MITSUBISHI HEAVY INDUSTRIES, LTD.
16-5, KONAN 2-CHOME, MINATO-KU
TOKYO, JAPAN

August 1, 2011

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

Attention: Mr. Jeffrey A. Ciocco

Docket No. 52-021
MHI Ref: UAP-HF-11244

Subject: **MHI's Responses to US-APWR DCD RAI for Chapter 7, Response to the Additional Questions from the NRC, Revision 8 of the Technical Report MUAP-07005-P "Safety System Digital Platform –MELTAC-", and mark up of DCD Tier 1 on Revision 3**

References: 1) "REQUEST FOR ADDITIONAL INFORMATION 771-5827 REVISION 5, SRP Section: 07.01 – Instrumentation and Controls – Introduction, Application Section: Section 07.01" dated June 15, 2011.

2) "REQUEST FOR ADDITIONAL INFORMATION 772-5734 REVISION 3, SRP Section: 07-14 – Branch Technical Position – Guidance on Software Reviews for Digital Computer, Application Section: Section 07.01" dated June 17, 2011.

3) "REQUEST FOR ADDITIONAL INFORMATION 778-5866 REVISION 3, SRP Section: 07.09 – Data Communication Systems, Application Section: Section 07.09" dated July 8, 2011

4) "REQUEST FOR ADDITIONAL INFORMATION on Topical Report MUAP-07004(R2) Safety I&C System Description and Design Process dated May 1, 2009"

5) "REQUEST FOR ADDITIONAL INFORMATION 677-5325 REVISION 2, SRP Section: 07.08 – Diverse Instrumentation and Control System, Application Section: Section 07.08" dated January 10, 2011

With this letter, Mitsubishi Heavy Industries, Ltd. ("MHI") transmits to the U.S. Nuclear Regulatory Commission ("NRC") documents and CDs as listed in Enclosures.

Enclosure 2 and 3 are the responses to RAIs contained within Reference 1 through 3, and enclosure 4 and 5 are the amended responses to the RAIs contained within Reference 4 and 5.

Enclosure 6 and 7 are the response to additional questions from the NRC on conference calls held from May to July.

Enclosure 8 and 9 include the markups of DCD Tier 1 and Revision 8 of the Technical Report entitled "Safety System Digital Platform –MELTAC-", which was previously submitted in April

DO81
NRO

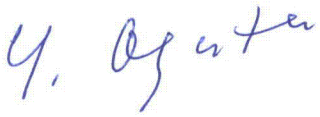
2011, as revision 7

As indicated in the enclosed materials, this submittal contains information that MHI considers proprietary, and therefore should be withheld from public disclosure pursuant to 10 C.F.R. § 2.390 (a)(4) as trade secrets and commercial or financial information which is privileged or confidential. A non-proprietary version of the document is also being submitted with the information identified as proprietary redacted and replaced by the designation "[ ]".

This letter includes copies of the proprietary version of documents (Enclosures 2, 4, 6 and 8), copies of the non-proprietary version of documents (Enclosures 3, 5, 7 and 9), and the Affidavit of Yoshiki Ogata (Enclosure 1) which identifies the reasons MHI respectfully requests that all materials designated as "Proprietary" in Enclosures 2 and 4 be withheld from public disclosure pursuant to 10 C.F.R. § 2.390 (a)(4).

Please contact Dr. C. Keith Paulson, Senior Technical Manager, Mitsubishi Nuclear Energy Systems, Inc. if the NRC has questions concerning any aspect of this submittal. His contact information is provided below.

Sincerely,



Yoshiki Ogata,
General Manager- APWR Promoting Department
Mitsubishi Heavy Industries, LTD.

Enclosures:

1. Affidavit of Yoshiki Ogata

2. Response to Request for Additional Information for Chapter 7
   (Proprietary Version)

3. Response to Request for Additional Information for Chapter 7
   (Non-Proprietary Version)

4. Amended Response to Request for Additional Information for Chapter 7
   (Proprietary Version)

5. Amended Response to Request for Additional Information for Chapter 7
   (Non-Proprietary Version)

6. Response to the Additional Questions from the NRC (Proprietary Version)

7. Response to the Additional Questions from the NRC (Non-Proprietary Version)

8. CD 1:
   "Mark up of DCD Tier 1 on Revision 3"
   "MUAP-07005-P(R8) Safety System Digital Platform –MELTAC-"
   - Version containing Proprietary information

9. CD 2:
   "Mark up of DCD Tier 1 on Revision 3"
   "MUAP-07005-NP(R8) Safety System Digital Platform –MELTAC-"

   - Version not containing Proprietary information

CC: J. A. Ciocco
C. K. Paulson

Contact Information
C. Keith Paulson, Senior Technical Manager
Mitsubishi Nuclear Energy Systems, Inc.
300 Oxford Drive, Suite 301
Monroeville, PA 15146
E-mail: ck_paulson@mnes-us.com
Telephone: (412) 373-6466

Enclosure 1

Docket No. 52-021
MHI Ref: UAP-HF-11244

MITSUBISHI HEAVY INDUSTRIES, LTD.

AFFIDAVIT

I, Yoshiki Ogata, state as follows:

1. I am General Manager, APWR Promoting Department, of Mitsubishi Heavy Industries, LTD ("MHI"), and have been delegated the function of reviewing MHI's US-APWR documentation to determine whether it contains information that should be withheld from public disclosure pursuant to 10 C.F.R. § 2.390 (a)(4) as trade secrets and commercial or financial information which is privileged or confidential.

2. In accordance with my responsibilities, I have reviewed the enclosed documents have determined that portions of the document contain proprietary information that should be withheld from public disclosure. Those pages containing proprietary information are identified with the label "Proprietary" on the top of the page and the proprietary information has been bracketed with an open and closed bracket as shown here "[ ]". The first page of the document indicates that all information identified as "Proprietary" should be withheld from public disclosure pursuant to 10 C.F.R. § 2.390 (a)(4).

   Enclosed Documents:
   - Response to Request for Additional Information for Chapter 7
   - Amended Response to Request for Additional Information for Chapter 7
   - Response to the Additional Questions from the NRC
   - MUAP-07005-P(R8) "Safety System Digital Platform –MELTAC-"

3. The information identified as proprietary in the enclosed document has in the past been, and will continue to be, held in confidence by MHI and its disclosure outside the company is limited to regulatory bodies, customers and potential customers, and their agents, suppliers, and licensees, and others with a legitimate need for the information, and is always subject to suitable measures to protect it from unauthorized use or disclosure.

4. The basis for holding the referenced information confidential is that it describes the unique design of the safety I&C system design, developed by MHI and not used in the exact form by any of MHI's competitors. This information was developed at significant cost to MHI, since it required the performance of Research and Development and detailed design for its software and hardware extending over several years.

5. The referenced information is being furnished to the Nuclear Regulatory Commission ("NRC") in confidence and solely for the purpose of information to the NRC staff.

6. The referenced information is not available in public sources and could not be gathered readily from other publicly available information. Other than through the provisions in paragraph 3 above, MHI knows of no way the information could be lawfully acquired by organizations or individuals outside of MHI.

7. Public disclosure of the referenced information would assist competitors of MHI in their design of new nuclear power plants without incurring the costs or risks associated with the design and testing of the subject systems. Therefore, disclosure of the information contained in the referenced document would have the following negative impacts on the competitive position of MHI in the U.S. nuclear plant market:

   A. Loss of competitive advantage due to the costs associated with development of the safety I&C system. Providing public access to such information permits competitors to duplicate or mimic the safety I&C system design without incurring the associated costs.

   B. Loss of competitive advantage of the US-APWR created by benefits of enhanced plant safety, and reduced operation and maintenance costs associated with the safety I&C system.

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 1st day of August, 2011.

Y. Ogata

Yoshiki Ogata,
General Manager- APWR Promoting Department
Mitsubishi Heavy Industries, LTD.

Enclosure 3

Docket No. 52-021
UAP-HF-11244

Response to Request for Additional Information for Chapter 7

August 2011

Non-Proprietary Version

This Enclosure includes following response of RAIs

RAI No. 771-5827 Revision 5, Question No.: 07.01-40

RAI No. 771-5827 Revision 5, Question No.: 07.01-41

RAI No. 771-5827 Revision 5, Question No.: 07.01-42

RAI No. 771-5827 Revision 5, Question No.: 07.01-43

RAI No. 772-5734 Revision 3, Question No.: 07-14-43

RAI No. 772-5734 Revision 3, Question No.: 07-14-44

RAI No. 778-5866 Revision 3, Question No.: 07-9-24

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

8/1/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**NO.771-5827 REVISION 5**
SRP SECTION:	**07.01 – INSTRUMENTATION AND CONTROLS - INTRODUCTION**
APPLICATION SECTION:	**07.01 – INSTRUMENTATION AND CONTROLS - INTRODUCTION**
DATE OF RAI ISSUE:	**6/15/2011**

QUESTION NO. : 07.01-40

The criteria of Appendices A and B of 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," apply to systems and related quality assurance processes, and if those systems include software, the requirements extend to the software elements. In Section 3.0, "Applicable Code, Standards and Regulatory Guidance," of MUAP- 07005-P, Rev. 7, conformance to the IEEE software standards (examples: items 65 – 74) are identified as being provided in the pre-Appendix B based QAP procedures, not the Appendix B-based QAP procedures.

If the pre-Appendix B-based QAP procedures can be used to meet 10 CFR 50 Appendix B criteria with no changes required, the reasons why each pre-Appendix B procedure was replaced, as shown by Appendix C of MUAP-07005, to an Appendix B-based QAP procedure should be identified. Otherwise, MHI is requested to reference the Appendix B-based QAP procedures in Section 3.0 and throughout the document.

ANSWER:

The description provided in the MELTAC Technical Report (MUAP-07005), Item 65 - 67, 69 - 70, 72 - 74 in Section 3.0 will be revised as follows:

65. IEEE 730 1989 Software Quality Assurance Plans

    The Software Quality Assurance Plans are described in Section 6. Common elements that do not depend on individual projects are described in [ ] for QAP Rev.1/Rev.2. QAP Rev.1/Rev.2, which applies to the original MELTAC platform that was developed in Japan, has been commercially dedicated for safety applications (see Item 46). These procedures were replaced by ~~and in~~ [ ].

[ ], [ ] and [ ] to meet the requirements of 10 CFR 50 Appendix B. These procedures are part of the App. B-based QAP which will be used specifically for US-APWR plants. Project-dependent individual elements are described in the Project Plan and the Software V&V Plan.

66. IEEE 828 1990 IEEE Standard for Software Configuration Management Plans

The software Configuration Management Plan is described in Section 6.1.5. It is controlled by internal documents [ ] and [ ] for QAP Rev.1/Rev.2. QAP Rev.1/Rev.2, which applies to the original MELTAC platform that was developed in Japan, has been commercially dedicated for safety applications(see Item 46). These procedures were replaced ~~and~~ by [ ] to meet the requirements of 10 CFR 50 Appendix B. This procedure is part of the App. B-based QAP which will be used specifically for US-APWR plants.

67. IEEE 829 1983 Software Test Documentation

The software test documentation is described in Section 6.1.4. It is controlled by internal documents [ ] and [ ] for QAP Rev.1/Rev.2. QAP Rev.1/Rev.2, which applies to the original MELTAC platform that was developed in Japan, has been commercially dedicated for safety applications (see Item 46). These procedures were replaced ~~and~~ by [ ] and [ ] to meet the requirements of 10 CFR 50 Appendix B. These procedures are part of the App. B-based QAP which will be used specifically for US-APWR plants.

69. IEEE 1008 1987 IEEE Standard for Software Unit Testing

Software unit testing is described in Section 6.1.4. It is controlled by [ ] and [ ] for QAP Rev.1/Rev.2. QAP Rev.1/Rev.2, which applies to the original MELTAC platform that was developed in Japan, has been commercially dedicated for safety applications (see Item 46). These procedures were replaced ~~and~~ by [ ] and [ ] to meet the requirements of 10 CFR 50 Appendix B. These procedures are part of the App. B-based QAP which will be used specifically for US-APWR plants.

70. IEEE 1012 1998 IEEE Standard for Software Verification and Validation Plans (2004 not yet endorsed by NRC)

Software V&V is described in Section 6.1.4. It is controlled by [ ] for QAP Rev.1/Rev.2. QAP Rev.1/Rev.2, which applies to the original MELTAC platform that was developed in Japan, has been commercially dedicated for safety applications (see Item 46). These procedures were replaced ~~and~~ by [ ] and [ ] to meet the requirements of 10 CFR 50 Appendix B. These procedures are part of the App. B-based QAP which will be used specifically for US-APWR plants.

72. IEEE 1028 1997 IEEE Standard for Software Reviews and Audits

Software reviews and audits are described in Section 6.1. Reviews and audits are controlled by [ ], [ ], and [ ] for QAP Rev.1/Rev.2. QAP Rev.1/Rev.2, which applies to the original MELTAC platform that was developed in Japan, has been commercially dedicated for safety applications (see Item 46). These procedures were replaced ~~and~~ by [ ] to meet the requirements of 10 CFR 50 Appendix B. This procedure is part of the App. B-based QAP which will be used specifically for US-APWR plants.

73. IEEE 1042 1987 IEEE Guide To Software Configuration Management

Configuration Management is described in Section 6.1.5. It is controlled by [ ] and [ ] for QAP Rev.1/Rev.2. QAP Rev.1/Rev.2, which applies to the original MELTAC platform that was developed in Japan, has been commercially dedicated for safety applications (see Item 46). These procedures were replaced ~~and~~ by [ ] to meet the requirements of 10 CFR 50 Appendix B. This procedure is part of the App. B-based QAP which will be used specifically for US-APWR plants.

74. IEEE 1074 1995 IEEE Std for Developing Software Life Cycle Processes 1997 version not yet endorsed by NRC

The software life cycle process is described in Section 6. It is controlled by [ ], [ ], [ ], and [ ] for QAP Rev.1/Rev.2. QAP Rev.1/Rev.2, which applies to the original MELTAC platform that was developed in Japan, has been commercially dedicated for safety applications (see Item 46). These procedures were replaced ~~and~~ by [ ] and [ ] to meet the requirements of 10 CFR 50 Appendix B. These procedures are part of the App. B-based QAP which will be used specifically for US-APWR plants.

Impact on DCD
There is no impact on the DCD.

Impact on R-COLA
There is no impact on the R-COLA.

Impact on S-COLA
There is no impact on the S-COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

8/1/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**NO.771-5827 REVISION 5**
SRP SECTION:	**07.01 – INSTRUMENTATION AND CONTROLS - INTRODUCTION**
APPLICATION SECTION:	**07.01 – INSTRUMENTATION AND CONTROLS - INTRODUCTION**
DATE OF RAI ISSUE:	**6/15/2011**

QUESTION NO. : 07.01-41

GDC 24, "Separation of Protection and Control Systems," of 10 CFR Part 50, Appendix A, states, "The protection system shall be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired."

The staff has not accepted that permanent connection of the maintenance network, including the engineering tool, conforms to this GDC and thereby safety is not significantly impaired. Several sections of MUAP-07005-P, Rev.7, discuss the permanent connection of the maintenance network to the safety system controllers including the design basis which states that this permanent connection improves plant safety.

As this technical report applies only to US-APWR and the maintenance network will be temporarily connected for US-APWR, MHI is requested to review all discussion of the maintenance tool being permanently connected and revise the discussions in this technical report accordingly.

ANSWER:

The descriptions on the permanent connection that remain in Section4.0, 4.2.2.2, and 4.3.4.1 will be deleted in the next revision of MELTAC-Technical Report (Rev.8). The description in Section 4.0, 4.1.4.2, 4.2.2.2, 4.3.4.1, 4.3.4.2 and 4.3.4.3 will be revised as follows:

[Section 4.0]

The description of NOTE 1 in Figure 4.0-1 will be revised as follows:

~~The Controllers and the safety VDU processors are temporarily connected to the Maintenance Network and the MELTAC engineering tool. The temporary connection of the Maintenance Network and the MELTAC engineering tool is application dependent.~~
For the US-APWR, connection of the Maintenance Network and the MELTAC engineering tool to the Controllers is normally disconnected.

[Section 4.1.4.2]

There is a separate Maintenance Network for each division. There are no Maintenance Network interconnections between safety divisions. ~~The temporary connection of the MELTAC engineering tool and Maintenance Network is application dependent.~~ There is also a separate MELTAC engineering tool for each division. The specification of the Maintenance Network is described below.

[Section 4.2.2.2]

The safety VDU processors are temporarily connected to the Maintenance Network and the MELTAC engineering tool. ~~The temporary connection of the Maintenance Network and the MELTAC engineering tool is application dependent.~~

[Section 4.3.4.1]

~~In this figure the Maintenance Network is connected to the controllers. However, for some applications, continuous connection of the controllers to the Maintenance Network can be permitted, for US-APWR, that connection is normally disconnect. Where continuous connection is not permitted, the controllers are normally disconnected at the controller end. The controllers are connected for equipment maintenance. If controllers are normally disconnected,~~ For US-APWR, MELTAC is normally disconnected from the Maintenance Network. MELTAC is connected to the Maintenance Network when maintenance of the controllers is required. When the controllers are connected to the Maintenance Network, a connection signal is generated which can be used by the application configuration for an alarm in the Main Control Room (MCR).

[Section 4.3.4.2]

The sentence will be changed as follows:

~~If the Controller is normally disconnected~~ The controller is normally disconnected from the Maintenance Network, so there is no communication with the MELTAC engineering tool. However, when the controller is connected to the Maintenance Network, the following communication description applies:

And the following sentence will be deleted.

~~The MELTAC platform was qualified with the non-safety MELTAC engineering tool connected, as described above.~~

[Section 4.3.4.3]

~~Although the MELTAC engineering tool and Maintenance Network are non-safety components, they can be connected to the MELTAC controllers to improve system availability and thereby improve plant safety.~~

The MELTAC engineering tool is used to read diagnostic failure data from the MELTAC controller memory. Failure information is retained in the MELTAC controller memory until the MELTAC engineering tool is connected. ~~Therefore, there is no potential that this data would be lost if the MELTAC engineering tool is not permanently connected.~~ Therefore, there is no potential that this data would be lost before the MELTAC engineering tool is connected.

The controller(s) to which the Maintenance Bus is temporarily connected would need to be declared INOPERABLE any time the controller(s) is connected to the Maintenance Network. The affected safety functions are managed by the plant technical specifications. If multiple controllers are connected to the Maintenance Network, this could result in numerous safety functions being declared INOPERABLE, and therefore entry into numerous concurrent LCO actions.

Impact on DCD
There is no impact on the DCD.

Impact on R-COLA
There is no impact on the R-COLA.

Impact on S-COLA
There is no impact on the S-COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

8/1/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**NO.771-5827 REVISION 5**
SRP SECTION:	**07.01 – INSTRUMENTATION AND CONTROLS - INTRODUCTION**
APPLICATION SECTION:	**07.01 – INSTRUMENTATION AND CONTROLS - INTRODUCTION**
DATE OF RAI ISSUE:	**6/15/2011**

QUESTION NO. : 07.01-42

10 CFR 50.55a(h)(2), Protection systems, states, in part, that protection systems must meet the requirements stated in IEEE Std. 603-1991, which would apply to the USAPWR application. IEEE Std. 603-1991, criterion 5.8.3, Indication of Bypasses, 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."

Section 4.3.4.2 of MUAP-07005-P, Rev. 7, discusses powering off a MELTAC controller to write to F-ROM memory and the resulting signal that can be used to generate an alarm in the MCR. However, not in this section, nor anywhere else in the TR or Chapter 7, is there a discussion of how continuous indication is provided for the affected functions associated with each controller when any part of the safety system is inoperative.

MHI is requested to provide in this section, or a section in Chapter 7, that will identify how criterion 5.8.3 of IEEE Std. 603, and all subparagraphs, are met.

ANSWER:

For the single controller configuration adapted to the RPS and safety VDU, a system should be placed in a bypassed condition before turning off the CPU Module for any reason, including to place the CPU Module in a dedicated re-programming chassis for application software change, because turning off the CPU Module results in loss of the function of that system. This bypassed condition is continuously displayed on the Large Display Panel and operational VDU by the manual BISI operation described in the US-APWR DCD Subsection 7.5.1.2. Additionally, alarms are generated in the MCR if the locked cabinet door of the safety-related system is open or the CPU Module is turned off.

For the redundant controller configuration adapted to the ESFAS, SLS and COM, turning off one

of the redundant CPU Module does not result in bypassed condition of that system because that system maintains the function. When both of the CPU Modules are turned off, bypassed condition for that system is indicated by manual BISI operation. The cabinet door open and the turning off the CPU Module are alarmed in the MCR as same as the single controller configuration system.

As explained above, the bypassed status of safety functions due to turning off CPU Modules is automatically or manually indicated via BISI. This design meets the requirements of clause 5.8.3 in IEEE Std. 603-1991. However, since there is no discussion on the bypass indication for CPU Module turning off in the DCD or its supporting documents, MHI will revise the DCD Chapter 7 and Safety I&C Technical Report (MUAP-07004).

The first paragraph of Subsection 4.2.5 b-(2) of MUAP-07004 will be revised as follows:

> If a safety-related function of the PSMS is bypassed or inoperable at the train level, this is continuously indicated on the Large Display Panel and operational VDU. Other bypassed or inoperable conditions that do not result in inoperability of safety-related functions at the train level are indicated on operational VDUs but not on the Large Display Panel. For example, if a CPU Module of one redundant controller configuration ~~sub~~system fails or is turned off within the ~~an~~ ESFAS, ~~or RPS~~SLS and COM ~~controller~~, the safety-related function of the ~~controller~~ system is still maintained for that train, so this ~~inoperable~~ condition is only ~~indicated on operational VDUs~~ alarmed at MCR. For these redundant controller configuration systems, when both of the CPU Modules are turned off, bypassed condition for that system is indicated on LDP and operational VDU by manual BISI operation. Compared with this, before turning off a CPU Module within the RPS or safety VDU of single controller configuration, the system should be placed in a bypassed condition, and this bypassed status is continuously indicated on the LDP and operational VDU by manual BISI operation. ~~Alternately~~ In addition, if an instrument input to a train of the RPS is bypassed or inoperable, this is continuously indicated on the ~~Large Display Panel~~ LDP because that RPS train can no longer perform its safety-related function for that parameter.

Impact on DCD

The following description will be added to the fourth paragraph of Subsection 7.9.1.5 as shown in Attachment-1.

> When a MELTAC controller is temporarily connected to the maintenance network, the engineering tool can be used for monitoring MELTAC controller performance, self-testing diagnostics and functional logic execution. The PSMS application setpoints, constants and application software are changeable only by removing the CPU ~~m~~Module that contains the memory devices from the MELTAC controller and placing it in a dedicated reprogramming chassis. In case any safety functions are bypassed due to turning off the CPU Module (i.e., turning off a CPU Module from the single configuration system or turning off both of CPU Modules from the redundant controller configuration system), bypassed or inoperable status is indicated via BISI. When the dedicated re-programming chassis is connected to the engineering tool, either directly or via the maintenance network, the engineering tool is used to down load changes. The software installation procedure verifies the authenticity and integrity of the application software through a software installation procedure, described in MUAP-07005 Section 6.1. The PSMS basic software is changeable only by removing and replacing the memory device that contains the software.

Impact on R-COLA
There is no impact on the R-COLA.

Impact on S-COLA
There is no impact on the S-COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

8/1/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**NO.771-5827 REVISION 5**
SRP SECTION:	**07.01 – INSTRUMENTATION AND CONTROLS - INTRODUCTION**
APPLICATION SECTION:	**07.01 – INSTRUMENTATION AND CONTROLS - INTRODUCTION**
DATE OF RAI ISSUE:	**6/15/2011**

QUESTION NO. : 07.01-43

In MUAP-07005, Safety System Digital Platform - MELTAC - Section Section 3.0, Applicable Code, Standards and Regulatory Guidance, MHI is requested to do the following:

MUAP-07017, US-APWR Software Program Manual, should be the reference to plant software life cycle processes conforming to life cycle process RGs (1.152, 1.168 - 1.173) and BTP 7-14.

Also, JEXU-1012-1132, MELTAC Platform Basic Software Program Manual, should be the reference to digital platform software processes conforming to life cycle process RGs (1.152, 1.168 - 1.173) and BTP 7-14. These are identified in items 22, 24 - 29.

ANSWER:

The description provided in the MELTAC Technical Report (MUAP-07005), Item 22, 24 - 29. Item 22, 24 – 29 in Section 3.0 will be revised as follows:

22. RG 1.152 Criteria for Programmable Digital Computers in Safety Systems of Nuclear Power Plants endorses IEEE 7-4.3.2-2003

    The methods used for specifying, designing, verifying, validating and maintaining software for this Equipment conforms to these requirements. The life cycle process for the original MELTAC digital platform software, that was developed in Japan and has been commercially dedicated for safety applications (see Item 46), is described in this Technical Report. The life cycle process for the current MELTAC platform is described in

the MELTAC Platform Basic Software Program Manual (JEXU-1012-1132) ~~the Safety I&C System Description and Design Process Technical Report for the US-APWR DCD~~. The life cycle process for the system application software is described in US-APWR Software Program Manual (MUAP-07017). The methods used for ~~controlling cyber threats~~ ensuring a secure development and operational environment throughout the life cycle are described in these documents.

24. RG 1.168 Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants endorses IEEE Std 1012-1998 and IEEE Std 1028-1997

    This Equipment uses processes for verification, validation, reviews and audits that conform to this Regulatory Guide. The software life cycle design processes for the original MELTAC digital platform, that was developed in Japan and has been commercially dedicated for safety applications (see Item 46), are described in Section 6 of this Technical Report. The software life cycle design processes for the current MELTAC platform is described in the MELTAC Platform Basic Software Program Manual (JEXU-1012-1132). Section 6 of this Technical Report includes references to the corresponding original MELTAC software life cycle ~~planning documents~~ procedures. Appendix C of this Technical Report provides a complete list of MELTAC software life cycle ~~documents~~ procedures with a cross correlation to the guidance of BTP 7-14. The software life cycle design processes for plant systems are described in US-APWR Software Program Manual (MUAP-07017) ~~the Safety I&C System Description and Design Process Technical Report for the US-APWR DCD~~.

25. RG 1.169 Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants endorses IEEE Std 828-1990 and IEEE Std 1042-1987

    This Equipment is designed and maintained using a Configuration Management process that conforms to this Regulatory Guide. The Configuration Management process for the original MELTAC digital platform, that was developed in Japan and has been commercially dedicated for safety applications (see Item 46), is described in Section 6.1.5 of this Technical Report. The Configuration Management process for the current MELTAC platform is described in the MELTAC Platform Basic Software Program Manual (JEXU-1012-1132). The Configuration Management process for plant systems is described in US-APWR Software Program Manual (MUAP-07017) ~~the Safety I&C System Description and Design Process Technical Report for the US-APWR DCD~~.

26. RG 1.170 Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants endorses IEEE Std 829-1983

    The test documentation for this Equipment conforms to this Regulatory Guide. The test process and corresponding documentation for the original MELTAC digital platform, that was developed in Japan and has been commercially dedicated for safety applications (see Item 46), are ~~is~~ described in Section 6.1.4 of this Technical Report. The test process and corresponding documentation for the current MELTAC platform are described in the MELTAC Platform Basic Software Program Manual (JEXU-1012-1132). The test documentation for plant systems is described in US-APWR Software Program Manual

(MUAP-07017) ~~the Safety I&C System Description and Design Process Technical Report for the US-APWR DCD~~.

27. RG 1.171 Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants endorses IEEE Std 1008-1987

    Unit testing for this Equipment conforms to this Regulatory Guide. This unit testing for the original MELTAC digital platform, that was developed in Japan and has been commercially dedicated for safety applications(see Item 46), is described in Section 6.1.4 of this Technical Report. The unit testing for the current MELTAC platform is described in the MELTAC Platform Basic Software Program Manual (JEXU-1012-1132). Unit testing for plant systems is described in US-APWR Software Program Manual (MUAP-07017) ~~the Safety I&C System Description and Design Process Technical Report for the US-APWR DCD~~.

28. RG 1.172 Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants endorses IEEE Std 830-1993

    The Software Requirements Specifications for this Equipment conforms to this Regulatory Guide. The Software Requirements Specifications for the original MELTAC digital platform, that was developed in Japan and has been commercially dedicated for safety applications (see Item 46), are described in Section 6.1.4 of this Technical Report. The Software Requirements Specifications for the current MELTAC platform are described in the MELTAC Platform Basic Software Program Manual (JEXU-1012-1132). The Software Requirements Specifications for plant systems are described in US-APWR Software Program Manual (MUAP-07017) ~~the Safety I&C System Description and Design Process Technical Report for the US-APWR DCD~~.

29. RG 1.173 Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants endorses IEEE Std 1074-1995

    The Software Life Cycle Process for this Equipment conforms to this Regulatory Guide. The Software Life Cycle Processes for the original MELTAC digital platform, that was developed in Japan and has been commercially dedicated for safety applications (see Item 46), are described in Section 6 of this Technical Report. The Software Life Cycle Processes for the current MELTAC platform are described in the MELTAC Platform Basic Software Program Manual (JEXU-1012-1132). The Software Life Cycle Processes for plant systems is described in US-APWR Software Program Manual (MUAP-07017) ~~the Safety I&C System Description and Design Process Technical Report for the US-APWR DCD~~.

Impact on DCD
There is no impact on the DCD.

Impact on R-COLA
There is no impact on the R-COLA.

Impact on S-COLA
There is no impact on the S-COLA.

Impact on PRA

There is no impact on the PRA.

ports utilized). Each ESFAS controller includes two bus master modules to receive the broadcast data from the eight RPS controllers in all four trains. One bus master module receives data from RPS controllers A - Group 1, A - Group 2, B - Group 1, and B - Group 2 (four of four ports utilized), the second bus master module receives data from RPS controllers C - Group 1, C - Group 2, D - Group 1, and D - Group 2 (four of four ports utilized).

The failure of a bus master module and E/O conversion device is considered in the FMEA.

7.9.1.4 I/O Bus

The I/O bus provides a bi-directional interface between a controller and its I/O modules. The I/O bus is interfaced via the bus master module in the controller and the repeater module within each I/O chassis. For single non-redundant controller configurations, the I/O bus is not redundant. For redundant controller configurations, the I/O bus is redundant. Various redundancy configurations are utilized as described in MUAP-07005 Section 4.1.1.1.

I/O can be located in close proximity to the controller or in locations remote from the controller. Remote I/O is utilized for both PCMS and PSMS applications.

7.9.1.5 Maintenance Network

The maintenance network is a non-safety system that allows for monitoring the status of the PSMS and PCMS equipment failure indications and diagnostics, updating setpoints and constants, and the installation of new application software. PSMS controllers are normally not connected with the maintenance network. PSMS controllers that are temporarily connected to the maintenance network are declared inoperable and the affected inoperable functions of that controller are managed by the technical specifications. Access control for the maintenance network is described in MUAP-07004 Section 6.4.1. There is communication independence for the maintenance networks for each division. However, since all maintenance networks are non-safety, no electrical independence is required and there are locations in the plant where all maintenance networks are in close physical proximity. The following description is applicable to the maintenance network for any one division.

The major components of the maintenance network are the switching hub and the engineering tool. The maintenance network interfaces to the system management module of each controller via qualified E/O converters.

The engineering tool is a dedicated non-safety personal computer, which runs on the Microsoft Windows operating system (OS). It contains MELTAC software, which allows it to interact with the controller via the maintenance network. The engineering tool is continuously connected to the maintenance network.

When a MELTAC controller is temporarily connected to the maintenance network, the engineering tool can be used for monitoring MELTAC controller performance, self-testing diagnostics and functional logic execution. The PSMS application setpoints, constants and application software are changeable only by removing the CPU ~~module~~ that contains

Replace with "Module"

the memory devices from the MELTAC controller and placing it in a dedicated re-programming chassis. When the dedicated re-programming chassis is connected to the engineering tool, either directly or via the maintenance network, the engineering tool is used to down load changes. The software installation procedure verifies the authenticity and integrity of the application software through a software installation procedure, described in MUAP-07005 Section 6.1. The PSMS basic software is changeable only by removing and replacing the memory device that contains the software.

Insert the following description:
In case any safety functions are bypassed due to turning off the CPU Module (i.e. , turning off a CPU Module from the single configuration system or turning off both of CPU Modules from the redundant controller configuration system), bypassed or inoperable status is indicated via BISI.

T to
tl
c er is
c val.
In addition, technical specifications ensure that functions affected by powering down a PSMS controller or connecting it to the maintenance network are declared inoperable in accordance with plant technical specifications.

There are multiple engineering tools connected to the maintenance network via the switching hub. An engineering tool is located in each of the I&C rooms. In addition, an engineering tool for each division is centrally located in the plant maintenance facility.

7.9.1.6 Station Bus

The station bus provides information to plant and corporate personnel and to the EOF and ERDS. The station bus receives information from the DCS via the unit management computer. The unit management computer provides a firewalled interface, which allows only outbound communication. There are no other connections from external sources to the DCS.

7.9.1.7 External Network Interface

The only interface from the PCMS and PSMS to external networks is via the firewall within the unit management computer. The unit management computer provides an outbound only interface to the plant Station Bus to allow communication to EOF computers, the NRC (via ERDS), corporate information systems and plant personnel computers.

7.9.2 Design Basis Information

7.9.2.1 Quality of Components and Modules

The PSMS includes the safety bus, data links, I/O bus, and safety VDU communications. The MELTAC platform is applied for all safety DCS components and follows the MELCO QA program. The quality of PSMS components and modules and the quality of the PSMS design process is controlled by a program that meets the requirements of ASME NQA-1-1994 (Reference 7.9-3). Conformance to ASME NQA-1-1994 is described further in Chapter 17.

The PCMS includes the unit bus, data links, I/O Bus, and the PCMS computers. The PCMS data communications uses the same hardware as the PSMS. The PCMS has a similar quality program to the PSMS, without the same level of documentation.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

08/01/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**NO.772-5437 REVISION 3**
SRP SECTION:	**07-14 Branch Technical Position - Guidance on Software Reviews for Digital Computer-Based Instrumentation and Controls Systems**
APPLICATION SECTION:	**07.01**
DATE OF RAI ISSUE:	**06/17/2011**

QUESTION NO. : 07-14 Branch Technical Position-43

10 CFR 50, Appendix A, General Design Criterion 1, "Quality Standards and Records," requires in part that systems and components important to safety be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. Section B.3.1.1 of SRP, BTP 7-14, contains an acceptable approach to software project management.

US-APWR MUAP-07017-P (R4), Section 2.3.1, states, "MHI applies the PSMS application software life cycle process for US-APWR projects described in this SPM based on these experiences, ..." The staff requests applicant to clarify the statement "based on these experiences". The staff also requests MHI to expand on how these experiences relate to PSMS application software conforming to BTP 7-14 if that was the intent of the statement.

US-APWR MUAP-07017-P (R4), Section 3.1.1.2, states, "The PSMS application software is fully qualified by..." and "The PSMS is designed with four fully redundant and independent divisions..." The staff requests that the extraneous adjective "fully" be removed. The PSMS software is either qualified or not, and PSMS system either has redundant divisions or not.

US-APWR MUAP-07017-P (R4), Section 3.1.2, 2nd to last paragraph, states, "Section 2.2 of this SPM also describes the criteria and responsibilities for assuring independence of the QA and V&V organizations..." While Section 2.2 does describe the roles and responsibilities of the V&V organization, the staff requests MHI to address V&V independence with regards to the makeup of the V&V team. If the V&V team members consist of software developers, are the software developers allowed to write test scripts for and execute tests of the code that they prepared? Also, the staff requests MHI to address the reporting chain of those helpers for the duration of the V&V testing.

US-APWR MUAP-07017-P (R4), Section 3.1.2, last paragraph, states, "...Section 2.2 of this SPM satisfy the requirements in Section B.3.1.1 of BTP 7-14..." The staff requests that applicant substitute the word "requirements" with "guidance." BTP 7-14 is staff guidance and not regulation.

US-APWR MUAP-07017-P (R4), Section 3.1.9, states "VVTM is responsible for assuring that the VVTE are trained and qualified for their assigned activities. Training and qualification of the DTE and VVTE shall include technical competencies,..." The staff requests MHI to clarify the qualification process and what training and qualification records, if any, will be kept.

Per BTP 7-14, Sections B.2.2 and B.2.3, the staff requests MHI provide a list of implementation and design outputs to support staff audit or inspection activities.

ANSWER:

See Attachment-1.

Impact on DCD
There is no impact on the DCD.

Impact on R-COLA
There is no impact on the R-COLA.

Impact on S-COLA
There is no impact on the S-COLA.

Impact on PRA
There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

08/01/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**NO.772-5437 REVISION 3**
SRP SECTION:	**07-14 Branch Technical Position - Guidance on Software Reviews for Digital Computer-Based Instrumentation and Controls Systems**
APPLICATION SECTION:	**07.01**
DATE OF RAI ISSUE:	**06/17/2011**

QUESTION NO. : 07-14 Branch Technical Position-44

10 CFR 50, Appendix A, General Design Criterion 1, "Quality Standards and Records," requires in part that systems and components important to safety be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. SRP, BTP 7-14, Section B.3.1.2 provides an acceptable approach for Software Development Plan (SDP).

US-APWR MUAP-07017-P (R4), Section 3.2 did not specify a software life cycle model that is to be used for the US-APWR application software. Section B.3.1.2.1 of BTP 7-14 states that a life cycle model should be documented in the SDP. The staff requests MHI to specify the software lifecycle model used for the US-APWR application software.

US-APWR MUAP-07017-P (R4), Section 3.2.6.4.2 descibes developing application software. Since PSMS application software code is generated as described in Section 3.2.6.4.2, how are suitable comments incorporated into the software code? The staff requests MHI to address suitable comments per Clause 5.3.4 of IEEE 1074-1995.

US-APWR MUAP-07017-P (R4), Section 3.2.8.2.3 describes two application software development tools. The staff requests MHI to address Clause 5.3.2 of IEEE 7-4.3.2-2003 on the subject. Also, this section states how the two application software development tools are developed and qualified in accordance with MELCO Quality Assurance Program. Generally, the staff associates the term 'qualified' with the commercial dedication of safety-related SSCs. Please clarify or change the wording as appropriate to avoid confusion with the standard use of the term 'qualified'.

ANSWER:

See Attachment-2.

Impact on DCD

There is no impact on the DCD.

Impact on R-COLA
There is no impact on the R-COLA.

Impact on S-COLA
There is no impact on the S-COLA.

Impact on PRA
There is no impact on the PRA.

RAI 772-5437 Question No.: 07-14 BTP-43, Attachment-1

07-14 Branch Technical Position-43

10 CFR 50, Appendix A, General Design Criterion 1, "Quality Standards and Records," requires in part that systems and components important to safety be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. Section B.3.1.1 of SRP, BTP 7-14, contains an acceptable approach to software project management.

Question No.1-1

US-APWR MUAP-07017-P (R4), Section 2.3.1, states, "MHI applies the PSMS application software life cycle process for US-APWR projects described in this SPM based on these experiences, ..." The staff requests applicant to clarify the statement "based on these experiences". The staff also requests MHI to expand on how these experiences relate to PSMS application software conforming to BTP 7-14 if that was the intent of the statement.

MHI Answer

The life cycle model applied to the US-APWR is based on MHI experience for Japanese operating PWR plants, and the description relating to conformance to BTP7-14 should have been removed in this paragraph at the same time when Appendix B was deleted from MUAP-07017-P (R4). Therefore, the second paragraph of MUAP-07017, Section 2.3.1, will be revised as follows:

~~MHI applies the PSMS application software life cycle process for US-APWR projects described in this SPM based on these experiences, and this PSMS application software life cycle process conforms to BTP7-14 (Reference-1) as shown in Appendix B.~~ This life cycle process is based on MHI experience for Japanese operating PWR plants. Section 3 describes the key contents of each of the lifecycle plans described in this SPM, which are the same plans listed in BTP7-14. Exceptions to specific BTP7-14 guidance (or referenced Regulatory Guide or Standard) are explained at the end of each section of this SPM that describes a specific plan.

Question No.1-2

US-APWR MUAP-07017-P (R4), Section 3.1.1.2, states, "The PSMS application software is fully qualified by..." and "The PSMS is designed with four fully redundant and independent divisions..." The staff requests that the extraneous adjective "fully" be removed. The PSMS software is either qualified or not, and PSMS system either has redundant divisions or not.

MHI Answer

MHI agrees with the staff's request. The third and forth bullets of MUAP-07017, Section 3.1.1.2 will be revised as follows.

- The PSMS application software is ~~fully~~ qualified by Independent V&V activities as described in Section 3.10 "SVVP" of this SPM.

- The PSMS is designed with four ~~fully~~ redundant and independent divisions (four trains) with a 2-out-of-4 trip/actuation logic to satisfy the reliability goals of the US-APWR.

The forth paragraph of MUAP-07017, Section 3.9.3 will be revised as follows:

MELTAC has been ~~fully~~ qualified to nuclear standards and has significant nuclear operating experience as described in the technical report MUAP-07005 "Safety System Digital Platform – MELTAC- ".

The first paragraph of MUAP-07017, Section 3.9.7.11 will be revised as follows:

MELTAC platform has been ~~fully~~ qualified to nuclear standards and has significant nuclear operating experience as described in the technical report MUAP-07005 "Safety System Digital Platform – MELTAC- ".

Question No.1-3

US-APWR MUAP-07017-P (R4), Section 3.1.2, 2nd to last paragraph, states, "Section 2.2 of this SPM also describes the criteria and responsibilities for assuring independence of the QA and V&V organizations..." While Section 2.2 does describe the roles and responsibilities of the V&V organization, the staff requests MHI to address V&V independence with regards to the makeup of the V&V team. If the V&V team members consist of software developers, are the software developers allowed to write test scripts for and execute tests of the code that they prepared? Also, the staff requests MHI to address the reporting chain of those helpers for the duration of the V&V testing.

MHI Answer

V&V independence with regards to the makeup of the V&V team as well as QA independence is described in the second paragraph of Section 2.2.1 and illustrated in Figure 2.2-1.

As described in item (3) of MUAP-07017 Section 3.3.2, independence criteria are met for the personnel selected for the V&V Team. The V&V team members prepare the test scripts and execute tests, and are personnel who are not involved in the software development as described in Annex C of IEEE Std 1012-1998.

In order to clearly describe the reporting chain and the independence of the V&V members, item (4) of MUAP-07017 Section 2.2.2 will be revised as follows:

> The VVTM is responsible for all independent V&V activities and tasks described in Section 3.10 "SVVP" of this SPM and shall report the results of V&V activities to the responsible General Manager (GM), QAM and PJM to assure oversight of any necessary corrective actions. The VVTM assigns VVTE resources for the PSMS application ~~software verification and validation~~ V&V activities which are described in Section 3.10, including assigned resources from other Design Teams. The VVTM is responsible for ensuring that the reporting chain and independence of the VVTE, including assigned resources from other Design Teams, meet the independence criteria as defined in Annex C of IEEE Std 1012-1998. ~~The VVTM is responsible for all V&V activities and shall report the results of V&V activities to the responsible General Manager (GM), QAM and PJM to assure oversight of any necessary corrective actions.~~

Following description will be added in a new paragraph below the second paragraph of Section 3.12.2.

> The V&V team members prepare the test scripts and execute tests, and are personnel who are not involved in the software development as described in Annex C of IEEE Std 1012-1998.

Question No.1-4

US-APWR MUAP-07017-P (R4), Section 3.1.2, last paragraph, states, "...Section 2.2 of this SPM satisfy the requirements in Section B.3.1.1 of BTP 7-14..." The staff requests that applicant substitute the word "requirements" with "guidance." BTP 7-14 is staff guidance and not regulation.

MHI Answer

MHI agrees with the staff's request. The last paragraph of MUAP 07017, Section 3.1.2 will be revised as follows.

> The organizational roles and responsibilities for the PSMS application software described in Section 2.2 of this SPM satisfy the ~~requirements~~ guidance in Section B.3.1.1 of BTP 7-14 (Reference 1) and Section 3.1.1 of NUREG/CR-6101 (Reference 26).

The last paragraph of MUAP-07017, Section 3.10.1.2 will be revised as

This SVVP serves the purpose of the V&V planning activity ~~required~~ guided by BTP 7-14 (Reference 1), and it demonstrates how the requirements of IEEE Std 1012-1998 are to be carried out in the form of implementing procedures, which are required to follow this SVVP.

Question No.1-5

US-APWR MUAP-07017-P (R4), Section 3.1.9, states "VVTM is responsible for assuring that the VVTE are trained and qualified for their assigned activities. Training and qualification of the DTE and VVTE shall include technical competencies,..." The staff requests MHI to clarify the qualification process and what training and qualification records, if any, will be kept.

MHI Answer

MHI agrees with staff's request. The last paragraph of MUAP-07017 Section 3.1.9 will be revised as follows.

> Training and qualification of the DTE and VVTE shall include technical competencies, software engineering competencies, and the PSMS application software life cycle process knowledge as determined by the DTM and the VVTM, respectively. The following process shall be included in the training and qualification.
>
> - Define the competence requirements for the design or V&V activities, designate the personnel having the work experience and prepare designation records.
> - Prepare training program, implement training and prepare training records.

Question No.1-6

Per BTP 7-14, Sections B.2.2 and B.2.3, the staff requests MHI provide a list of implementation and design outputs to support staff audit or inspection activities.

MHI Answer

The output documents, which are provided in accordance with BTP 7-14, Section B.2.2 and B.2.3 and can support staff audit or inspection activities, are provided in Table 4-1.

RAI 772-5437 Question No.: 07-14 BTP-44, Attachment-2

07-14 Branch Technical Position-44

10 CFR 50, Appendix A, General Design Criterion 1, "Quality Standards and Records," requires in part that systems and components important to safety be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. SRP, BTP 7-14, Section B.3.1.2 provides an acceptable approach for Software Development Plan (SDP).

Question No.2-1

US-APWR MUAP-07017-P (R4), Section 3.2 did not specify a software life cycle model that is to be used for the US-APWR application software. Section B.3.1.2.1 of BTP 7-14 states that a life cycle model should be documented in the SDP. The staff requests MHI to specify the software lifecycle model used for the US-APWR application software.

MHI Answer

The waterfall model illustrated in Figure 3.2-1 is used for the US-APWR application software. In order to clearly specify the life cycle model for the US-APWR, the first paragraph of MUAP-07017 Section 3.2.2.1 will be revised as follows.

> As described in Section 2.3.1, the PSMS application software life cycle process consists of the following seven phases. The life cycle model used for the US-APWR application software is the waterfall model illustrated in Figure 3.2.1. ~~Figure 3.2-1 illustrates the application software life cycle.~~

Question No.2-2

US-APWR MUAP-07017-P (R4), Section 3.2.6.4.2 descibes developing application software. Since PSMS application software code is generated as described in Section 3.2.6.4.2, how are suitable comments incorporated into the software code? The staff requests MHI to address suitable comments per Clause 5.3.4 of IEEE 1074-1995.

MHI Answer

MHI understands that "suitable comments" envisioned by Clause 5.3.4 of IEEE Std. 1074-1995 are traditionally meant for source codes written in languages such as C or C++, and that some graphic block diagram editors may also have a capability for inserting in-line comments next to or between function blocks. However, the MELTAC engineering tool has no such capability for providing "suitable

comments". The GBD, which is generated from the Function Block Diagram (FBD), the Setpoint List and the I/O List, have clear traceability to the System Design Description. The functional representation presented by the GBDs and FBDs meet the underlying objective of "suitable comments" by enabling an adequately trained and qualified engineer to understand the functional design and flow of the application software without requiring detailed knowledge of any specific programming language, other than the function blocks described in Appendix B of MUAP-07005 (Technical Report: Safety System Digital Platform – MELTAC -).

Following description will be added in a new paragraph above the last paragraph of Section 3.2.8.2.3, item (2), "Application".

"Suitable comments" envisioned by Clause 5.3.4 of IEEE Std. 1074-1995 are traditionally meant for source codes written in languages such as C or C++, and that some graphic block diagram editors may also have a capability for inserting in-line comments next to or between function blocks. However, the MELTAC engineering tool has no capability for providing "suitable comments". The GBD, which is generated from the Function Block Diagram (FBD), the Setpoint List and the I/O List, have clear traceability to the System Design Description. The functional representation presented by the GBDs and FBDs meet the underlying objective of "suitable comments" by enabling an adequately trained and qualified engineer to understand the functional design and flow of the application software without requiring detailed knowledge of any specific programming language, other than the function blocks described in Appendix B of MUAP-07005 (Technical Report: Safety System Digital Platform – MELTAC -).

Question No.2-3

US-APWR MUAP-07017-P (R4), Section 3.2.8.2.3 describes two application software development tools. The staff requests MHI to address Clause 5.3.2 of IEEE 7-4.3.2-2003 on the subject. Also, this section states how the two application software development tools are developed and qualified in accordance with MELCO Quality Assurance Program. Generally, the staff associates the term 'qualified' with the commercial dedication of safety-related SSCs. Please clarify or change the wording as appropriate to avoid confusion with the standard use of the term 'qualified'.

MHI Answer

Relating to the subject of Clause 5.3.2 of IEEE 7-4.3.2-2003, the methods of verifying the development and V&V tools is described in MUAP 07017, Section 3.10.7, which states that "The VVT

shall verify that Basic Software and Tools have been supplied in accordance with above Technical Report and the Basic Software Program Manual".
In order to clearly describe the relationship to the statement of Clause 5.3.2 of IEEE 7-4.3-2003, the second paragraph of MUAP-07017, Section 3.10.7 will be revised as follows.

> Conforming to Clause 5.3.2 of IEEE 7-4.3.2-2003, ~~T~~the VVT shall verify that basic software and Tools have been supplied in accordance with above Technical Report and the Basic Software Program Manual.

As described in MUAP-07017 Section 3.2.8.2.3, both of the application software development tools are non-safety. In order to avoid confusion, the term qualified will be changed to 'verified'. Item (2) of MUAP-07017, Section 3.2.8.2.3 will be revised as follows.

> RAPID is developed and ~~qualified~~ verified in accordance with the MELCO Quality Assurance Program for non-safety items.
>
> The MELTAC engineering tool is developed and ~~qualified~~ verified in accordance with the MELCO Quality Assurance Program for non-safety items.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

08/01/2011

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

RAI NO.:	NO.778-5866 REVISION 3
SRP SECTION:	07.09 - Data Communication Systems
APPLICATION SECTION:	07.09 - Data Communication Systems
DATE OF RAI ISSUE:	06/30/2011

QUESTION NO. : 07.09-24

GDC 24 states,
"The protection system shall be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired."

IEEE-603 (incorporated by reference via 50.55a(h)) also requires demonstration of interdivisional independence and high reliability as well for safety system design. ISG-04, Staff Position 1.3 states, in part, that safety systems should be as simple as possible. Functions that are not necessary for safety, even if they enhance reliability, should be executed outside the safety system. A safety system designed to perform functions not directly related to the safety function would be more complex than a system that performs the same safety function, but is not designed to perform other functions. The more complex system would increase the likelihood of failures and software errors. Such a complex design, therefore, should be avoided within the safety system.

Section 7.9.1.1.2 of DCD Tier 2, revision 3, states "Signals transmitted from the PCMS to PSMS for interlocks and automatic control of safety components during normal operation. These signals are blocked by automatic safety signals and logic in the PSMS, which ensures priority of all safety functions. All safety components controlled by the PSMS have automated safety signals and priority logic." Interface from PCMS to PSMS for automatic control of safety-related components during normal operation is not credited in Chapter 15 and adds significant complexity to the interdivisional communication. This interface therefore should be avoided to make safety systems as simple as possible. The staff is unable to confirm that this PCMS to PSMS interface conforms to the ISG-04 guidance stated above to which MHI commits to conform.

The staff requests MHI to fully address conformance to the stated guidance

ANSWER:

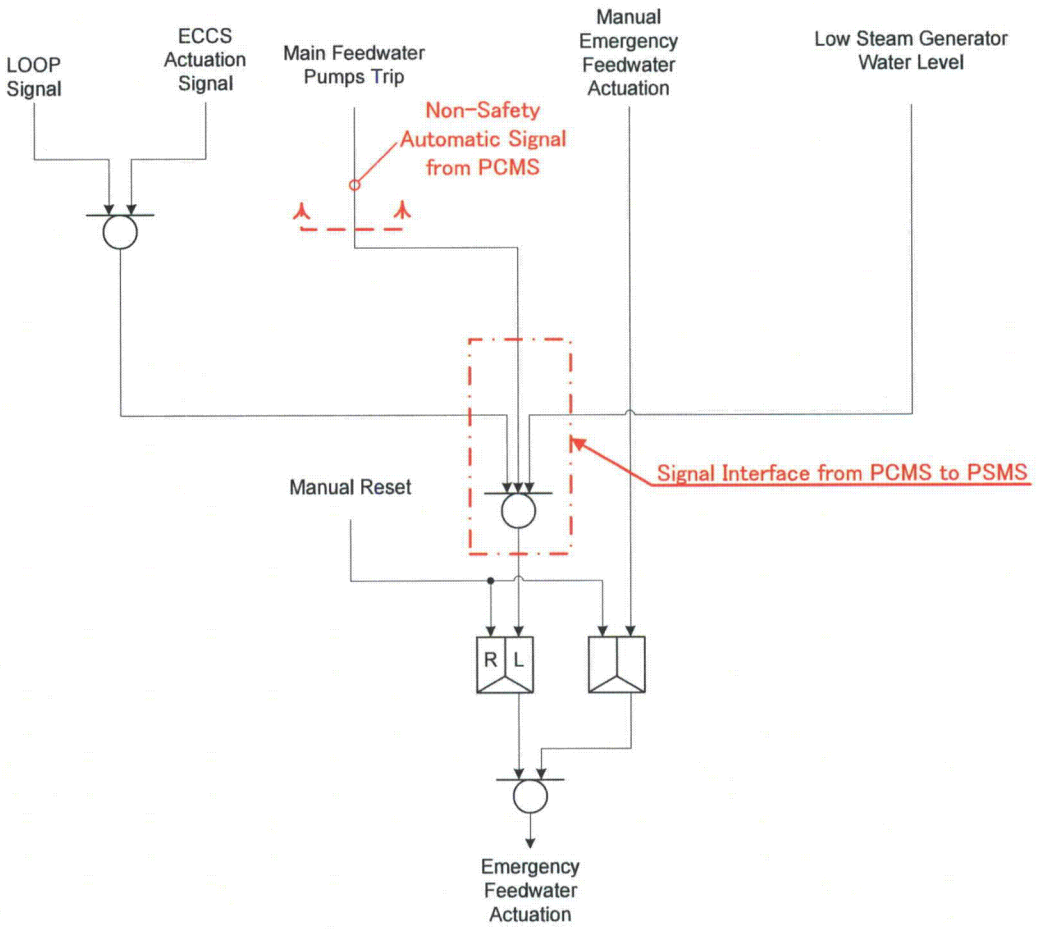
The non-safety automatic control signals of the safety-related functions from the PCMS enhance the plant safety as described in Subsection 7.7.1.13 of the DCD markup submitted to the NRC on May 31st (MHI Letter No.UAP-HF-11159).

The interface logics for the non-safety automatic control signals from the PCMS consist of simple "AND" and "OR" logic functions within the PSMS, as shown typically in Figures 1 (a) and (b), below. Therefore, the added complexity for these additional signals and logic functions in the PSMS is very limited. In all cases, safety-related signals in the PSMS have priority over these non-safety automatic control signals from the PCMS.

If the non-safety automatic control signals from the PCMS to the PSMS are interfaced by hardwired cables, the "AND" and "OR" logic functions shown in Figures 1 (a) and (b) are still needed in the PSMS. In addition, for the hardwired cables interface design must require additional hardware devices in the PSMS, such as, binary I/O modules, isolation modules, etc.

On the other hand, the Unit Bus interface can minimize the hardware devices and reduce the complexity of the system architecture of the PSMS, to compare with the hardwired cables interface because the Unit Bus interface does not require any additional hardware devices. Therefore, the Unit Bus interface results in the simplest architecture of the PSMS, as complying with the guidance of ISG-04, Staff Position 1.3.

(a) Example of Control Logic for Letdown Orifice Isolation Valve



(b) Example of Actuation Logic for Emergency Feedwater Actuation

Impact on DCD
The following is added to Section 7.9.1.1.2 of the DCD Chapter 7. See Attachment-1, also.

The interface logics for the non-safety automatic control signals from the PCMS consist of simple "AND" and "OR" logic functions (within the PSMS. Therefore, the added complexity for these additional signals and logic functions in the PSMS is very limited. In all cases, safety-related signals in the PSMS have priority over these non-safety signals from the PCMS.

Impact on R-COLA
There is no impact on the R-COLA.

Impact on S-COLA
There is no impact on the S-COLA.

Impact on PRA
There is no impact on the PRA.

7.9.1.1.2 Unit Bus

The unit bus provides non-safety data communication between all I&C systems. The main signals transmitted through the unit bus are:

- Manual operation signals transmitted from the operational VDUs in the MCR and RSR to the PSMS and PCMS. Signals to the PSMS are blocked by automatic safety signals and logic in the PSMS, which ensures priority of all safety functions. All safety components controlled by the PSMS have automated safety signals and priority logic.
- Signals transmitted from the PCMS to PSMS for interlocks and automatic control of safety components during normal operation. These signals are blocked by automatic safety signals and logic in the PSMS, which ensures priority of all safety functions. All safety components controlled by the PSMS have automated safety signals and priority logic.
- Process and alarm signals transmitted from the PSMS and PCMS to the LDP and VDUs in all operating locations, MCR, RSR, and TSC and to the computer systems such as process recording computer system, alarm processor system, etc.
- Shared sensor signals, such as pressurizer pressure, and shared calculated signals, such as T_{avg}, are transmitted from each PSMS division to the PCMS.

Signals interfaced between the PSMS and PCMS use qualified E/O isolators that are part of the safety system. In addition, communication and functional isolation are provided, within the PSMS, for signals sent from the PCMS to PSMS, such as process control signals and signals from operational VDUs. These signals are interfaced via redundant communication subsystems within the PSMS, referred to as the COM, which provide the communication interface between the unit bus and all PSMS controllers for non-safety control signals that originate in the PCMS.

Further details on communication independence are discussed in MUAP-07004 (Reference 7.9-2) Appendix B.5.6.

Add the following paragraph:
The interface logics for the non-safety automatic control signals from the PCMS consist of simple "AND" and "OR" logic functions (within the PSMS. Therefore, the added complexity for these additional signals and logic functions in the PSMS is very limited. In all cases, safety-related signals in the PSMS have priority over these non-safety signals from the PCMS.

7.9.1.2

The sa

- unit module within the safety VDU processor.
- The safety VDU touch panel is interfaced to the safety VDU processor through a touch panel interface module, which provides a conventional point-to-point data link.

Safety VDU processors are located in the Class 1E I&C room. There are separate safety VDU processors for the safety VDUs in the MCR and the safety VDUs in the RSR. Each safety VDU processor interfaces to the safety bus by a qualified E/O isolator. This

Enclosure 5

Docket No. 52-021
UAP-HF-11244

Amended Response to Request for Additional Information
for Chapter 7

August 2011

Non-Proprietary Version

This Enclosure includes following response of RAIs

Safety I&C 2nd Set, RAI-63 (UAP-HF-09261 R0)

RAI No. 677-5325 Revision 2, Question No.: 07.08-6

RAI-63

Section 5.1.9, Credit for Self-Diagnostics for Technical Specification Surveillance, this section should stipulate what surveillances are not longer necessary.
Additionally data should be provided that demonstrates the effectiveness of the self diagnostics.

Also, in the January 22, 23 meeting with the staff at ORNL, the MHI agreed to provide a description of how self-diagnostics are checked during manual surveillance tests. A history of self diagnostics success or failure (either specific factory or field data) is to be added to the topical report. The data should demonstrate that tests and operating experience did not detect something that self-diagnostics were expected to detect, and that self-diagnostics did not incorrectly report errors that were later determined to be acceptable. MHI is requested to make the above changes or provide justification for not including the information.

Response

The following has been added to Section 5.1.9 of MUAP-07004 Rev.7:

> Plant specific technical specifications identify manual surveillance tests that confirm input signal calibration and propagation through the digital system. Manual surveillance tests are also provided to confirm command propagation through the digital system and correct control of plant components. These manual surveillance tests, along with the self-diagnostics and Memory Integrity Checks discussed above, are credited to eliminate manual surveillance tests of functional logic and algorithms, setpoints and constants.

Also, we will identify in MELTAC Technical Report (MUAP-07005 Rev.8) the number of plants which the MELTAC system is applied in safety systems and the number of failures in safety system applications.
The description in Section 7.6 of MELTAC Technical Report (MUAP-07005 Rev.8) will be changed as follows;

In addition, the following will be added to the end of Section 7.6 of MELTAC Technical Report (MUAP-07005 Rev.8).

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

8/01/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	NO.677-5325 REVISION 2
SRP SECTION:	07.08 – DIVERSE INSTRUMENTATION AND CONTROL SYSTEMS
APPLICATION SECTION:	TECHNICAL REPORT MUAP-07014
DATE OF RAI ISSUE:	1/10/2011

QUESTION NO. : 07-08-6

Regulatory Guidance: BTP 7-19, Section B.3, states that, "Displays and manual controls provided for compliance with Point 4 of the NRC position on D3 should be sufficient both for monitoring the plant state and to enable control room operators to actuate the systems that will place the plant in a hot shutdown condition." DI&C-ISG-05, Part 3, section 1.A, states that the HFE analysis must demonstrate that the operator(s) can perform the actions correctly and reliably in the time available. Responses to the following questions are necessary to support the staff making a final safety determination on these general acceptance criteria.

Question: MUAP-07014-P(R2), Section 3.4, pg 3-6 regarding CCF immediate post-trip actions states, "Perform event specific immediate action(s) based on the first-out indication." The staff requests MHI address the following with respect to this action:

Is the diverse reactor trip actuation alarm always the "first-out indication" mentioned above? (List of prompting alarms on page 3-5 seems to imply it is. Section 3.5.4 says that operators will be trained to respond to DAS prompting alarms, regardless of other control room indications. This appears to be a different strategy than responding to the "first-out indication". Please explain this apparent difference. If multiple first-out indications will exist explain why additional time is not required to diagnose the event associated with the particular alarm. (Currently all the time estimates appear to assume the proper procedure will be readily apparent.)

ANSWER:

The diverse reactor trip actuation alarm is not always the first alarm generated by the diverse HSI panel (DHP). As described in DCD Subsection 7.8.1.1.2 and shown in Figure 6.2-1 of MUAP-07006-P(R2), the DHP generates one diverse actuation summary audible alarm tone, which indicates the DAS output demand for any DAS automatic actuation (reactor trip, turbine trip, MFW isolation, or EFW actuation, etc.). In addition, there are three first out alarm tiles, which indicate the specific input condition (low pressurizer pressure or high pressurizer pressure or low SG level) for the DAS automatic actuation. Other abnormal plant conditions, without DAS automatic actuation, are also indicated by individual alarm tiles on the DHP; the same alarm tone previously described for DAS automatic actuations is also generated for any of these other alarm

conditions. The DHP alarm list on MUAP-07014-P(R2) page 3-5 will be corrected to describe this design, as follows:

- DAS automatic actuation (summary audible, with first out indication of initiating input condition)
- Main steam line radiation (N-16)
- DAS automatic SI actuation

All of these DHP alarms are considered to be DHP prompting alarms for which operators will be trained to recognize a CCF and initiate mitigating actions from the DHP. The CCF response strategy is to respond to the DHP prompting alarm, which, depending on the specific event, may or may not include one of the first out indications associated with DAS automatic actuation.

All DHP alarms, including the DAS automatic actuation alarms, are blocked if the PSMS/PCMS functions correctly. Functioning correctly for automatic actuations means that the actuated plant components have repositioned correctly. Functioning correctly for plant conditions that are only alarmed means that the PCMS has generated the corresponding prompting alarm. The blocking logic for alarms corresponding to DAS automatic actuations is described in Section 6.2.2.2 of MUAP-07006. The blocking logic is also shown in DCD Figures 7.8-2 and 7.8-3. In response to NRC requests regarding consideration of partial CCF conditions, additional actuation/alarm blocking logic is described in various sections of MUAP-07014.

For partial CCF conditions, it is possible that other non-prompting alarms may be generated from the PSMS/PCMS or some parameter indications may be available on the PSMS/PCMS displays, even when DHP prompting alarms are generated. However, since DHP alarms have been generated, operators will be trained to assume that a CCF exists, that the PSMS/PCMS alarms and indications cannot be trusted, and to enter the DHP procedures. Therefore, regardless of any other PSMS/PCMS alarms or indications, operators will be trained to respond to any DHP alarm by initiating special event EOPs for CCF conditions. To support this operator training strategy, DHP prompting alarms have two alarm processing circuits arranged in a two-out-of-two configuration to prevent spurious DHP alarms.

In conclusion, MUAP-07014(R2) Section 3.5.4 is correct as written "operators will be trained to respond to DAS prompting alarms, regardless of other control room indications". However, the operator response description in Section 3.4, pg 3-6 regarding post-trip actions will be corrected as follows:

> Based on the unique DHP prompting alarm (including the first-out indication), the operator starts taking using the indications and controls on the diverse HSI panel (DHP). For the US-APWR the specific DHP indications and controls are defined in Tables 7.8-2 and 7.8-4 of the DCD. After the reactor is tripped, either automatically or by manual actions, operators will monitor and control the plant as follows:
>
> - Verify both the reactor and the turbine have tripped (through neutron flux and main steam line pressure indications on the DHP)
> - Verify sufficient emergency feedwater into each steam generator (through steam generator water level indications on the DHP)
> - Control EFW flow rate using the DHP T_{cold} indicator and EFW control valves
>
> Although most events will be mitigated or terminated upon completion of "immediate CCF event specific actions", the procedures direct the operator to continue to monitor the event, and all critical safety functions to ensure that plant conditions stabilize.

There is a unique event specific procedure for each DHP alarm. For most events concurrent with CCF there will not be multiple DHP prompting alarms. However, if multiple DHP prompting alarms are initiated, operators will be trained to prioritize their response. The procedures will then direct the operator to respond to other lower priority alarms. Therefore, operators can quickly select the appropriate event specific procedure based on the DHP prompting alarms and prioritization training.

In conclusion, the CCF strategy is to respond to the unique DAS prompting alarm, which, depending on the specific event, may or may not include one of the first out indications associated with the DAS automatic actuation. Operator training will ensure that operators understand the appropriate response and procedure for handling each DAS prompting alarm. For most events there will not be multiple DHP alarms. Where multiple DHP alarms are generated, operators will be trained to prioritize their procedure selection. In either case, the event specific procedure will be readily apparent without the need for additional diagnosis time.

Impact on DCD
There is no impact on the DCD.

Impact on R-COLA
There is no impact on the R-COLA.

Impact on S-COLA
There is no impact on the S-COLA.

Impact on PRA
There is no impact on the PRA.

Enclosure 7

Docket No. 52-021
UAP-HF-11244

Response to Additional Questions from the NRC

August 2011

Non-Proprietary Version

Responses to the Additional Questions from the NRC
(Sheet 1 of 11)

No.	Additional Questions from the NRC	Response to the Questions from MHI	Documents to be Revised
1	Clarify the number of multidivisional safety VDUs and make appropriate changes of the Safety I&C Technical Report.	Subsection 4.2.4 will be revised to clarify the number of multidivisional VDU as shown in markup of Safety I&C Technical Report.	Safety I&C Technical Report (MUAP-07004) See Attachment-4
2	Should Figure 2.5.6-1 of DCD Tier 1 Markup be revised (1) change division to train and (2) to include the proposed multidivisional safety VDUs?	Figure 2.5.6-1 of DCD Tier 1 will be revised to incorporate the multidivisional VDU.	DCD Tier 1 Figure 2.5.6-1 See Attachment-3
3	Section 7.7.1.13 of DCD Rev. 4 Markup (page 7.7-19) states "The reasons why the unit bust interface is selected are described in Subsection 7.9.1.2" regarding non-safety automatic control signals interface from PCMS to PSMS via the unit bus. Subsection 7.9.1.1.2 should be referred instead.	Subsection 7.7.1.13 will be revised to correctly refer Subsection 7.9.1.1.2 as shown in markup of DCD Chapter 7 (Attachment-2).	DCD Tier 2 Subsection 7.7.1.13 See Attachment-2 (yellow highlighted)
4	Keep consistency of words, such as Trip Switchgear, RTB and CRDM, etc. across all related documents including the Response Time of Safety I&C System Technical Report (MUAP-09021).	Reactor trip switchgear will be revised to reactor trip breaker or RTB in following portions. •Section 4.2.4.a, b and Table 6.5-2 of MUAP-07004 •Section 1.2 and Figure 3.2-1 and Table 4.1-1 of MUAP-09021 • Section 3.5.3 (1) and (4) of MUAP-07014	Safety I&C Technical Report (MUAP-07004) Response Time Technical Report (MUAP-09021) D3 Coping Analysis Technical Report (MUAP-07014) See Attachment-4, 5 and

Responses to the Additional Questions from the NRC
(Sheet 2 of 11)

			yellow highlighted in Attachment-6.
5	Multidivisional Safety VDUs must be evaluated and more clear descriptions on 100% testing capabilities of the PIF module must be added in JEXU-1015-1009 (MELTAC Platform ISG-04 Conformance Analysis).		
5-1	Section 3.2.4 of JEXU-1015-1009, Revision 4, states "The data link used between the S-VDU touch screen and the S-VDU processor is used only within the same safety division. Therefore, it is not evaluated within the scope of DI&C ISG-04, which applies only to inter-division data communication." [ ]	The data link identified in Section 3.2.4 of JEXU-1015-1009 is the data link described in Section 4.2.1.2.1.b of MUAP-07005. [	N/A

Responses to the Additional Questions from the NRC
(Sheet 3 of 11)

		] This data link is described in Section 4.3.3 of MUAP-07005; compliance to ISG-04 is addressed in JEXU-1015-1009, including analysis of communication faults in Section 3.2.2. Therefore, since the multi-division S-VDU touch screen data link is not an inter-division data communication interface, there is no need to revise JEXU-1015-1009.	
5-2	JEXU-1015-1009-P (R4), MELTAC Platform ISG-04 Conformance Analysis, p.61, Section 3.3.6. ISG-04 2.6 with regards to the PIF module, priority logic component (circuit board), now states (vs R3); [ ] [	[ ]	MELTAC Platform ISG-04 Conformance Analysis (JEXU-1015-1009)

	]		
6	8 questions on scope and method of the self-diagnostic features, the manual periodic tests and the continuous on-line tests, etc.		
6-1	The self-diagnostic features are confirmed by manual periodic tests and continuous on-line tests that are diverse from the self-diagnostic features. Information for the continuous on-line test, diverse from the self-diagnostic features, is requested. Does this refer to only the CHANNEL CHECK or are there other tests involved?	Continuous on-line test refers to CHANNEL CHECK.	N/A
6-2	The TS periodic manual surveillance tests confirm the accuracy of the self-diagnostic features. Does this mean that the self-diagnostic features is manually calibrated for use of testing devices?	This RAI response was amended on May 31, 2011 and the term "accuracy" was changed to "functionality" as follows. (Reference: UAP-HF-11159) The TS periodic manual surveillance tests confirm the accuracy functionality of the self-diagnostic	N/A

		features, thereby complying with 10 CFR Part 50 Appendix B, Criterion XII. Since the self-diagnosis feature is implemented in the digital device, no manual calibration for use of testing devices is needed.	
6-3	The continuous automatic CHANNEL CHECK is conducted by the PCMS, based on signals that are processed by the RPS controllers. The operability of the automatic CHANNEL CHECK is confirmed through periodic manual CHANNEL CALIBRATION. The surveillance test intervals for channel check and channel calibration are a different interval. How is the operability of the automatic channel check confirmed when the intervals of the two surveillance tests are so much different (i.e. continuously vs. 24 months)?	The automated CHANNEL CHECK is conducted continuously by the PCMS. Manually testing this function every 24 months is sufficient because the PCMS is fully redundant and continuously self-tested as follows: The PCMS includes internal redundancy throughout, including (1) the redundant digital data communications interface of the channel data from the PSMS, (2) the redundant Unit Management Computers which conduct the channel comparison algorithms, (3) the alarm and display computers which display any unacceptable channel deviations. All of these redundant components of the PCMS are continuously self-tested. As a result failures are quickly identified and repaired, allowing the PCMS to achieve high availability, including the automated CHANNEL CHECK function.	Safety I&C Technical Report (MUAP-07004) See Attachment-4.

		Therefore, Section 4.3 of MUAP-07004 will be revised as follows: The operability of the automatic CHANNEL CHECK is confirmed through continuous self-testing within the PCMS, and through periodic manual CHANNEL CALIBRATION.	
6-4	The RAI response states "The continuous PSMS self-diagnostic features allow elimination of most manual surveillance required for Technical Specification compliances." A clarification of this description is requested. Please begin by comparing, in a table preferably, the proposed new surveillances vs. the conventional surveillances identified in NUREG-1431.	Section 4.4 of MUAP-07004 will be changed as follows: The continuous PSMS self-diagnostic features allow elimination extending the surveillance frequency of most manual surveillances required for Technical Specification compliance. In addition, the self-diagnostic features simplify the manual surveillance tests. The differences between the conventional surveillances in NUREG-1431 and the US-APWR Technical Specifications are shown in Table-1 (Attachment-1). The key differences are the method of CHANNEL CHECK and CHANNEL CALIBRATION, and the method and frequency of COT and ALT.	Safety I&C Technical Report (MUAP-07004) See Attachment-4.

		Conventional CHANNEL CHECK is conducted manually by plant operators. For the US-APWR CHANNEL CHECK is conducted automatically on a continuous basis. The automated function is confirmed continuously. The automated function is also confirmed manually every 24 months by confirming generation of the channel deviation alarm during CHANNEL CALIBRATION. Conventional CHANNEL CALIBRATION requires three steps to calibrate the transmitter, then the electronic rack components and then confirmation of the total integrated loop. For the US-APWR CHANNEL CALIBRATION is conducted in one step that encompasses the entire loop from the transmitter to digital VDU display. Conventional COT and conventional ALT are conducted every 184 days. Conventional COT for analog functions requires simulated signal injection with precision signal wave forms and time constants. Conventional ALT for binary functions requires simulated signal injection in various combinations and time dependencies. On the other hand, the US-APWR COT-Digital and	

		ALT-Digital are limited to automated Memory Integrity Checks which are manually initiated every 24 months. This Memory Integrity Check is performed for each controller, encompassing all analog and binary functions.	
6-5	Apparently the Channel Operational Test-Digital and Actuation Logic Test-Digital are one in the same but also referred to as the Memory Integrity Check. Is this because the intent is to eliminate the conventional Channel Operational Test and the Actuation Logic Test with the Memory Integrity check?	Yes, that is correct. The COT-Digital replaces the conventional COT, which is applicable to analog processing functions. The ALT-Digital replaces the conventional ALT, which is applicable to binary logic functions. Both COT-Digital and ALT-Digital invoke the same Memory Integrity Checks. For all PSMS controllers only one Memory Integrity Check will be conducted. This test fulfills the technical specification surveillance requirement of the COT-Digital or ALT-Digital. The RPS controllers of the PSMS perform both analog and binary functions of predecessor conventional systems. Therefore, both COT-Digital and ALT-Digital are specified in the Technical Specifications. However, only one Memory Integrity Check will be conducted to fulfill both surveillance requirements.	N/A
6-6	The bit by bit check is done only on the CPU module,	The Staff is correct; the bit by bit memory integrity	N/A

	therefore only the checksum is done as part of the Memory Integrity Check for all other modules with software. Is this correct?	check is done only for the basic software and application software that resides on the CPU module. For other modules there are no software memory integrity checks. Instead the integrity of the Basic Software in other modules is confirmed by self-diagnostic functions conducted or monitored by the CPU module. If the software on a peripheral module is corrupted, that module will not function correctly, and errors will be detected by the CPU module.	
6-7	Is there an error message if the checksum or the bit by bit check is unacceptable? What does the procedure tell the technician to do if either of these tests fail?	There are error messages for all self-diagnostic functions of the controller. If an error is detected by a self-diagnostic function, a signal that can be used for alarm is generated from the controller. Self-diagnostic errors are categorized into three types of alarms, as described in Section 4.1.5 of MUAP-07005. For sustained or recurring alarms, technicians will be instructed to replace faulty modules. For non-recurring transient alarms, technicians will be instructed to monitor the system for further degradation. The bit by bit memory integrity check is performed	N/A

		using the MELTAC engineering tool. If a memory error is detected, an error message is indicated on the screen of the MELTAC engineering tool. For this error Technicians will be instructed to replace the faulty CPU module. Alarms, system memory errors and module replacements will be entered into the plant corrective action program for tracking and trending.	
6-8	How is results of the bit by bit check verified or is the MELENS software being validated (Ref. ISG-04, Staff Position 2.6)?	The bit-by-bit memory integrity test is conducted only to confirm the same Basic Software and Application memory as is confirmed by the Remaining Time Diagnosis self-test described in Section 4.1.3.1(10) of MUAP-07005. The Remaining Time Diagnosis is conducted by Class 1E software. The bit-by-bit memory integrity test is a diverse confirmation method conducted by an I&C technician, using the MELTAC engineering tool. Therefore, for this application the MELTAC engineering tool is Measurement and Test Equipment (M&TE), comparable to other digital test equipment such as oscilloscopes, volt meters, data communication analyzers and digital devices	N/A

		used for transmitter calibration. The software in this type of equipment does not require validation since the output is monitored and confirmed by the technician using this equipment. In addition, the software quality for typical M&TE is confirmed based on operating history. Similarly, the technician using the MELTAC Engineering Tool will confirm the output of the bit-by-bit memory integrity check. In addition, the MELTAC engineering tool software has demonstrated reliable operation since 1987, as explained in Section 6.5 of MUAP-07005.	
7	Question on DCD Section 7.9.1.2, Safety VDU Communication, p.7.9-3, first paragraph: The statement is made that the location described is different than that of the MELTAC Technical Report "(The location of the safety VDU processors is different from the location described in MUAP-07005.)."	In Section 4.2.1.2.1 of MELTAC Technical Report (MUAP-07005 Rev.7), the following is described. "The optical interface is not credited for any isolation function since the safety VDU processor and safety VDU panel are located in the same safety division and always in the same fire zone." This description is inconsistent with that stated in DCD Section 7.9.1.2 and will be deleted to keep consistency in MUAP-07005 Rev.8. A draft markup is already provided to the NRC on July 13th.	MELTAC Technical Report MUAP-07005

Attachment-1

Table-1 Difference between conventional surveillance in NUREG-1431 and US-APWR Tech Spec

Surveillance	Conventional (NUREG-1431)		US-APWR	
	Method	Frequency	Method	Frequency
Channel Check	Manual	12 hours	Manual / Automatic	12 hours / Continuously
Channel Calibration	Manual	18 months	Manual	24 months
COT	Manual	184 days	Self-diagnosis / Manual Memory Integrity Check	Continuously / 24 months
ALT	Manual	31 days with staggered basis	Self-diagnosis / Manual Memory Integrity Check	Continuously / 24 months
TADOT	Manual	92 days with staggered basis	Manual	24 months*

*24 months is based on I&C reliability. However, this test also tests the mechanical plant components (e.g. pumps, valves). Therefore, the actual frequency is determined by in-service testing of mechanical plant components, which is conducted typically every three months.

7.7.1.9 Turbine Protection Control

The turbine protection system in the PCMS receives signals regarding the turbine-generator and provides appropriate trip actions when it detects undesirable operating conditions of the turbine-generator.

7.7.1.10 Electrical System Control

The electrical system in the PCMS controls and monitors the non-safety plant electrical systems.

7.7.1.10.1 Generator Transformer Protection System

The generator transformer protection system in the PCMS monitors important parameters of the main generator such as vibration and temperature. The generator transformer protection system provides a generator trip in case of turbine trip. This system also controls related components (e.g., breakers) in case of undesirable operating conditions of the generator and associated transformer(s).

7.7.1.10.2 Auto Voltage Regulator/Automatic Load Regulator System

The auto voltage regulator (AVR)/automatic load regulator (ALR) system provides regulation of generator voltage.

7.7.1.11 Radiation Monitoring System

The radiation monitoring system (RMS) section of the PCMS provides non-safety area and process radiation monitoring to generate displays and alarms. Refer to Chapters 11 and 12 for additional related details.

7.7.1.12 Auxiliary Equipment Control System

The auxiliary equipment control system section of the PCMS controls and monitors auxiliary systems (e.g., radioactive waste disposal system, CVCS water treatment).

HSI for the auxiliary equipment control system is located in the auxiliary equipment control room, which is located in the auxiliary building. This control room is manned periodically for auxiliary equipment operation (i.e., radioactive waste management). Key alarms are displayed on the alarm VDU, LDP and the operational VDU and key indications are provided on operational VDUs. Refer to Chapter 11 related details.

7.7.1.13 Automatic Control of Safety-Related System

There are several automatic control signals interface from the PCMS to the PSMS via unit bus and COM, which actuate safety-related components and safety-related actuation signals in order to enhance the plant safety. These automatic controls enhance the plant safety, but not credited in the safety analysis of DCD Chapter 15. The priority logic within the SLS ensures that a safety-related signal, either manually or automatically, generated from the PSMS has higher priority than those automatic control

signals from the PCMS. These signlas are transmitted from the PCMS to the PSMS via the non-safety unit bus. The reasons why the unit bus interface is selected are described in Subsection 7.9.1.1.2.

No.3

These automatic controls from the PCMS to the PSMS are same as the conventional standard PWR plants, and the design conformances to the reguratory requirements are described in Subsection 7.1.4, Subsection 7.9.2.7 and the Safety I&C Technical Report (Reference 7.7-1). The detailed design conformances to the ISG-04 (Reference 7.7-3) are described in Appendix E of MUAP-07004 (Reference 7.7-1).

Non-Safety Signal from the PCMS to the SLS via Unit Bus

(1) Closure signal of Steam Generator Blowdown Line and Blowdown Sampling Line Isolation Valve from non-safety Radiation Monitor related signal

The high radiation signal of non-safety radiation monitor related to SG blowdown lines closes the safety-related isolation valves of the steam generator blowdown flow and the blowdown sampling line. For detailed description, refer to Subsection 10.4.8.

Radioactive material releases at an accident, such as SGTR accident, can be minimized by this non-safety automatic function. Therefore, this non-safety automatic function enhances the plant safety, but is not credited in the safety analysis of DCD Chapter 15.

(2) Closure signal of Letdown Orifice Isolation Valve from Pressurizer Water Level Control

This non-safety function automatically closes the safety-related letdown line isolation valves by a low water level signal from the pressurizer to prevent the excessive low water level conditions. For detailed description, refer to Subsection 7.7.1.1.8.

The pressurizer water level at an abnormal condition can be maintained in high level, and the reactor coolant inventory decreses can be minimized by this non-safety automatic function. Therefore, this non-safety automatic function enhances the plant safety, but is not credited in the safety analysis of DCD Chapter 15.

(3) Actuation signal of Class 1E Battery Room Exhaust Fan from Battery Room Exhaust Fan Outlet Airflow Control.

The battery rooms should be ventilated in order to limit the hydrogen concentration. The safety-related back up battery room fan automatically starts upon non-safety signal of the running fan airflow failure. For detailed description, refer to Subsection 9.4.5.3.2.

Hydrogen concentration can be minimized by this non-safety automatic function to protect the Class 1E battery room from the fire and explosion. Therefore, this non-safety automatic function enhances the plant safety, but is not credited in the safety analysis of DCD Chapter 15.

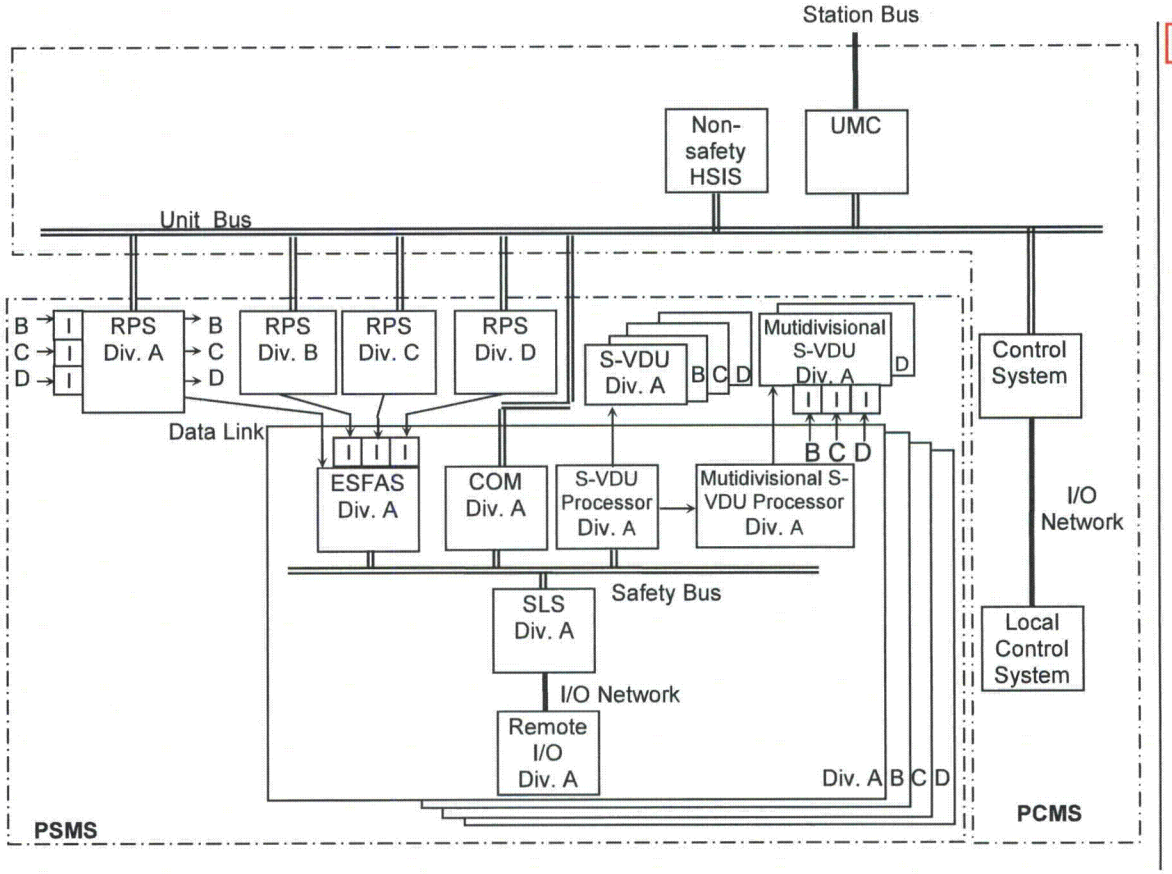


Figure 2.5.6-1 DCS Configuration

c. Control of Interlocks Important to Safety

The SLS receives interlocks from the RPS which operate to reduce the probability of occurrence of specific events or to ensure availability of safety functions.

The Safety Logic System controls these Interlocks Important to Safety through the component level application software in the SLS controllers. Non-safety systems are not required for Interlocks Important to Safety.

4.2.4 Safety-Related HSI System

All automated safety-related functions may be manually initiated and monitored by operators using the safety-related HSI System. The safety-related HSI System is also used to manually initiate other safety-related functions that are not automated, including safety-related functions credited for safe shutdown. The safety-related HSI System also provides all safety-related plant information to operators, including critical parameters required for post accident conditions. The safety-related HSIS includes two types of VDUs. Ones (safety VDUs) provide the information and operation for components and system level functions of the own train. The others (multidivisional safety VDUs) provide the information for critical safety functions for safe shutdown of all four trains.

a. Control of Reactor Trip Breaker~~Switchgear~~ | No.4

Operators can trip the Reactor Trip Breakers using conventional switches on the Operator Console. There is one switch for each Reactor Trip Actuation train.

b. Control of ESF Components

The ESF components are controlled from the Safety-Related HSI System on the Operator Console. There are two types of control.

- Touch operations on the safety VDUs
  Touch operations include component and system level functions. Touch operations of component control on the safety VDU are duplicated on the non-safety operational VDUs. Due to better graphics and better screen navigation features, the operational VDUs are the preferred HSI for all normal and abnormal plant conditions. Therefore, the touch operations on the safety VDU are considered backup controls. However, for all design basis events, the safety VDUs are the component level HSI devices credited for compliance to applicable Class 1E criteria.
- Conventional switches on the Operator Console
  Conventional switches are provided to initiate each train level ESF actuation signal. The switches are hardwired to the ESFAS. For all design basis events, the hard controls are the system level HSI devices credited for compliance to applicable Class 1E criteria.

c. Post Accident Monitoring (PAM)

The Safety-Related HSI system displays PAM parameters that are designated Type A, B or C in RG 1.97. The purpose of displaying these post-accident monitoring (PAM) parameters is to assist main control room personnel in evaluating the safety-related status of the plant. PAM parameters are direct measurements or derived variables representative of the safety-related status of the plant. The primary function of the PAM parameters is to aid the operator in the rapid detection of abnormal operating conditions. As an operator aid, the PAM variables represent a minimum set of plant parameters from which the plant safety-related status can be assessed.

The Type A and B PAM parameters are normally displayed continuously on the multidivisional safety VDUs on the Operator Console in the Main Control Room. There is twoone multidivisional safety VDUs; one is for Train A and the other is for Train D for Train A and D. The parameters are selected based on R.G. 1.97 and at least two channels of each parameter are available. The bases for the selection of the US-APWR PAM variables is described in Appendix H. No.1

d. Safe Shutdown from Outside the Main Control Room

The Remote Shutdown Console, located outside the Main Control Room fire zone, is installed so that safe shutdown can be achieved in the case that the operators can not stay within the Main Control Room.

In order to achieve and maintain the reactor in the cold shutdown condition (safe shutdown state), it is necessary to remove excess heat to control the temperature, pressure and volume of the reactor coolant, and to supply boric acid, etc. Therefore, the operating controls, of those plant systems necessary for the above mentioned operations, can be operated from the Remote Shutdown Console. The Remote Shutdown Console provides the same functions of the operational VDUs and the safety VDUs in the Main Control Room.

These controls are switched over from the Main Control Room to the Remote Shutdown Room by MCR/RSR Transfer Switches. The configuration of MCR/RSR transfer system is illustrated in Figure 4.2-1.

Separate Transfer Switch Panels to control each of the four PSMS trains and the PCMS are located just outside of the Main Control Room fire zone (switches dedicated for each of four PSMS trains and dedicated for PCMS in the panel) and in the Remote Shutdown Room (same switch configuration as that of in the Main Control Room fire zone). When the transfer actions from the Main Control Room to Remote Shutdown Console are initiated from both sets of switches for any one train, HSI signals from the MCR are blocked and HSI signals at the RSR are enabled. Transfer is controlled separately for each of the four PSMS trains and separately for the PCMS. Any subsequent damage to MCR HSI devises, caused by the fire in the Main Control Room, does not affect the functions of the Remote Shutdown Console. Transfer from the RSC back to the MCR is activated separately for each of the four PSMS trains and the PCMS using the same transfer switches. Access to the Remote Shutdown Console, and the

RPS controllers. This test confirms the operability of the RPS controllers through automated testing that is diverse from the MELTAC self-diagnostic features. If a failure is detected that should have been detected by the MELTAC self-diagnostic features, a failure of the MELTAC self-diagnostic features is also identified. The operability of the automatic CHANNEL CHECK is confirmed through continuous self-testing within the PCMS, and through periodic manual CHANNEL CALIBRATION. No.6-3

4.4 PSMS Manual Testing and Calibration Features

The integrity of safety-related function of the PSMS is continuously checked by their self-diagnostic features. The continuous PSMS self-diagnostic features allow ~~elimination~~ extending the surveillance frequency of most manual surveillances required for Technical Specification compliance. In addition, the self-diagnostic features simplify the manual surveillance tests. No.6-4

The verification of self-diagnostic features is performed by the combination of (1) manual periodic surveillance tests, that confirm the integrity of all program memory within each MELTAC controller in the PSMS, including the software memory that controls the self-diagnostic functions, and (2) manual periodic surveillance tests that confirm that each controller can correctly execute that program memory. The overlap of these periodic surveillance tests confirms that the PSMS self-diagnostic features are fully operable.

The self-diagnostic features are also confirmed by manual periodic tests and continuous on-line tests that are diverse from the self-diagnostic features. These tests confirm the operability of each MELTAC controller in the PSMS, thereby ensuring that failures have not been missed by the self-diagnostic features.

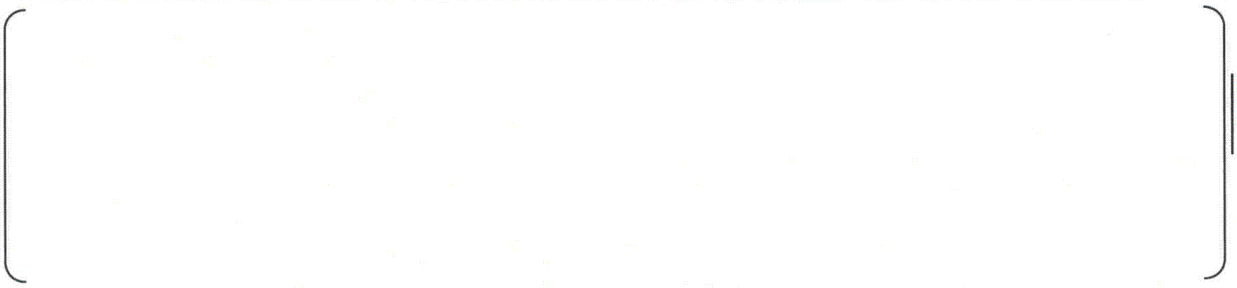
The coverage of self-diagnosis and manual testing is shown in Figure 4.4-4, and the description of each testing in Figure 4.4-4 is described in Section 4.4.1 and 4.4.2.

4.4.1 Manual Testing

Manual test features are provided for system level manual initiation of reactor trip and ESF actuation signals, the safety VDU touch screens, binary process inputs and final actuation of plant process components. An additional manual test is conducted to confirm the integrity of the PSMS software memory. Most manual tests may be conducted on-line without full system actuation and without plant disturbance. Each of these manual tests is described in the sections below.

- Manual Reactor Trip (TRIP ACTUATION DEVICE OPERATIONAL TEST)
  The manual reactor trip actuation signals are tested by actuating the conventional switches on the Operator Console, one train at a time. Also, TADOTs are conducted from the O-VDU or S-VDU for the separate undervoltage and shunt trip functions of the reactor trip breakers, as shown in Figure 4.4-1. Correct functionality is confirmed by status signals sent from the RTBs to the O-VDU or S-VDU via the RPS controllers. When the reactor trip function is tested one train of reactor trip breakers will open, but the plant will not trip, since breakers in two trains must open to de-energize the CRDMs.

  The Reliability Analysis method, which demonstrates the need to conduct this test no more frequently than once per 24 months, is described in Section 6.5. However, this test may be conducted more frequently, if required by the reliability of the reactor trip breakers. The test frequency for the reactor trip breakers is described in the US-APWR DCD Chapter 16.



No.4

Figure 6.5-2 Breakdown Response Time for Reactor Trip

No.4

6.5.4 Accuracy Analysis Method

The accuracy of each instrumentation loop for safety-related function is analyzed to determine the instrument channel set points. A typical loop consists of the following components:

- Sensor
- Analog input module

Loops that include an interface to the DAS would have an additional analog splitter/isolation module.

The accuracy of the complete channel is calculated by combining the accuracy of each component in the loop using statistical methods. A square root of the sum of the squares

Response time of I&C system in RT is broken down to each delay time from process value reach setpoint until control rods are released by the CRDM. Refer to the Safety I&C Technical Report (Reference 2) Section 6.5.3 for the breakdown response time for RT. This document repeats the description of the Safety I&C Technical Report (Reference 2) for better understanding of the response time. It is noted that the response time of control rod drop is excluded from this report, because that response time is outside the scope of the I&C system discussed in this document. The response time of control rod drop is described in DCD (Reference 1) Subsection 15.0.0.2.5.

No.4

No.4

Figure 3.2-1 Breakdown Response Time for Reactor Trip

(2) Response time of ESF actuation
Response time of ESF actuation is broken down to delay time as the following in each process from process value reach setpoint until ESF actuation signal is generated.

Figure 3.2-2 Breakdown Response Time for ESF Actuation

4.0 ALLOCATED RESPONSE TIMES

4.1 Response Time Requirement for RT and ESF System

The allocated response times for the RT signal and the ESF actuation signal are shown in Tables 4.1-1 and 4.1-2, respectively. These allocations establish the response time requirement for each component. It can be seen that the total response times for the safety I&C system is equivalent to the analytical limits shown in Table 7.2-3 and 7.3-4 of DCD (Reference 1) Section 7.2 and 7.3 and credited in safety analysis in DCD (Reference 1) Section 15.0.0.3.

Table 4.1-1 Allocated Response Time of Reactor Trip

No.4

3.5.3 Erroneous Signals

Since the DAS includes blocking logic, which prevents DAS actuation if the PSMS actuates correctly, the DAS functions could be blocked by erroneous signals (i.e., signals indicating that the protection system has actuated correctly, when it actually has not). To avoid any potential for erroneous signals that may be generated by the digital CCF, the signals used to block the DAS actuation are obtained from sources that are not affected by the digital CCF, as follows:

(1) Reactor Trip, Turbine Trip and Main Feedwater Isolation

The DAS automatic reactor trip, automatic turbine trip and automatic main feedwater isolation functions are blocked only when the DAS receives signals hardwired directly from the reactor trip ~~switchgear~~ breaker and low turbine emergency oil pressure signals (i.e., down stream of the postulated digital CCF) in the condition that the pressurizer pressure is above the P-11 setpoint. The diverse actuation signal from DAS is manually defeated in the condition that the pressurizer pressure below the P-11 setpoint. These hardwired signals indicate that the required number of circuit breakers and turbine emergency trip oil pressure trip signal have correctly actuated. If either actuation is unsuccessful, the DAS will generate backup reactor trip, backup turbine trip and backup main feedwater isolation signals. For example, if there is a partial CCF in the PSMS that affects only reactor trip, the PSMS will actuate turbine trip and main feedwater isolation, and the DAS will actuate reactor trip. Similarly, if there is a partial CCF in the PSMS that affects only turbine trip, the PSMS will actuate reactor trip and main feedwater isolation, and the DAS will actuate turbine trip. No.4

A partial CCF could also result in failure of the main feedwater isolation function of the PSMS, but may not affect the reactor trip and turbine trip functions of the PSMS. For this scenario, the DAS will receive successful reactor trip and turbine trip feedback, which will result in blocking all three functions, including DAS actuation of main feedwater isolation. To accommodate this partial CCF condition, the main feedwater isolation valves are diversely closed by both the PSMS (by actuating binary pilot solenoids) and PCMS (by actuating modulating electro-pneumatic positioners). Since this failure only affects the main feedwater function of the PSMS (not all functions), the software defect cannot be in the PSMS Basic Software (which is common to all functions). Instead, the software defect must be in PSMS software that is unique to the main feedwater isolation function (i.e., the solenoid component control Application Software, or the portion of the MELTAC Basic Software that executes those unique binary solenoid application functions). Therefore, the PCMS main feedwater isolation function, which controls the valve's modulating positioners, is not adversely affected, because it does not rely on the same Application Software or Basic Software used to actuate binary solenoids, as in the PSMS.

(2) EFW Actuation

The DAS automatic actuation of emergency feedwater is blocked only when the DAS receives signals hardwired directly from the motor driven EFW pump switchgear and the turbine driven EFW pump control valves (i.e., down stream of the postulated digital CCF) in the condition that the pressurizer pressure is above the P-11 setpoint. The diverse actuation signal from DAS is manually defeated in the condition that the pressurizer

pressure below the P-11 setpoint. These hardwired signals indicate that the required number of EFW pumps have correctly actuated. If the PSMS EFW pump actuation is unsuccessful, the DAS will generate backup EFW actuation signals.

It is noted, that there are also valves in the EFW flow lines. Therefore, it could be postulated that the EFW pumps would start as expected, but a partial CCF could prevent opening the valves. However, this failure does not need to be considered, because during normal plant operating conditions, the EFW flow line valves are open. If these valves are closed for any reason, this state can be detected by an indication in MCR. This will prompt correct positioning of these valves to their required normally open position, prior to a Chapter 15 event. Since BTP-19 allows the use of best estimate methods, only normal pre-event plant conditions are considered in the D3 Coping Analysis. It is also noted, that spurious closure of these valves due to CCF, concurrent with a design basis event, does not need to be considered, as discussed in Section 5.5 of MUAP-07006 and Section 4 of DI&C Interim Staff Guidance 02.

(3) Main Steam Line Radiation (N-16) Alarm

The DAS N-16 high radiation alarm is credited to prompt manual action to mitigate the SGTR event. This alarm is blocked only when the DAS receives signals hardwired directly from an output of the PCMS, which generates the PCMS N-16 alarm in the condition that the pressurizer pressure is above the P-11 setpoint. The diverse actuation signal from DAS is manually defeated in the condition that the pressurizer pressure below the P-11 setpoint. These hardwired signals indicate that the required PCMS N16 alarm has correctly actuated. If the PCMS N-16 alarm actuation is unsuccessful due to CCF, the alarm processor will not generate this output and the DAS will generate a backup N-16 alarm.

For the SGTR event, there are no PSMS automated actions credited in the Chapter 15 analysis, and no DAS automated actions credited in the D3 coping analysis. Therefore, if the PCMS correctly generates the N-16 alarm, operators are prompted to take the mitigating actions credited in the Chapter 15 analysis.

(4) High-High Steam Generator Water Level Alarm

The DAS high-high steam generator water level alarm is not credited to prompt diverse manual actions for any event in the D3 coping analysis. The alarm is provided only to support operator tasks after diverse mitigation actions are prompted by other alarms. This alarm is blocked only when the DAS receives signals hardwired directly from the reactor trip ~~switchgear~~ breaker (i.e., down stream of the postulated digital CCF) in the condition that the pressurizer pressure is above the P-11 setpoint. The diverse actuation signal from DAS is manually defeated in the condition that the pressurizer pressure below the P-11 setpoint. These hardwired signals indicate that the required number of circuit breakers have correctly actuated. If the reactor trip actuation is successful, the manual actions credited in the D3 coping analysis are not needed. This is true regardless of any partial CCF conditions that may block other PSMS functions. Therefore, it is appropriate to block the DAS high-high steam generator water level prompting alarm.

No.4

ATTACHMENT 1

FILES CONTAINED IN CD 1

CD 1: "Mark up of DCD Tier 1 on Revision 3"
"MUAP-07005-P(R8) Safety Digital Platform –MELTAC-"

- Version containing proprietary information

Contents of CD

File Name	Size	Sensitivity Level
DCD_Tier1.pdf	0.3MB	Non-Proprietary
MUAP-07005-P(R8).pdf	7.8MB	Proprietary

ATTACHMENT 2

FILES CONTAINED IN CD 2

CD 2: "Mark up of DCD Tier 1 on Revision 3"
"MUAP-07005-NP(R8) Safety Digital Platform –MELTAC-"

- Version not containing proprietary information

Contents of CD

File Name	Size	Sensitivity Level
DCD_Tier1.pdf	0.3MB	Non-Proprietary
MUAP-07005-NP(R8).pdf	6.6MB	Non-Proprietary