



HITACHI

GE Hitachi Nuclear Energy

Richard E. Kingston
Vice President, ESBWR Licensing

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

T 910 675 6192
F 910 362 6192
rick.kingston@ge.com

MFN 08-319, Supplement 1

Docket No. 52-010

August 19, 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. 178 Related to ESBWR Design
Certification Application – RAI Number 7.1-65, Supplement 1**

Enclosure 1 contains GEH's response to the subject NRC RAI transmitted via the Reference 1 letter.

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

Sincerely,

Richard E. Kingston
Vice President, ESBWR Licensing

D068
MRW

Reference:

1. MFN 08-460, Letter from U.S. Nuclear Regulatory Commission to Robert E. Brown, *Request for Additional Information Letter No. 178 Related To ESBWR Design Certification Application*, May 6, 2008

Enclosure:

1. MFN 08-319 Supplement 1 - Enclosure 1 - Response to Portion of NRC Request for Additional Information Letter No. 178 Related to ESBWR Design Certification Application – RAI Number 7.1-65, Supplement 1

cc: AE Cabbage USNRC (with enclosures)
RE Brown GEH/Wilmington (with enclosures)
DH Hinds GEH/Wilmington (with enclosures)
eDRF 0000-0080-0485

MFN 08-319 Supplement 1

Enclosure 1

**Response to Portion of NRC Request for Additional
Information**

**Letter No. 178 Related to ESBWR Design Certification
Application**

RAI Number 7.1-65 Supplement 1

For historical purposes, the original text of NRC RAI 7.1-65 and the GEH response are included below.

NRC RAI 7.1-65

The DCD states the NMS to ATLM and MRBM is an example of a safety-related to non-safety-related communications path that does not involve gateways but does not mention isolation. What are the other safety-related to non-safety related communications paths and how are they isolated?

GEH Response

As stated in Subsection 7.1.3.3 and the response to RAI 7.1-64, submitted via MFN 08-116 dated February 26, 2008, all safety-related communication is electrically, physically, data, and communication isolated and separated at the source using safety-related fiber optic communication interface modules (CIMs), either transmitters or receivers. Thus, regardless of whether a datalink or a combination of datalinks and gateways is used, the required (IEEE Std. 603, Sections 5.6 and 6.3) safety-related isolation and separation are always provided by the safety-related fiber optic CIMs.

See the response to RAI 7.1-56, submitted via MFN 07-560 dated October 24, 2007, for detailed information on the boundary between the Safety-related Distributed Control and Information System (Q-DCIS) and the Nonsafety-related DCIS (N-DCIS) as well as the use of gateways. Subsection 7.1.3.3 describes the use of gateways for data translation or packaging but not for isolation and separation. When a gateway is not needed for data translation or packaging, (as in the case of NMS to ATLM and MRBM communication) there is only a datalink via fiber optic cable between the Q-DCIS CIM and the N-DCIS.

The "other safety-related to nonsafety-related communication" pathways are not listed because the only communication pathways between the Q-DCIS and the N-DCIS are those that pass through the safety-related fiber optic CIMs (which provide the required safety-related isolation), fiber optic cable, datalinks, and in some cases gateways. All data from the Q-DCIS is presented to the N-DCIS. This is indicated in the DCD Tier 2, Revision 4, Subsection 7.1.3.3 statement, "The safety-related communications interfaces indiscriminately retrieve all of the divisional information from the network and send it one way to the nonsafety-related gateway." This statement is modified in the attached markup below to clarify that the divisional information is sent to the N-DCIS, not specifically to the nonsafety-related gateway because gateways are not always used. This transfer of data is always through proper isolation as described above. The N-DCIS is then capable of using the data, which is now nonsafety-related, as needed (e.g., for display, alarm, or recording).

DCD Tier 2, Subsection 7.1.3.3 will be revised to state that the safety-related fiber optic CIMs provide the safety-related isolation and that the CIMs indiscriminately retrieve all of the divisional information from the safety-related (Q-DCIS) networks and send it one way to the N-DCIS.

DCD Impact

DCD Tier 2, Subsection 7.1.3.3 will be revised in Revision 5 as shown below:

The safety-related fiber optic ~~communications interfaces~~ CIMs provide the safety-related isolation. The CIMs indiscriminately retrieve all of the divisional information from the safety-related (Q-DCIS) networks and send it one way to the N-DCIS (via fiber optic cable and a datalink or via a combination of fiber optic cable, datalinks and nonsafety-related gateways. Time tags are described below.

NRC RAI 7.1-65 S01

The RAI response states that the safety-related fiber optic communications interfaces modules (CIMs) provide safety-related isolation. The staff does not consider the use of safety related fiber optic communication transmitter or receiver modules, where the electrical signal is first converted to light, as sole and adequate communication isolation. The staff has provided in DI&C-ISG-04 an acceptable method for implementing communications between a safety and non-safety equipment. Please identify whether the communication isolation will conform to DI&C-ISG-04 and clarify any departures from DI&C-ISG-04.

The RAI response does not identify whether any DAC are applicable to isolation function of the CIMs. If so, this should be explicitly identified in DCD Tier 1, Section 2.2.15.

If DAC are not applicable to the CIMs, the DCD needs to provide design information on the CIMs; in particular, how communication isolation is implemented in or with the CIMs. This discussion should address the criteria in DI&C-ISG-04 or an alternative method identified and justified by GEH. DCD Tier 2, Revision 4, Section 7.1.6.6.1.7 appears to be inconsistent with the response provided to RAI 7.1-65. For example the fourth paragraph of this section states, "Communication from safety-related systems to nonsafety-related systems is carried out with proper signal isolation devices, such as CIMs and fiber optic cable wired network, and data path gateway." This statements (sic.) implies that CIMs are one possible means of communication isolation and not necessarily safety-related. Please clarify the discussion of CIMs in the DCD.

GEH Response

Please identify whether the communication isolation will conform to DI&C-ISG-04. Please clarify any departures from DI&C-ISG-04.

DI&C-ISG-04 provides interim staff guidance for digital communications systems. The ESBWR DCIS design conforms to Staff Position 1 of USNRC DI&C-ISG-04 Section 1, entitled "Interdivisional Communications". The following statement from DCD Tier 2, Rev. 5, Subsection 7.1.3.3.2: "Safety-related system functions do not depend on the correctness or even the existence of the safety-related/nonsafety-related communications", addresses ISG-04, Section 1, Staff Position 1, when applied to communication isolation between safety-related and nonsafety-related equipment. In addition, the following statement from DCD Tier 2, Rev. 5, Subsection 7.1.3.3.2: "Safety-related software is as simple as possible so that Q-DCIS components have neither interrupts from nonsafety-related devices nor do they respond to nonsafety-related component queries for information" addresses DI&C-ISG-04, Section 1, Staff Positions 1, 2, 3, and 8.

The RAI response does not identify whether any DAC are applicable to isolation function of the CIMs. If so, this should be explicitly identified in DCD Tier 1, Section 2.2.15.

Design Acceptance Criteria (DAC) applicable to the isolation function of the safety-related CIMs are part of the safety-related instrumentation and control (I&C) systems' DAC/ITAAC. The DAC/ITAAC applicable to the systems listed in DCD Tier 1, Rev. 5, Table 2.2.10-1, Systems and Functions Comprising the Q-DCIS, are applicable to the CIMs within those systems.

Specifically, IEEE Std. 603 Criteria 5.6 and 6.3 address physical, electrical, and data/communications isolation and separation. As indicated in DCD Tier 1, Rev. 5, Subsection 2.2.15, Instrumentation & Control Compliance with IEEE Std. 603, the safety-related ESBWR I&C systems are designed to the IEEE Std. 603 criteria as listed in Table 2.2.15-1, ITAAC Applicability Matrix. The Tier 1 Table 2.2.15-2, ITAAC for IEEE Std. 603 Compliance Confirmation, item 5 DAC addressing IEEE Std. 603 Criteria 5.6 and 6.3 is applicable to the CIMs within the safety-related ESBWR I&C systems.

If DAC are not applicable to the CIMs, the DCD needs to provide design information on the CIMs; in particular, how communication isolation is implemented in or with the CIMs. This discussion should address the criteria in DI&C-ISG-04 or an alternative method identified and justified by GEH.

As discussed above, DAC are applicable to the CIMs since the CIMs are part of the safety-related system platforms that perform the safety-related functions described in DCD Tier 1, Rev. 5, Table 2.2.10-1.

DCD Tier 2, Revision 4, Section 7.1.6.6.1.7 appears to be inconsistent with the response provided to RAI 7.1-65. For example the fourth paragraph of this section states, "Communication from safety-related systems to nonsafety-related systems is carried out with proper signal isolation devices, such as CIMs and fiber optic cable wired network, and data path gateway." This statement implies that CIMs are one possible means of communication isolation and not necessarily safety-related. Please clarify the discussion of CIMs in the DCD.

The discussion of CIMs has been clarified throughout Chapter 7 of DCD Revision 5 and inconsistencies have been resolved. For example, in the fourth paragraph of DCD Revision 4, subsection 7.1.6.6.1.7, the statement:

"Communication from safety-related systems to nonsafety-related systems is carried out with proper signal isolation devices, such as CIMs and fiber optic cable wired network, and data path gateway"

was reworded to:

"Communication ~~from~~ between safety-related systems ~~to~~ and nonsafety-related systems is carried out via fiber optic cable with through proper the required qualified safety-related signal isolation devices, ~~such as~~ (CIMs) ~~and fiber optic cable wired network~~, and data pathways such as ~~gateways or~~ datalinks and gateways (when necessary)."

This updated statement clarifies that the CIMs are safety-related and provide the communication isolation (it no longer implies that CIMs are only one possible means of communication isolation and not necessarily safety-related).

It is the understanding of GEH that the concern of the NRC staff as presented in this RAI Supplement (7.1-65 S01) is that the safety-related fiber optic communication interface modules (CIMs) are not sufficient "as sole and adequate communication isolation". This is potentially due to insufficient explicit explanation in previous (prior to Rev. 5) revisions of the ESBWR Design Control Document (DCD). In order to address this concern, the following actions were taken.

Reference to the software plans ("ESBWR I&C Software Management Plan," NEDO-33226, NEDE-33226P, and "ESBWR I&C Software Quality Assurance Plan" NEDO-33245, NEDE-33245P) were added to the last paragraph of Subsection 7.1.3.3.1,

“Safety-Related Isolation”. The updated statement, “These protocols are governed by References 7.1-10 and 7.1-12 and control the transmission, acceptance, and authentication of data from outside the division so that these communications cannot adversely affect the operation or safety-related functions of that division”, is intended to highlight the method required in the development of Q-DCIS software which will ensure the necessary isolation.

In addition, DCD Rev. 5, Subsection 7.1.3.3, “Q-DCIS Safety Evaluation”, was reorganized in order to more clearly present information related to Distributed Control and Information System (DCIS) communications.

DCD Figure 7.1-1, ESBWR Instrumentation and Control Simplified Block Diagram, shows a simplified functional block diagram of the DCIS instrumentation and controls. While “Comm. Interfaces” are shown as a separate box interfacing the Q-DCIS and N-DCIS, it is only a functional representation; safety-related CIMs are not located in their own separate cabinets/enclosures. DCD Figure 7.1-2, ESBWR Distributed Control and Information System (DCIS) Functional Network Diagram, does not show the CIMs because they are part of the Q-DCIS equipment (not separate boxes) and are located within the safety-related DCIS cabinets (RTIF, NMS, & SSLC/ESF).

DCD Impact

DCD Tier 2, Subsection 7.1.3.3, Revision 5 was reworked for clarity with specific reference made in Subsection 7.1.3.3.1, Safety Related Isolation, to the software plans (the SMP & SQAP), as a preemptive measure to highlight information presumed to address the concern(s) of the NRC staff.

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