrumentation & Control Systems - Licensing Topical Report Markups for RAI Numbers 7.1-127, 7.1-128, 7.1-129, and 7.1-130 - GEH Proprietary Information," in dark red font and a dashed underline inside double square brackets. ~~[[This sentence is an example.....⁽³⁾]]~~ 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 of the proprietary determination. Specific information that is not so marked is not GEH proprietary. A non-proprietary version of this information is provided in Enclosure 3, "Response to Portion of NRC Request for Additional Information Letter No. 257 Related to ESBWR Design Certification Application - Licensing Topical Report Markups for RAI Numbers 7.1-127, 7.1-128, 7.1-129, and 7.1-130 - Non-Proprietary Version."
- (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 2.390(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, or subject to the terms under which it was licensed to GEH. 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 the application of the software plans to the GEH ESBWR.

The development of the evaluation process along with the interpretation and application of the regulatory guidance 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.

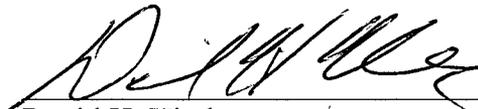
The precise value of the expertise to devise an evaluation process and apply the correct analytical methodology is difficult to quantify, but it clearly is substantial.

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 17th day of December 2008.



David H. Hinds
GE Hitachi Nuclear Energy Americas LLC