US-APWRRAIsPEm Resource

From: Ward, William
Sent: Tuesday, March 15, 2016 5:11 PM
To: 'us-apwr-rai@mhi.co.jp'; US-APWRRAIsPEm Resource; Joe Tapia
Cc: Zhang, Deanna; Taneja, Dinesh; Ward, William; Williams, Donna
Subject: US-APWR Design Certification Application RAI 1097-8499 (7.1 Instrumentation and Controls - Introduction)
Attachments: US-APWR DC RAI 1097 ICE 8499.pdf

MHI,

The attachment contains the subject request for additional information (RAI). This RAI was sent to you in draft form. Your licensing review schedule assumes technically correct and complete responses within 30 days of receipt of RAIs. However, MHI requests, and we grant, 60 days to respond to this RAI. We will adjust the schedule accordingly.

Please submit your RAI response to the NRC Document Control Desk.

Thank you,

William R. Ward, P.E.
Senior Project Manager
U.S. Nuclear Regulatory Commission
m/s T6-D38M
Washington, DC, 20555-0001
NRO/DNRL/Licensing Branch 2
ofc T6-D31
ofc (301) 415-7038

Hearing Identifier: Mitsubishi_USAPWR_DCD_eRAI_Public
Email Number: 168

Mail Envelope Properties (44675ec914184218a5fe4e082e704635)

Subject: US-APWR Design Certification Application RAI 1097-8499 (7.1 Instrumentation and Controls - Introduction)
Sent Date: 3/15/2016 5:10:49 PM
Received Date: 3/15/2016 5:10:51 PM
From: Ward, William

Created By: William.Ward@nrc.gov

Recipients:
"Zhang, Deanna" <Deanna.Zhang@nrc.gov>
Tracking Status: None
"Taneja, Dinesh" <Dinesh.Taneja@nrc.gov>
Tracking Status: None
"Ward, William" <William.Ward@nrc.gov>
Tracking Status: None
"Williams, Donna" <Donna.Williams@nrc.gov>
Tracking Status: None
"'us-apwr-rai@mhi.co.jp'" <us-apwr-rai@mhi.co.jp>
Tracking Status: None
"US-APWRRAIsPEm Resource" <US-APWRRAIsPEm.Resource@nrc.gov>
Tracking Status: None
"Joe Tapia" <joseph_tapia@mnes-us.com>
Tracking Status: None

Post Office: HQPWMSMRS05.nrc.gov

Files	**Size**	**Date & Time**
MESSAGE	792	3/15/2016 5:10:51 PM
US-APWR DC RAI 1097 ICE 8499.pdf	90990	

Options
Priority: Standard
Return Notification: No
Reply Requested: No
Sensitivity: Normal
Expiration Date:
Recipients Received:

REQUEST FOR ADDITIONAL INFORMATION 1097-8499

Issue Date: 03/15/2016
Application Title: US-APWR Design Certification - Docket Number 52-021
Operating Company: Mitsubishi Heavy Industries
Docket No. 52-021
Review Section: 07.01 - Instrumentation and Controls - Introduction
Application Section:

QUESTIONS

07.01-47

Clarify whether there is bypassed or inoperable status indications (BISI) for components locked from the non-safety operational Video Display Unit (VDU) on the Large Display Screen (LDP). 10 CFR 50.55a(h)(3) states, in part, that application filed on or after May 13, 1999, for design certifications must meet the requirements for safety systems in IEEE Std. 603-1991 and the correction sheet dated January 30, 1995. IEEE Std 603-1991, Clause 5.8.3, states, "If the protective actions of some part of a safety system have been bypassed or deliberately rendered inoperative for any purpose other than an operating bypass, continued indication of this fact for each affected safety group shall be provided in the control room." IEEE Std 603-1991 defines maintenance bypass as the "removal of the capability of a channel, component, or piece of equipment to perform a protective action due to a requirement for replacement, repair, test, or calibration."

[

PROPRIETARY INFORMATION WITHHELD

]

Based on the definition of a maintenance bypass and the requirements of IEEE Std 603-1991, Clause 5.8.3, BISI should be provided for locked components at the component level. Further, there appears to be a discrepancy between Technical Report MUAP-07004, Section 5.1.13 and the response to RAI 7368, Question 07.09-27 with respect to whether BISI is provided for locked components on the LDP. As such, the staff requests the applicant to demonstrate how the requirements of IEEE Std 603-1991, Clause 5.8.3 are met, and resolve any discrepancy between Technical Report MUAP-07004, Section 5.1.13 and the response to RAI 7368, Question 07.09-27.

REQUEST FOR ADDITIONAL INFORMATION 1097-8499

07.01-48

Provide additional design information to demonstrate that the software used to implement the watchdog timer (WDT) will not be susceptible to the same failure as the software used to implement the safety bus master module and DO module.

10 CFR 50.55a(h)(3) states, in part, that application filed on or after May 13, 1999, for design certifications must meet the requirements for safety systems in IEEE Std. 603-1991 and the correction sheet dated January 30, 1995. IEEE Std 603-1991, Clause 5.5, states “The safety systems shall be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis.” Clause 5.7 of this standard states, in part, “Capability for testing and calibration of safety system equipment shall be provided while retaining the capability of the safety systems to accomplish their safety functions.” Branch Technical Position (BTP) 7-21, “Guidance on Digital Computer Real-Time Performance,” NUREG-0800, Standard Review Plan (SRP), Appendix 7.1-C, “Guidance for Evaluation of Conformance to IEEE Std. 603,” and NUREG-0800, SRP Appendix 7.1-D, “Guidance For Evaluation of The Application of IEEE Std 7-4.3.2,” provide guidance on how to meet the requirements IEEE Std 603-1991, Clauses 5.5 and 5.7. BTP 7-21, in "Use of Cyclic Real-Time Executive," states, “A basis should be provided that describes the cycle and demonstrates that the watch-dog timer is correctly implemented, the time required for the application modules does not exceed the allotted time given in the architecture timing budget, and diagnostic and other support modules will not cause the allotted time to be exceeded.” SRP Appendix 7.1-C, section 5.5, states, “The review of system integrity should confirm that the design provides for safety systems to fail in a safe state, or into a state that has been demonstrated to be acceptable on some other defined basis, if conditions such as disconnection of the system, loss of energy, or adverse environments, are experienced.” SRP Appendix 7.1-D, section 5.7, states “A non-software watchdog timer is critical in the overall diagnostic scheme. A software watchdog will fail to operate if the processor freezes and no instructions are processed. The reviewer should look for a hardware watchdog timer whose only software input is reset after the safety processor completes its function.”

[

PROPRIETARY INFORMATION WITHHELD

]

REQUEST FOR ADDITIONAL INFORMATION 1097-8499

1. [

PROPRIETARY INFORMATION WITHHELD

]

2. [

PROPRIETARY INFORMATION WITHHELD

]

3. [

PROPRIETARY INFORMATION WITHHELD

]

REQUEST FOR ADDITIONAL INFORMATION 1097-8499

07.01-49

Provide additional design details regarding data communications between the operational video display unit (O-VDU) to the protection and safety monitoring system (PSMS), and between redundant divisions of the PSMS.

10 CFR 50.55a(h)(3) states, in part, that application filed on or after May 13, 1999, for design certifications must meet the requirements for safety systems in IEEE Std. 603-1991 and the correction sheet dated January 30, 1995. IEEE Std 603-1991, Clause 5.6.1, states, “Redundant portions of a safety system provided for a safety function shall be independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any design basis event requiring that safety function.” Clause 5.6.3 of this standard states, “The safety system design shall be such that credible failures in and consequential actions by other systems, as documented in 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard.” Digital I&C Interim Staff Guidance-4 (DI&C ISG-04), “Highly-Integrated Control Rooms—Communications Issues“ provides guidance for data communication between redundant portions of safety systems and between safety and non-safety systems to meet the requirements of IEEE Std 603-1991, Clauses 5.6.1 and 5.6.3. The staff reviewed the information provided the supplemental response to RAI 1076-7368, Question 7.9-27, and data communications design descriptions in Technical Report MUAP-07004, Rev. 8, “Safety I&C System Description and Design Process,” and Technical Report MUAP-07005, Rev. 9, “Safety System Digital Platform -MELTAC-,“ and requests the applicant to provide the following additional information in the US-APWR DCD or its referenced documents to demonstrate compliance to IEEE Std 603-1991, Clauses 5.6.1 and 5.6.3.

1. Section 4.3.2.5.1 of Technical Report MUAP-07005 provides only the data flow from the O-VDU to the central processing unit (CPU) module within the COM. As such, the staff does not understand how data is then sent from the CPU module in the COM to the designated safety controller. Provide a detailed description of the data flow from the O-VDU to the safety controllers within the reactor protection system (RPS), safety logic system (SLS) and engineered safety feature actuation system (ESFAS). In addition, for each division, clarify if there is a single dedicated Control Network I/F module for each safety I&C controller or do all the safety I&C controllers share one Control Network I/F module? Further, provide the detailed software algorithm for sending command signals from the O-VDU to a safety controller.

2. **[**

PROPRIETARY INFORMATION WITHHELD

]

3. **[**

PROPRIETARY INFORMATION WITHHELD

]

4. **[**

PROPRIETARY INFORMATION WITHHELD

]

5. In response to RAI 1076-7368, Question 7.9-27, Additional Item 4-1, the applicant states, “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.” It is unclear to the staff how the applicant defines the term “hardwired.” Does the term “hardwired” include programmable logic devices (e.g. Field Programmable Gate Arrays (FPGAs))? The staff requests the applicant to include a definition of “hardwired” in the US-APWR FSAR or its referenced documents and ensure the use of this term in the US-APWR DCD is consistent with this definition.