

---

## AMENDED RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

---

06/03/2015

**US-APWR Design Certification  
Mitsubishi Heavy Industries  
Docket No.52-021**

**RAI NO.:** 1076-7368  
**SRP SECTION:** 07.09 – Data Communication Systems  
**APPLICATION SECTION:** 07.09 – Data Communication Systems  
**DATE OF RAI ISSUE:** 2/5/2014

---

**QUESTION NO.: 07.09-27**

Background

The staff issued RAI 992-6999, Question 07.09-26 requesting the applicant to address the compliance with GDC 24 and IEEE Std. 603-1991. In summary, the staff requested the applicant to provide the following:

1. Sufficient evidence associated with the HFE full scope simulator testing or a quantitative analysis to demonstrate that the use of operational visual display unit (O-VDU) to operate safety equipment enhances the performance of the safety function.
2. An ITAAC that adequately verifies testing for normal and abnormal data transmission conditions for all non-safety to safety interfaces.

The applicant responded to this RAI in two parts:

Response Part 1:

In the RAI response Part 1, dated August 26, 2013 (ML13240A040), the applicant stated, in parts, that the full scope simulator testing with U.S. operators was performed to show reduced time required and improved situation awareness when operators managed accident scenarios using O-VDUs, compared to the same accident management using only Safety-VDUs (S-VDUs).

New Appendix I of MUAP-07004 shows the results of time required analysis using operational sequence diagram patterns for the operation of a main steam isolation valve, which is one of typical risk-important and credited operator actions in the safety analysis, and also performed in normal operation for plant shutdown. The results show that the time required to complete these actions is reduced by almost half using only O-VDUs for both safety-related and non-safety monitoring and controls, compared to using both O-VDUs and S-VDUs.

In conclusion, the applicant stated that the reduction of response time and operator's workload by utilizing O-VDUs to control both safety-related and non-safety systems will contribute to plant safety.

#### Response Part 2:

In the RAI Response Part 2, dated November 1, 2013 (ML13308C479), the applicant stated, in parts, that regarding manual controls of safety-related components from O-VDUs, the following functions will be verified by existing ITAAC to ensure normal data transmission for manual operations from O-VDUs:

- (1) Manual operations of the safety-related components from O-VDUs
- (2) Priority logic between S-VDUs and O-VDUs (i.e., overrides of O-VDU by S-VDU)
- (3) Priority logic between safety signals and O-VDUs (i.e., overrides by safety signal)
- (4) Disable manual operations of safety-related components from O-VDUs by safety-related disable switch on S-VDUs

Also, the applicant proposed the addition of new acceptance criteria 6.iii to Tier 1, Table 2.5.6-1, ITAAC #6 to verify that the communication processors used for the DCS can mitigate all the design-basis communication faults and technical report MUAP-07005-P was revised to include an appendix that documents the design-basis communication faults analyses.

#### Staff Evaluation

The staff evaluation of the response to RAI 992-6999, Question 07.09-26 is summarized as follow:

1. Time to complete an action is generally not accepted as a direct measure of safety improvement. However, it can be used to help determine that an action can be reliably performed within the analysis limits, which in turn is used to support a safety conclusion. Therefore, the staff found that the Response Part 1 is reasonable and acceptable.
2. The staff found that the Response Part 2 is not fully acceptable for the following reasons:
  - On Page 07.09-3 of the response, the applicant stated that "The tests of the as-built PSMS [safety systems] as described in ITAAC#4 of Table 2.5.1-6 will be conducted to demonstrate that all normal data transmission conditions. These test results will adequately demonstrate that the DCS can mitigate the design-basis communication faults results in abnormal data transmission conditions, and can perform all required normal data transmission conditions from all non-safety systems to PSMS." In this statement, the first sentence is incomplete and the second sentence is not clear. It is not clear how the result of ITAAC#4 of Table 2.5.1-6, which requires tests to be performed to verify normal data transmission, can be used to demonstrate that the DCS can mitigate the design-basis communication faults results in abnormal data transmission

- conditions.
- The Tier 1, Table 2.5.6-1, ITAAC #6 proposed acceptance criteria 6.iii, is not adequate to address the staff request. There is no design commitment made to demonstrate that all possible design-basis communication faults are identified and mitigated. In addition, the proposed ITAAC does not call for performing any tests (or type tests) for verifying this design commitment.

Follow-up RAI:

The staff found that the response is partially unacceptable and in this follow-up RAI requests the applicant to provide the following:

1. Explanation of the statement in the Part 2 response to RAI 992-6999, “The tests of the as-built PSMS [safety systems] as described in ITAAC#4 of Table 2.5.1-6 will be conducted to demonstrate that all normal data transmission conditions. These test results will adequately demonstrate that the DCS can mitigate the design-basis communication faults results in abnormal data transmission conditions, and can perform all required normal data transmission conditions from all non-safety systems to PSMS.” In this statement, the first sentence is incomplete, and the second sentence is not clear how the result of ITAAC#4 of Table 2.5.1-6, which requires tests to be performed to verify normal data transmission, can be used to demonstrate that the DCS can mitigate the design-basis communication faults results in abnormal data transmission conditions.
2. A revision of ITAAC#6 or a new ITAAC to address the staff concern as discussed in the second bullet of Part 2 of the Staff Evaluation section above. This ITAAC should include (a) design commitment, (b) inspections, tests, analyses, and (c) acceptance criteria. The design commitment section should at least clearly state that digital communication independence is achieved by communication processors that can mitigate all identifiable design-basis communication faults. The inspections, tests, analyses section should include tests (or type tests) being performed for each design-basis communication fault.
3. A description in Section 7.9 of DCD Tier 2 of the design-basis communication faults and a reference to technical report MUAP-07005-P for the details.

---

**ANSWER:**

**Response to Item 1**

The first statement in question, “The tests of the as-built PSMS as described in ITAAC#4 of Table 2.5.1-6 will be conducted to demonstrate that all normal data transmission conditions,” is a typographical error on MHI’s behalf. MHI communicated in the second paragraph of the response to part two of RAI 992-6999 that all normal data transmission conditions from non-safety to safety interfaces is confirmed through as-built tests of the PSMS as described in various referenced ITAAC.

The referenced sentence, “These test results will adequately demonstrate that the DCS can mitigate the design-basis communication faults results in abnormal data

transmission conditions, and can perform all required normal data transmission conditions from all non-safety systems to PSMS,” was meant to follow the sentence which preceded the typographical error discussed above.

The seventh paragraph of the response to part two of RAI 992-6999 was intended to be written as the following:

“Compliance with the ISG-04 regarding communication faults is achieved through the MELTAC platform (hardware and basic software) which has been adequately analyzed, and the results are described in MUAP-13018 (JEXU-1015-1009 will be resubmitted as MHI document MUAP-13018), ISG-04 Conformance Analysis Technical Report. Tests of the MELTAC platform will be conducted to demonstrate that the data communication system (DCS) can mitigate all the design-basis communication faults that result in the abnormal data transmission conditions listed in Attachment 2-2 which covers all communication faults described as example in ISG-04 Staff Position 1.12. ~~The tests of the as-built PSMS [safety systems] as described in ITAAC#4 of Table 2.5.1-6 will be conducted to demonstrate that all normal data transmission conditions.~~ These MELTAC platform test results will ~~adequately~~ demonstrate that the DCS can adequately mitigate the design-basis communication faults that results in abnormal data transmission conditions, and can perform all required normal data transmission conditions from all non-safety systems to safety systems (PSMS).”

### **Response to Item 2**

MHI will delete ITAAC#6.iii and add ITAAC#7 to Table 2.5.6-1, as shown in Attachment-1. The addition verifies digital communication independence is achieved by the PSMS that can mitigate all identifiable design-basis communication faults of the other PSMS divisions and the non-safety DCS. Also, the inspections, tests, analyses section indicates type tests are to be performed for each design-basis communication fault of the other PSMS divisions and the non-safety DCS.

### **Response to Item 3**

MHI will add a description of the design-basis communication faults and a reference to technical report MUAP-07005 to Section 7.9 of DCD Tier 2, as shown in Attachment-2.

Also, the descriptions of Appendix H of MUAP-07005 will be revised to add clarity and detail regarding the design-basis communication faults and the fault mitigation functions of the PSMS, as shown in Attachment-3. The related descriptions of MUAP-13018 will also be revised to follow the MUAP-07005 changes, as shown in Attachment-4.

### **Additional Item-1**

MHI recognizes that some additional descriptions related to the data communication design descriptions throughout DCD Tier 2 Chapter 7 and related technical reports should be included for clarity as follows:

Appendix G “The FMEA for PSMS” of MUAP-07004, Revision 8, “Safety I&C System Description and Design Process” describes that the failure mode of “valid but frozen data” in the communication part of the RPS and ESFAS are detected by manual periodic testing. However, there is no description in DCD Tier 2, Chapter 7 and the related

technical reports of how to detect the failure mode of “valid but frozen data” in the communication part of the RPS and ESFAS by manual periodic testing.

MHI plans to perform the manual periodic test to detect the failure mode of “valid but frozen data” using the memory integrity check (MIC) since the failure mode can potentially occur in the 2-port memory circuit on the Control Network I/F Module and the Bus Master Module. MHI believes the test description in DCD Chapter 7 and MUAP-07005 should also describe this test method for improved understanding, not just in the FMEA description in MUAP-07004.

Therefore, MHI will add descriptions of the memory integrity check to DCD Tier 2, Chapter 7, MUAP-07004 and MUAP-07005, as shown in Attachments-5, 6 and 7.

### **Additional Item-2**

The NRC provided the following clarification regarding the communication faults mitigation functions of the PCMS during the NRC audit in the week of November 17<sup>th</sup>, 2014;

- (Item 2-1): The number of operational commands (eight (8) for the US-APWR) from the operational VDU to the PSMS at every communication cycle of the unit bus in the DCD Tier2 Chapter 7.
- (Item 2-2): Clearly describe the non-safety HSI system in PCMS consisting of the MR computer platform, and the quality requirements (augmented quality requirements) for the MR computer platform which are the same as the non-safety MELTAC platform for PCMS (Note).  
Note) Appendix C of MUAP-07004 describes that the operational VDU consists of the MR series processor, but it does not clearly describe the quality requirements.

Based on Item 2-1, MHI will add descriptions on the number of operational VDU commands (8) to DCD Tier 2 Chapter 7, as shown in Attachment-8. Also, the related descriptions of Appendix E of MUAP-7004 are revised to follow the DCD Tier 2 Chapter 7 changes, as shown in Attachment-9.

Based on Item 2-2, MHI will add descriptions on the MR computer platform to DCD Tier 2 Chapter 7, as shown in Attachment-10. Also, the description of Appendix C of MUAP-07004 is revised to keep consistency with the name of the MR computer platform, as shown in Attachment-11.

### **Additional Item-3**

The NRC provided the following clarification regarding Bypass, Lock, Reset and maintenance trip commands from the operational VDU during the NRC audit in the week of November 17<sup>th</sup>, 2014 and the follow-up teleconference;

- (Item 3-1): All types of operational VDU commands to PSMS in DCD Tier 2 Chapter 7.
- (Item 3-2): Clarity for the descriptions and figures of MUAP-07004 regarding the priority logics of the Bypass, Lock, Reset and maintenance trip command from the operational VDU.

- (Item 3-3): The descriptions of Appendix I of MUAP-07004 demonstrate that the operation commands from the operational VDU enhance the performance of safety functions and comply with ISG-04 Staff Position 1.3, but there are no evaluation on the Bypass, Lock, Reset and maintenance trip commands from the operational VDU. Demonstrate conformance to ISG Staff Position 1.3 on the Bypass, Lock, Reset and maintenance trip commands from the operational VDU.
- (Item 3-4): Conformance evaluation to ISG Staff Position 3.1.3 regarding the Bypass, Lock, Reset and maintenance trip commands from the operational VDU in Appendix E of MUAP-07004.
- (Item 3-5): Check if the following information is described in the licensing documents and add if necessary;
  - (1) Legends for latch symbols, including R-S block latch symbol and one input latch symbol
  - (2) Default setting and dominance of latch for each permissive/bypass/lock function from the operational VDU
  - (3) Operation meanings of unlock
  - (4) Permissive allowing all bypass/lock functions in the train
  - (5) Latch for maintenance bypass signal (2-out-of-4 bypass logic)

Based on Item 3-1, MHI will add descriptions and a table to describe all types of the commands from the operational VDU to PSMS in DCD Tier 2 Chapter 7, as shown in Attachment-12.

Based on Item 3-2, MHI will revise and add clear descriptions and figures of the priority logics for the commands from the operational VDU to MUAP-07004, as shown in Attachment-13. For the maintenance trip command, the maintenance trip command from the operational VDU is assigned to the "Operation" command type as shown in the "Maintenance Trip" row on Table 7.7-6 "Manual Command Signals from O-VDU to PSMS" in Attachment-12.

[

]

Based on Item 3-3, MHI will add the descriptions for the conformance evaluation to ISG-04 Staff Position 1.3 in Section I.2 of MUAP-07004 Appendix I, as shown in Attachment-14, and add the related description of Appendix E of MUAP-07004 on ISG-04 Staff Position 1.3 evaluation is also revised, as shown in Attachment-15. The descriptions in Attachment-14 (mark-up of Appendix I of MUAP-07004) also reflect the NRC Staff's comments and requests which were provided at the follow-up teleconference after the NRC audit in the week of November 17<sup>th</sup>, 2014.

Based on Item 3-4, MHI will revise the conformance evaluation to ISG-04 Staff Position 3.1.3 in Appendix E of MUAP-07004, as shown in Attachment-16. The revised

conformance evaluation will include the evaluation on the maintenance trip, etc. in the Analysis Item-1 "Priority logic for the manual operational commands" in Attachment-16.

For Item 3-5, MHI will revise MUAP-07004 and include the necessary information in Attachment-13. For the latch symbol with two inputs (i.e., set and reset), MHI confirmed that this is defined as "MEMORY" in Figure 1.7-2 in DCD Chapter 1. This latch symbol will be uniquely used for the latch symbol with two inputs in DCD Chapter 7 and related reports, and R-S block latch symbol in Figure 5.1-6 of MUAP-07004 will be replaced with the latch symbol defined in DCD Chapter 1.

#### **Additional Item-4**

The NRC provided feedback comments and requests to MHI at the follow-up teleconference after the NRC audit in the week of November 17<sup>th</sup>, 2014. The following items are added to this RAI response and document markups as a result;

(Item 4-1): Item to address FPGA versus hardware in the application (e.g. Hardware Arbitration Interlock). Only addressed for WDT.

(Item 4-2): [

]

(Item 4-3): [

]

(Item 4-4): Does the safety CPU module receive any process signal data from the control systems?

(Item 4-5): [

]

(Item 4-6): [

]

(Item 4-7): [

]

(Item 4-8): [

]

(Item 4-9): [

]

(Item 4-10): [

]

(Item 4-11): [

]

(Item 4-12): [

]

(Item 4-13): [

]

(Item 4-14): [

]

(Item 4-15): [

]

(Item 4-16): [

]

(Item 4-17): [

]



(Item 4-18): [

]

- (Item 4-19): Are spurious actuations of multiple trains of safety equipment due to CCF of PSMS addressed in the application?
- (Item 4-20): Does the application contain descriptions of the specific maintenance activities that would require the connection of MELTAC Engineering Tool, the process for connecting this engineering tool to the controller, and any changes to the modes of operation for controller that is connected?
- (Item 4-21): What communication protocol is used on the WNET and what software programming language is used to program the data communications error detection features?

#### **Response to Additional Item 4-1**

The DCD and Technical Reports using “hardware” for the special meaning that the logic consist of hardwired circuits without any software will be revised to “hardwired”, as shown in Attachments-3, 4, 17 and 18.

The DCD and Technical Reports use of “hardware” is only to differentiate from “software”, such as “hardware specification” and “hardware failure”. MHI will continue to use “hardware” for these cases.

#### **Response to Additional Item 4-2**

The DCD and associated Technical Reports are reviewed for terms like “multiple spurious commands” to confirm the use is appropriate and in alignment with the CCF analysis in Appendices D and J of MUAP-07004, and will be revised as shown in Attachments-19 and 20.

#### **Response to Additional Item 4-3**

The description on the over-length message will be added in Section 3.2.1 Table of MUAP-13018, WNET-8 as shown in Attachment-4.

#### **Response to Additional Item 4-4**

The safety CPU of the PSMS receives some type of process signals, such as non-safety grade sensor signals, from the non-safety I&C systems. However, the PSMS receives these signals by using the hardwired interfaces (e.g., 4-20mA signal) via hardwired cables and analog input modules. The PSMS does not receive any process signals (analog signals) data from the non-safety PCMS via the data communication (unit bus) interface. The description to explain above issues will be added in Subsection 7.9.1.1.2 “Unit Bus” of the DCD Chapter 7 as shown in Attachment-21.

#### **Response to Additional Item 4-5**

The description on the destination node ID will be added in No.13 of MUAP-13018 Table 3.5-4 as shown in Attachment-4.

**Response to Additional Item 4-6**

[

]

The description to explain above condition will be added in No.24-26 of MUAP-13018 Table 3.5-4 as shown in Attachment-4.

**Response to Additional Item 4-7**

[

]

**Response to Additional Item 4-8**

[

]

**Response to Additional Item 4-9**

[

]

**Response to Additional Item 4-10**

[

]

**Response to Additional Item 4-11**

[

]

**Response to Additional Item 4-12**

[

]

**Response to Additional Item 4-13**

[

]

**Response to Additional Item 4-14**

[

]

**Response to Additional Item 4-15**

[

]

**Response to Additional Item 4-16**

[

]

**Response to Additional Item 4-17**

[

]

**Response to Additional Item 4-18**

[

]

**Response to Additional Item 4-19**

The operational VDU has capability to manually control multiple trains (all four trains) of the safety equipment. The spurious actuations of multiple trains of safety equipment due to a failure (CCF) of the operational VDU are analyzed in Appendix J.3 "Events Initiated

by Operational VDU Failures” of MUAP-07004. This analysis assumes spurious actuations of multiple trains of safety equipment, and also covers spurious actuations of multiple trains of safety equipment due to CCF of the PSMS.

**Response to Additional Item 4-20**

The MELTAC Engineering Tool (maintenance tool) is normally disconnected from the PSMS, and can only be connected to one PSMS train under control of the T-Spec. If the MELTAC Engineering Tool is connected to the PSMS for maintenance activities, an alarm is initiated in the Main Control Room. The MELTAC Engineering Tool can monitor the conditions of the PSMS controller and can change field changeable process values in the data table while in normal operation mode. The PSMS software can only be changed by removing the CPU module from the on-line controller chassis. The details on the MELTAC Engineering Tool are described in Sections 4.1.4.1 and 4.3.4 of MUAP-07005.

**Response to Additional Item 4-21**

An original protocol cycle communication is implemented on the RPR protocol according to IEEE std 802.17, as described in Section 4.3.2.2 of MUAP-07005.

[

]

**Impact on DCD**

ITAAC#6.iii is to be deleted and ITAAC#7 is to be added to DCD Tier 1 Table 2.5.6-1, as shown in Attachment-1.

Descriptions for the design-basis communication faults are added in DCD Tier 2, Section 7.9, as shown in Attachment-2.

Descriptions of the memory integrity check functions to verify the 2-port memory circuit on the Control Network I/F Module and the Bus Master Module are added to Section 7.1 of DCD Tier 2, as shown in Attachment-5.

Descriptions of the number of operational commands from the operational VDU to the PSMS are added in DCD Tier 2, Section 7.1, as shown in Attachment-8.

Descriptions of the MR computer platform are added in DCD Tier 2, Section 7.1, as shown in Attachment-10.

Descriptions and the table of the all types of the commands from the operational VDU are added in DCD Tier 2, Section 7.7, as shown in Attachment-12.

The use of “hardware” to identify hardwired circuits is revised to clearly describe the use of hardwired circuits in DCD Tier 2, Chapter 7, as shown in Attachment-17.

The descriptions to explain “multiple spurious commands from the operational VDU” are corrected in DCD Tier 2, Chapter 7 to keep consistency with Appendices D and J of MUAP-07004, as shown in Attachment-19.

Descriptions of process signals from the non-safety I&C systems to the PSMS are added in Subsection 7.9.1.1.2 of the DCD Chapter 7 as shown in Attachment-21.

**Impact on R-COLA**

There is no impact on the R-COLA.

**Impact on PRA**

There is no impact on the PRA.

**Impact on Technical / Topical Report**

The descriptions on the design-basis communication faults and the fault mitigation functions of the PSMS in Appendix H of MUAP-07005 are revised, as shown in Attachment-3. The related descriptions of MUAP-13018 are also revised to follow the MUAP-07005 changes, as shown in Attachment-4. Detail descriptions related to the data communication items are also added to MUAP-13018, as shown in Attachment-4.

Descriptions for the memory integrity check functions to verify the 2-port memory circuit on the Control Network I/F Module and the Bus Master Module are added to Subsection 4.4.1 of MUAP-07004, as shown in Attachment-6.

Descriptions for the memory integrity check of the data communication model are added to Subsection 4.1.5 and 4.1.7.2 of MUAP-07005, as shown in Attachment-7.

Descriptions of the number of operational commands from the operational VDU to the PSMS to comply with ISG-04 Staff Position 1.7 are added in Appendix E of MUAP-07004, as shown in Attachment-9.

The description of the MR computer platform is revised in Appendix C of MUAP-07004, as shown in Attachment-11.

The descriptions and the figures on the priority logics of the command from the operational VDU are revised and added to Section 5.1.14 of MUAP-07004, as shown in Attachment-13.

The conformance evaluation to ISG-04 Staff Position 1.3 on the Bypass, Lock and Reset commands from the operational VDU is added in Appendix I of MUAP-07004, as shown in Attachment-14, and the related description of Appendix E of MUAP-07004 on ISG-04 Staff Position 1.3 evaluation is also revised, as shown in Attachment-15.

The conformance evaluations to ISG-04 Staff Position 3.1.3 in Appendix E of MUAP-07004 are revised to clearly describe on the priority logics of the Bypass, Lock and Reset commands from the operational VDU, as shown in Attachment-16.

The use of “hardware” to identify hardwired circuits is revised to clearly describe the use of hardwired circuits in MUAP-07004, as shown in Attachment-18.

The descriptions to explain “multiple spurious commands from the operational VDU” are corrected in MUAP-07004 to keep consistency with Appendices D and J of MUAP-07004, as shown in Attachment-20.