Enclosure 3

UAP-HF-09393
Docket No. 52-021

MHI's Response to 2nd round Requests for Additional Information

on

Topical Report MUAP-07005-P(R3)
Safety System Digital Platform -MELTAC-

July 2009
(Non-Proprietary)

MHI's Responses to 2nd round RAI on Topical Report MUAP-07005-P(R3) "Safety System Digital Platform -MELTAC-"

Non-proprietary Version

July 2009

©2009 Mitsubishi Heavy Industries, Ltd.
All Rights Reserved

INTRODUCTION

This report documents Mitsubishi Heavy Industries' (MHI's) responses to U.S. Nuclear Regulatory Commission's (NRC's) request for additional information (RAI) on the MHI Topical Report, MUAP-07005-P (R3), "Safety System Digital Platform –MELTAC–".

This report describes the responses for forty-six (46) requests for information from the NRC.

The RAI, "Request For Additional Information 07/01/2009 US-APWR TOPICAL REPORT: Safety System Digital Platform – MELTAC MUAP-07005-P(R3)" , was issued on July 1st, 2009.

RESPONSE TO THE RAI (JULY 1, 2009)

Following provides the responses to RAI.

RAI-01

Original question: (In part) Identify the specific differences in the MELTAC equipment applied for non-safety applications vs. the equipment applied to safety applications.

Response: (In part) The differences between the safety and non-safety platform are primarily in system configuration and application software. The Basic Software of the two platforms is essentially the same.

NRC Supplement:
The information should provide sufficient details to allow the NRC staff to understand all the differences and arrive at an independent conclusion that the regulations and guidance for the safety system are met in comparison to the non-safety system. The "specific" differences, at a minimum, would be included in the design and quality assurance (QA) programs that incorporate software QA and verification and validation (V&V) as discussed by RG 1.152, Criteria for use of Computers in Safety Systems of Nuclear Power Plants. Therefore the hardware and software that use the same safety or non-safety process would be identified, how they are marked and how the processes are different.
At the January 22, 23 meeting with the staff, MELTAC agreed to identify the MELTAC modules that are common to safety and non-safety are interchangeable. Clarify that there are unique MELTAC hardware and software modules that can only be used in non-safety applications. The topical report should state that total safety module set is described in TR Appendix, but additions can be made following same process for hardware and software development, as described in TR. The topical report should describe differences in identification for safety vs. non-safety hardware and software modules.

Response

Since they are the same in function as the modules manufactured for the non-safety system, the modules manufactured for safety system can be applied to the non-safety system. However, the module manufactured for non-safety system cannot be applied to the safety system. The modules will be identified to clarify for which system they are manufactured. The Topical Report will be revised to clarify that there are modules for non-safety system, different in function from the modules for the safety system written in the TR Appendix.

RAI-04

Original question: Item 53 indicates compliance with IEEE 7-4.3.2, "2003 Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations," yet exceptions on Verification and Validation (V&V) have been taken due to the development of the system under Japanese standards. Please clarify. Has the code remained in Japanese or has it been translated into English? If the code has been translated, please discuss the traceability, V&V, testing, and management of the translation.

Response: (In part) [

]

NRC Supplement: MHI is requested to specifically identify compliance to IEEE 7-4.3.2 to identify ALL software tools used (see software tool definition for scope in Section 3.1.42 of the standard and Section 5.3.2 with regards use software tools).

Response

[

]

RAI-05

Original question: Identify how the MELCO internal design documents are marked for the safety and non-safety MELTAC systems. Section 3.0, Applicable Code, Standards and Regulatory Guidance, (item 62), referencing IEEE 494 1974 (this is also required by IEEE Std 603-1991, Criterion 5.11) states that documents used for internal use do not contain the "Nuclear Safety Related" designation. Also discuss how documents for the non-safety MELTAC system are differentiated from the safety related system.

Response: [

]

NRC Supplement: The staff considers, for documents, there are two issues per the requirements of IEEE Std 603-1991 and IEEE Std 494 1974; 1) The term to be used is "nuclear safety related" and is to be used on all documents described by IEEE 494. 2) This shall apply to all documents pertaining to software and hardware to the extent described in IEEE Std 494.

For identification of equipment, there are two issues per IEEE Std 603-1991 and IEEE 420, 1) which states in part, "All equipment and wiring should be permanently marked and identified on the interior of Class IE control boards, panels, or racks 2) Also states in part, "Class IE equipment and its wiring shall be identified as such, so that personnel may easily confirm its independence from non-Class IE and redundant Class IE equipment and wiring." MHI is requested to describe in the Topical Report how IEEE Std 603-1991, Criterion 5.11, will be specifically met.

Response

The following will be added to the Topical Report:

> The software document titles for the Safety MELTAC contain "MELTAC Nplus-S", where S means Safety, while the titles for the non-safety (conventional) MELTAC is "MELTAC Nplus." These titles are applicable to all MELTAC software documents used internally by MELCO. The hardware components are common for the safety and non-safety MELTAC. Therefore, there is no distinct identification for the hardware documents inside MELCO; all hardware is identified as "MELTAC Nplus".
>
> Application specific documentation (eg. cabinet layout and wiring diagrams, technical manuals, etc) for MELTAC Nplus-S systems will be marked "nuclear safety related".
>
> Cabinets and enclosures containing MELTAC Nplus-S equipment will be clearly marked externally and internally by system name and safety division, so that its Class 1E designation is clearly indicated. Where a single cabinet or enclosure contains equipment or wiring from divisions other than the division of the cabinet marking, the other equipment or wiring will be clearly marked for its own division. Wiring and equipment belonging to separate divisions will have suitable barriers and/or separation.

RAI-11

Original question: In Section 4.3.1, General Description, the design basis is discussed. The communications link is not protected against common mode failures in hardware or software; however, self-testing and diagnostics are in place to detect a failure if it occurs. Please discuss.

Response: The D3 Topical Report, MUAP-07006, describes many features of the MELTAC platform that provide protection against common mode failure. These include the QA process, equipment qualification process, simple single task operating system, single software trajectory and no external interrupts, which results in completely cyclical and deterministic performance, and self diagnostic features that can detect both hardware and software defects. The MELTAC platform has demonstrated 20 million hours with no plant shutdown due to software or hardware related problems in Japanese nuclear power plants. Therefore, there is minimum potential for a CCF within the MELTAC platform hardware or operating system, including the communications link. Regardless of this low potential for CCF, the D3 strategy assumes a software defect exists that result in CCF of all MELTAC controllers.

NRC Supplement:
MHI is requested to revise the topical report because it does not effectively address the Control Network description in terms of what is implemented point to point and ring network configuration within the **divisions** and external to the **divisions**. The term division should be used in the descriptions and in Figure 4.3-1. Also, MHI is requested to further elaborate on common mode failures of the individual component types shown in Figure 4.3-1.

Response

The MELTAC Topical Report is intended to define the generic capabilities of the platform. The actual configuration of the platform for any specific application is described in other application specific licensing documents. For example, for the PSMS and PCMS the configuration of the MELTAC platform is described in MUAP-07004. For the PSMS the ring network is used for safety related functions only within the same division. The ring network is used to communication non-safety related functions between the PSMS and PCMS. Data links are used to communication safety related functions between the divisions of the PSMS. If the MELTAC platform is used for other applications, there will be comparable application specific descriptions.

To ensure that the MELTAC communication capabilities are not misused in specific applications, the following change will be made to Section **4.3.2 Control Network:**

> The Control Network is used for the following applications:
> a) The Control Network can be used, and is used most frequently, to communicate safety related data between multiple Controllers, and between Controllers and the Safety VDU Processor(s), all in the same division.
> b) The Control Network can also be used to communicate non-safety related data between different divisions including non-safety system. This may be between multiple Controllers in different divisions. Or it may be between Operational VDU Processors and multiple Controllers in different divisions.

If there is a CMF of the components in the control network, there will be no communication

between controllers. For the specific US-APWR application this means there will be no communication between controllers within the ESFAS, SLS or between ESFAS and SLS, and no communication between controllers within the PCMS or between the PCMS and PSMS. All controllers will continue to function autonomously using the pre-defined failure state for the data that is no longer received. The predefined failure state is application dependent; it is either (1) the last known good value or (2) a predefined default value. A CMF of the control network will not affect the reactor trip function. A CMF of the control network will adversely affect the ESFAS function and the control of ESF components from the PSMS. This CMF is accommodated by the diverse automatic and manual controls provided in the DAS.

RAI-12

Original Question: In section 4.3.2, Control Network, item (b), the discussion indicates that the communication network has the capability of communicating with other divisions or non-safety system. DI&CISG-04, "Task Working Group #4: Highly Integrated Control Room - Communications Issues (HICR)" describes approximately 20 NRC staff positions on interdivisional and safety to non-safety communication. Please discuss any of these positions for which the MELTAC platform may not be in full compliance.

Response: (In Part) As a result of researching the requirements No.1 through 20 of "1 .INTERDIVISIONAL COMMUNICATION", the MELTAC platform is in full compliance, except the following.

NRC Supplement:

1) Staff Postion 10 ;

a) MHI/MELCO is requested to provide a more detailed and acceptable basis in the topical report why the permanent connection of the maintenance network is necessary. Describe in detail how the MELTAC system will function with regard to fault reporting if the engineering tool is not connected to the system, or is failed, at the time the fault occurs. Include in the description whether detailed fault information will be lost if the engineering tool is not connected at the time of the fault and any differences in how the system operates if the engineering tool is connected versus not connected. Also, elaborate how the operational and safety VDU's are integrated or not integrated to fault reporting. This would include but not be limited to the messages, icons and alarming functions that will be provided to each type os display.

b) During the audit of the MELTAC platform, a demonstration of the system showed that the engineering tool did not display the system as failed when an improper module was installed in the chassis. The front panel lights on the CPU did indicate the system failure but the Engineering Tool did not. This demonstration indicates that Engineering Tool software which is not subject to the same verification and validation process as the MELTAC Basic Software is less reliable than the safety system software. A possible motivation for connecting the Engineering Tool continuously is that it provides more complete diagnostics of system condition; however, the Engineering Tool may be detrimental to safety if it gives erroneous or inaccurate diagnostic information. Please provide a justification for the inclusion of software whose reliability cannot be guaranteed to same level as software for Class 1E systems.

c) For the only exception, on staff position 10, MHI is requested to further elaborate in the topical report. Specifically, position 10 of the ISG states, "means of keylock switch that either physically opens the data transmission circuit or interrupts the connection by means of hardwired logic." As described, this appears to use the keylock switch as an electronic AND gate circuit and the process for the restriction relies on the basic software to effect the disconnection. That apparently is the exception to position 10 of the ISG that the staff finds unacceptable.

Also, MHI requested to review DI&C-ISG-04 including all 20 Staff positions. The following are examples where the staff has concerns:

2) Staff Position 1; "A safety channel should not be dependent upon any information or resource originating or residing outside its own safety division to accomplish its safety function." MHI is requested to describe how this guideline is met. Included should be the current ambiguous discussion of the safety to non-safety ring network.

3) Staff Position 3; "A safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function. Receipt of information that does not support or enhance the safety function would involve the performance of functions that are not directly related to the safety function. 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." In accordance with this guidance in DI&C-ISG-04, provide a description of all data flows from the PCMS to the PSMS, and provide justification for each communication channel as to how it enhances the performance of the safety function.

4) Staff Position 8: "Data exchanged between redundant safety divisions or between safety and nonsafety divisions should be processed in a manner that does not adversely affect the safety function of the sending divisions, the receiving divisions, or any other independent divisions." MHI is requested to address data exchanged and what safety to non-safety messages are included in the ring network.

5) Staff Position 14; "Vital communications should be point-to-point by means of a dedicated medium (copper or optical cable). In this context, "point-to-point" means that the message is passed directly from the sending node to the receiving node without the involvement of equipment outside the division of the sending or receiving node. Implementation of other communication strategies should provide the same reliability and should be justified." The topical report does not adequately explain the point to point topology between divisions. It should also specifically address the involvement of ANY outside information from the division, where it is received, how it is used.

6) Staff Position 18: "Provisions for communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complication." MHI is requested to analyze this for potential hazards of the point to point topology in the MELTAC configuration.

Response

1) Position 10 a)
[

]

1) Position 10 b)
[

]

[

]

1) Position 10 c)
The intent of the fully hardware based keylock required by the ISG is to ensure that "… a workstation should be physically restricted from making changes in more than one division at a time."

The basis of this guidance is that a workstation connected to multiple divisions can be a potential source of single failure that could disable multiple divisions. Therefore, physical disconnection ensures compliance with the single failure criterion.

[

]

2) Position 1 – [

]

3) Position 3 – [

]

[

]

4) Position 8 –The topical report fully explains the data communication method, which ensures communication independence between sending and receiving divisions. The safety to non-safety data messages included in the ring network are application dependent. For the PSMS to PCMS interface these include all instrumentation signals used within the PSMS and the status of PSMS actuation and control functions.

5) Position 14 –The requirements of this section of the ISG pertain only to inter-division data communication. The PSMS uses only point-to-point data links for all safety related inter-division communication. The ring network is only used for safety related data communication within the same division. The point to point topology between division is generically shown in Figure 4.3-5. However, the actual point to point source and destinations are application dependent; for the PSMS this topology is shown in Figure 4.1-4 of MUAP-07004.

6) Position 18 –The ring topology is used for safety related functions only within the same division. Therefore, within the ring topology "the message is passed directly from the sending node to the receiving node without the involvement of equipment outside the division of the sending or receiving node." [

]

RAI-13

Original Question (partial): Data Link communication is discussed in Section 4.3.3.1, Configuration. The various interconnections for the communication systems are listed and named in the topical report. The information describes the network connections but does not give a graphical representation. No information is provided that would substantiate the claim that the communications network design provides physical, electrical or functional isolation of the interconnections at any level of the communications stack.

Response (partial): Figure 4.3-5 provides a graphical representation of the data link connections between redundant safety divisions. This figure is expanded in Figure 13-1 in this response. This figure shows all the data link components described in Section 4.3.3.1 of Topical Report MUAP-07005.

NRC Supplement: Figure 13-1 and text should be included in the topical report.

Response

Figure 4.3-5 Data Link Configuration in Section 4.3.3.1 of Topical Report MUAP-07005 will be replaced by the following figure described in the response of 1st RAI-13.

Section 4.3.3.1 Configuration will be revised as follows:

> Figure 4.3-5 provides a graphical representation of the data link connections between redundant safety divisions. This figure shows all the data link components and the example of connection configuration when CH1 of Controller for division1 is transmission port(T), CH1 of Controllers for other divisions is reception port(R), CH4 of Controller for division4 is transmission port(T), and CH4 of Controllers for other divisions is reception port(R).

And the following sentences will be added to Section 4.3.3.2 Isolation.

> The physical, electrical, and functional isolation, based on the above figure, is as described below.
>
> a) Physical Separation
> The E/O converter module of the data link allows 1Kmeters between sending and receiving controllers. This allows the controllers to be geographically separated into separate I&C equipment rooms. For example for the PSMS of the US-APWR, the configuration of controllers for each division is described in MUAP-07004.
>
> b) Electrical Isolation
> The MELTAC Platform uses fiber optics and optical to electrical converters (E/O Converter) to ensure electric Isolation. The optical communication circuit is shown in Figure 4.3-5.
>
> c) Communication (Functional) Isolation
> [
>
>]

[

]

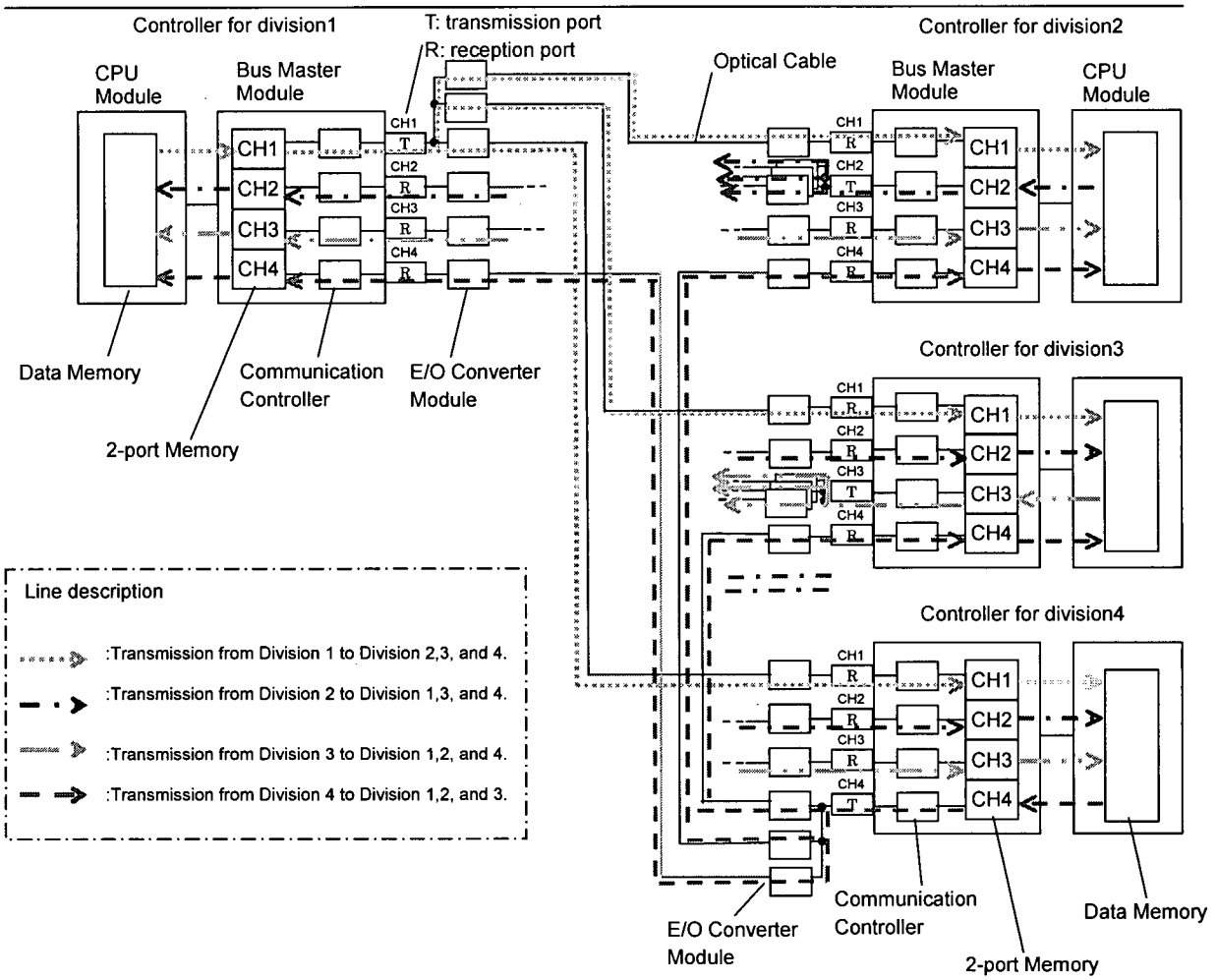


Figure 4.3-5 Example of connection configuration of Data Link configuration

RAI-14

Original Question: The module environment test conditions and test methods are based on industry standards in Japan [p. 98]. No discrepancy between those methods and procedures and the US standards is noted in the topical report, although an analysis was probably done. An audit of the test procedures and reports identifying the results and any corrective action is needed to complete acceptance of the MELTAC equipment qualification. Response: EMC, Environmental and Seismic Qualification Test Reports will be available at the MELTAC audit.
NRC Supplement:
1) During the recent audit, the staff was provided a summary report of the EMI/RFI test reports that were in Japanese. The staff noted that the summary report did not have sufficient information available that appeared to be in the full EMI/RFI test report. For example, the position of the antennas and whether the doors are open or not would impact the test results. Therefore the staff is requesting a report to be submitted to the NRC. The report should have sufficient information (and quality of information) for the staff to come to an independent conclusion that all test procedures, configurations, and results were adequate and the MELTAC system meets RG 1.180.
2) During the same audit, the staff questioned whether the optical switch was tested in the bypassed condition to see if it affects the operation of the control network. MELCO stated that the optical switch was not tested in the bypassed configuration, but will consider testing such configuration to address any operation limitations such as Technical Specification limitations that may apply for a bypassed optical switch. The staff is requesting, to be put on the docket, complete testing procedures and results and any operational considerations that may be imposed on the MELTAC platform when an optical switch is in the bypass mode. Note the listing of modules in Section 5.1.2.1 identifies the modules included for the environmental test which does not list the optical switch module. This must be addressed also. The staff is requesting a list of modules that were included in each qualification test. The staff refers MHI to IEEE Std 7-4.3.2, endorsed by RG 1.152, Section 5.4.1 Computer System testing, which states, in part, "All portions of the computer necessary to accomplish safety functions, or those portions whose operation or failure could impair safety functions, shall be exercised during testing." As this appears to be a finding in the development process, the staff is requesting the Corrective Action Report, in English, that identifies the omitted optical switch bypass mode test with English translated copies of the updated test procedures, reports and V&V reports.
3) During the Jan 21, 22 meeting, MHI agreed to provide Seismic Test Response Spectrum curves to the topical report.
Included should be a description of test configuration and any special mounting restrictions or interface requirements to ensure specific applications are bounded by seismic test.

Response

1) We will submit [ ] EMC Qualification Test Summary Report for the MELTAC Platform. This report describes the test procedures, including position of antennas, test configurations, including cabinet door open position, and results to demonstrate that the MELTAC platform meets RG 1.180.
2) A list of modules that were included in each qualification test will be added to each subsection within Section 5 of the Topical Report. In addition, we will submit a Corrective Action Report, in English, that identifies the omitted optical switch bypass mode test with English translated copies of the updated test procedures and reports. These documents will be submitted by January 2010. It is noted that the corrective action report will include an analysis which demonstrates that only seismic testing must be repeated, since the

components within the optical switch module that are used in the bypass mode would not be affected differently than when used in the normal mode for any other environmental stress conditions. There are no V&V reports associated with this test additional seismic test, since this is a hardware test.

3) We will add Seismic Test Response Spectrum curves to the topical report. The topical report will also be revised to include a description of the seismic test configuration and any special mounting restrictions or interface requirements to ensure specific applications are bounded by the seismic test.

RAI-20

Original Question: Will (did) the Failure Mode and Effect Analysis follow the guidance of any standard?

Response: None

NRC Supplement: Identify the guidance of any standards followed for the FMEA.

Response

As stated in Section 6.5.1 of MUAP-07004, the FMEA conducted for the safety functions follows the methodology of IEEE379, which confirms compliance to the Single Failure Criteria. This compliance is achieved at the application level through multiple safety divisions. The FMEA conducted for the MELTAC controller modules is not intended to confirm compliance to the single failure criteria, but rather to confirm that failures within the modules are detectable, either by self-diagnostics or by application level testing. MELCO does not use a specific standard to guide this analysis. The methodology for this FMEA is described in detail in [ ].

RAI-23

The staff is requesting additional information to be docketed for the MELTAC Platform Certification. See the Attachment titled: "Attachment to RAI 23, Additional Information to be Docketed"

Response

The response for each requested item is provided in the following table. In general, for most items, the MELTAC Platform Topical Report and other documentation submitted to date are expected to be sufficient to allow the NRC to make a safety determination. Additional detailed design documentation, which allows the Staff to confirm the information previously submitted, has been provided at the audits in Arlington and Kobe. The MELTAC Platform Topical Report will be updated to include other requested items, that are covered in the detailed design documentation provided at the audits in Arlington and Kobe, but are not included in documentation submitted to date.

No.	Request	Response
1	The Life Cycle Process for the MELTAC platform basic software is discussed in Section 6.1 of Topical Report MUAP-07005. This portion of the Topical Report does not address BTP-14 process planning or the 11 process plans. MHI is requested to specifically address and docket, as part of the MELTAC platform application, the information normally contained in the documents listed in Section B.2.1 of BTP-14.	[ ]
2	Equipment Qualification Program Documents	-
	Environmental Test Plan, Procedure & report	[ ]
	Seismic Test Plan, Procedure & report	[ ]
	Surge/Isolation Test Plan, Procedure & report	[ ]

No.	Request	Response
	EMI/RFI Test Plan & Procedure	[
	EMC test report for the MELTAC Platform	
	ESD Test Plan, Procedure & report	]
3	Hardware & Software Architecture Descriptions	[ ]
4	Requirements Safety Analysis	[ ]
5	Design Safety Analysis	[ ]
6	V&V Requirements Analysis Report	[ ]
7	V&V Design Analysis Report	[ ]
8	Configuration Management Requirements Report	[ ]
9	Configuration Management Design Report	[ ]

No.	Request	Response
		[ ]
10	System Requirements[1] Document or Specification	[ ]
11	Master or System Test Plan (composite of all hardware & software testing)	[ ]
12	Software Tool Development and Verification Program	[ ]
13	Software Requirements Specification	[ ]
14	Requirements Traceability Matrix	[ ]
15	Factory Acceptance Test procedure / reports (Including FAT)	[ ]
16	Maintenance manuals	[ ]
17	Operations procedures	[ ]
18	Q-7302.1 (V&V Detailed Proc. & Checklists)	[ ]
19	Q-7302.2 (Configuration Management Detailed Procedures)	[ ]

No.	Request	Response
		[ ]
20	Q-7104, "Guideline for Creating Safety System Digital Platform Project Plan"	[ ]
21	Current MELTAC US-APWR project plan, JEXU-1015-0002	[ ]
22	MELTAC Software Development Plan; including a MELTAC U.S. Conformance Program (UCP) assessment (Section 6.1.4 of MUAP-07005-P, Revision 2)	[ ]
23	MELTAC Platform Specification and Requirements Traceability Matrix (in accordance with Q-4102 per Section 6.1.7.1 of MUAP-07005-P, Revision 2)	[ ]

No.	Request	Response
24	MELTAC Software Specification; including the regression analysis for the UCP (Section 6.1.7.2 of MUAP-07005-P, Revision 2)	[ ]
25	MELTAC Hardware Specifications, original conformance to U.S. standards (Section 6.1.7 of MUAP-07005-P, Revision 2). This would include the single processor specification resented in the audit but also the remaining hardware should be addressed as well. (cabinets, modules, cards etc.)	[ ]

No.	Request	Response
26	Category -1 Assessments for Software Units (Section 6.1.7.3 of MUAP-07005-P, Revision 2)	[ ]
27	Category - 2 Assessments for Software Units (Section 6.1.7.3 of MUAP-07005-P, Revision 2) Final V&V report following new Integration Tests for UCP (Section 6.1.7.4 of MUAP-07005-P, Revision 2)	[ ]

Note) The V&V documents of the software unit of the Control Network (W-net) are listed for one thread of the category 1 software module.

Documents Available to be inspected at the next audit: These may be docketed in the Future:

No.	Request	Response
1	Documents to support a thread audit of a Category 2 module	[ ]
2	Documents identifying the design review process that constituted the V&V reporting of the Existing Platform.	[ ]

Documents Available For Possible Future Audits – Non Docketed

No.	Request	Response
1	Configuration Management Reports	[ ]
2	Detailed system and hardware drawings	[ ]
3	Final circuit schematics	[ ]
4	Final Software Integration Report	[ ]
5	Individual completed test procedures / reports	[ ]
6	Vacant	[ ]
7	Individual V&V Problem reports up to FAT	[ ]
8	Set point calculations	[ ]
9	Software code listings.	[ ]
10	Training manuals & course material	[ ]
11	Vendor Build Documentation	[ ]

RAI-24

MHI is requested to further provide design information, in Section 4.1.2.4, Power Interface Module. At a minimum, the following should be provided:
1. At the Jan. 22, 23 meeting, MHI agreed to clarify, in the topical report, that there are two priority logic functions – one is software based within MELTAC CPU (priority between PSMS and PCMS functions), one is hardware based within PIF module (state based priority to ensure either DAS or PSMS can place component in the credited safety state). Also, a typical functional logic for PIF for at least one component type (i.e. one IPL subboard) will be added.
2. Description of the specific interfaces between the different sections of the PIF; Communication Interface, Interposing Logic and Switching Device part.
3. During the March Audit in Kobe, the staff observed that daughter boards implement part of the priority logic path. Currently, MELCO only has daughter boards for system-based priority logic. Daughter boards are being created using state-based priority logic for the US-APWR. The staff is requesting schematics and necessary logic diagrams associated with the discrete (non-software) portions of the device
4. At the March Audit in Kobe, the staff observed that the communications interface portion of the PIF module was implemented using an ALTERA field-programmable gate array (FPGA). Additionally, as with the MELTAC basic software, the FPGA development process did not originally incorporate adequate independent verification and validation. The entire lifecycle process of the software portion in the Communication
Interface Part, and other uses of FPGAs in the MELTAC platform, needs to be addressed in the topical report including the FPGA development process and how the communication interface part of the PIF module was approached in the UCP.
Similarities/differences with other software in the MELTAC platform would be advantageous to the staff understanding of this particular issue.
5. Section 4.1.2.4 also states "Therefore, periodic replacement is unnecessary in contrast to electro-mechanical relays." MHI is requested to add the expected service life of the PIF modules to substantiate this comparison.

Response
1, 2, 3, 5:
The priority of PSMS over PCMS functions is within the application logic. Therefore, this is addressed in MUAP-07004, Section A.5.6.3.1.

Since the priority logic within the PIF modules is part of the basic MELTAC platform, we will add the description and figures below in the Topical Report.
[

]
The entire PIF module, including the Communications Interface part is considered Class 1E. Therefore, the life cycle process for the development and maintenance of the firmware within

the Communications Interface part is the same as the firmware for all other MELTAC modules. During manufacturing and production, the PIF modules are all tested to confirm the soundness of communication operation, IPL logic operation, and output operation.

Schematics for the PIF module were provided at the MELTAC audit in Kobe.
[

]

Unlike electro-mechanical relays, the power semiconductor output of the PIF module does not degrade mechanically nor electrically and can be treated the same as any other general semiconductor device. Thus, the PIF modules are not considered to have any limitations in their expected service life. The components of the MELTAC platform that have a limited service life are identified in Section 7.5 Periodic Replacement Equipment (Parts) to Keep Reliability. The PIF is not included in this list.

4 – The topical report will be revised to include the development process for MELTAC FPGAs. This will include additional UCP activities. This issue will be addressed in the response to the NRC letter of July 10, 2009.

RAI-25

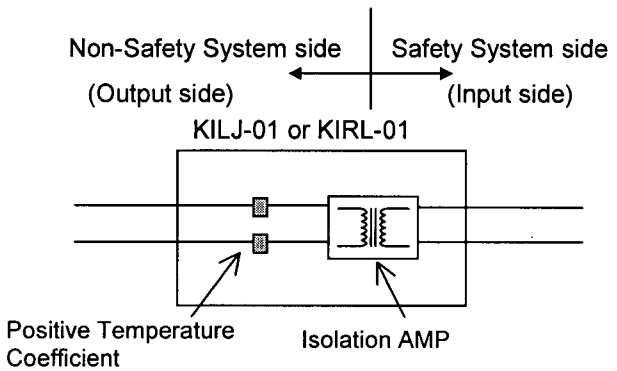
At the Jan. 22, 23 meeting MHI agreed to provide design information of the Isolation Modules identified in Section 4.1.2.3. Either by including in this Section or by separated docketed material, at a minimum the information should include:
1. Specific information, should be provided to explain the voltage isolation method (e.g. Transformer, opto-coupler) and current interrupting / limiting method (e.g. Thermistor, voltage regulator) by schematic or detailed description, of the circuits involved, how isolation circuit is maintained under all conditions and inputs.
2. How they are tested during manufacturing and production
3. How they are included in the equipment qualification program

Response

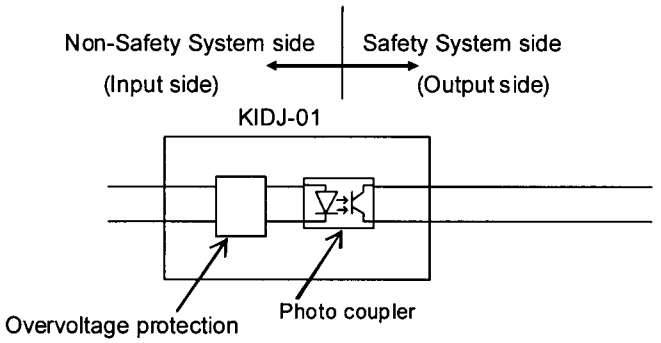
For the information on the isolation module, we will add the description and figures below in the Topical Report, Section **4.1.2.3 Isolation Module**. In addition, a description of the qualification testing will be added to Section 5.5. Schematics and qualification reports were provided at the MELTAC audit in Kobe.

Addition for Section 4.1.2.3:

The figure below shows the internal configuration diagram of the analog isolation modules KILJ-01 and KIRJ-01. For common mode faults, the input and output are electrically isolated by the isolation amplifier. The positive temperature coefficient device (e.g. PolySwitch ™) is used to limit overcurrent conditions for transverse mode faults. The positive temperature coefficient device raises its resistance value when it is heated by sustained overcurrent conditions.



The figure below shows the internal configuration diagram of the binary isolation module KIDJ-01. For common mode faults, the input and output are electrically isolated by a photo coupler. The over voltage protection circuit limits the current for transverse mode faults. The over voltage protection circuit consists of a transistor, FET, and high-resistance. The circuit converts to high resistance to restrict the current when a voltage that exceeds the FET gate voltage is supplied.



These isolation modules were included in qualification testing for temperature and humidity, seismic and EMI described in Section 5. Isolation fault testing was conducted, as described in Section 5.5.

Calibration of input circuit, output circuit and current limiting circuit is conducted for all modules during manufacturing. Functional input-output operation is also confirmed for all modules during production.

Addition for Section 5.5

[

]

[

]

[

]

[

]

[

]

RAI-26

MHI is requested to provide the Japanese QA standards, with the equivalent U.S. standards, that were used, if any, for the original software quality assurance program.

Section 3.0, "Applicable Code, Standards and Regulatory Requirements," states that "An assessment of the QA program in place during the original development of this Equipment is provided in this TR." Section 6.1.1 states "The original quality assurance program (referred to as Original QAP) used for the MELTAC Platform development was based on the Japanese Standard JEAG4101 and ISO9001." However, in a letter from Masahiko Kaneda to R. David B. Matthews, dated March 7, 2007, a table comparing U.S. and Japanese Quality Assurance requirements was provided in reference for the US-APWR design certification. In that table it states that "JEAG4101-1993 did not specifically address computer program testing" therefore no equivalent requirements to ASME NQA-1-1994, Part II, subpart 2.7, "QA Requirements of Computer Software," can be provided.

Response

MELCO's QA program for the original MELTAC basic software development was based on JEAG4101 and ISO9001. However, MELCO expanded the requirements of these standards in developing the current software quality program, which is defined in internal procedures [ ]; all of which have submitted for NRC review. These current MELCO QA procedures, along with their references to lower level software program procedures, are equivalent to ASME NQA-1-1994, Part II, subpart 2.7, "QA Requirements of Computer Software." As stated in Section MUAP-07005 Section **6.1.1 Overview of the MELTAC Quality Assurance Program:**

> The Original QAP and records of the Existing Platform have been assessed against these new procedures, to ensure suitable quality of the Existing Platform. The result shows the development process for the Existing Platform conforms to [ ] except the independent V&V requirement and other minor deficiencies.
>
> Therefore MELCO developed the MELTAC US Conformance Program (UCP), which is the combination of the corrective actions taken to compensate for differences between the Original QAP and [ ] and the assessment of the developed software by the independent V&V Team.

Therefore, since MELCO has assessed the original software development against [ ], and since the NRC has these software quality procedures for review, it is not necessary for MELCO to translate the Japanese QA standard JEAG4101 or compare the Japanese standard to US standards.

RAI-27

MHI is requested to identify the U.S. NRC recognized standards that would be equivalent to the Japanese Domestic Standards 84 through 87 of Section 3.0 and provide the translated English versions. Also, Section 4.1.1.4, "Environmental Specifications," identifies JIS-C0704-1995 as a Japanese standard.

MHI is requested to identify the U.S. NRC recognized standards that would be equivalent to, and identify the differences to, the Japanese Domestic Standards 84 through 87 of Section 3.0

Response

No.84 - JIS-C0704-1985 defines insulation test standards for control gear. There is no equivalent regulatory guide.
No.85 - JEC-210-1981 defines methods of dielectric test and values of test voltages for low-voltage control circuits in power stations and substations. There is no equivalent regulatory guidance.
No.86 - JEIDA-63-2000 is issued by the Japan Electronics and Information Technology Industries Association. This standard defines the environmental test conditions for industrial information processing and control equipment (temperature, humidity, power supply, EMI, etc.). For EMI the MELTAC equipment has been qualified to RG 1.180. The response to RAI 44 addresses other environmental testing.
No.87 - JEAG-4101 issued by the Japan Electric Association. This standard defines quality assurance requirements for equipment in nuclear power plants in Japan. MELCO has now adopted a 10CFR50 Appendix B quality program, as described in the response to RAI-26.

The Japanese Domestic Standards 84 through 87 of Section 3.0 were provided at the MELTAC audit in Kobe.

RAI-28

MHI is requested to identify, in the topical report, if in the single controller and redundant parallel configuration, the subsystem will stay in the Failure Mode after initial power activation then the power is momentarily lost.

Section 5.6.3.3, Effects of a Single Random Failure, of IEEE Std 603, states that " the remaining portions of the safety system shall be capable of providing the safety function even when degraded by any separate single failure."

Response

Section 4.1.1.2.1 Mode Management of Single Controller and Redundant Parallel Controller will be clarified as follows:

> The Subsystem initializes to the Failure Mode after initial power activation. The Subsystem also shifts to this mode automatically after it detects its own failure or there is a momentary loss of power (typically greater than 20msec).
> A Subsystem shifts from the Failure Mode to the Control Mode only by pushing the reset button on the Status Display & Switch module.

In the Parallel Redundant Controller, Subsystem-A and Subsystem-B operate independently with the Mode Management described above, including failure detection, loss of power detection and manual reset.

Single failure compliance is achieved through multiple controllers located in physically separate and independent safety divisions as described in Section 4.1.1.1 Concept of Configuration.

RAI-29

In Section 4.1.1.3, "Scale and Capacity," the software cycle time is identified between 20msec to 1 sec. This should be explained in the topical report relative to Section 4.1.3.1, Basic Software, also states that "If processing time exceeds 80% the application is divided into two or more controllers, as necessary." MHI is requested to identify in the topical report if the range for software cycle time is programmable or user definable once it is in the field. Also, is the 80% limit relative to the 20msec to 1 sec range?

Per BTP 7-21, Guidance on Digital Computer Real-Time Performance, timing measurements should meet projections or the anomalies should be satisfactorily explained. It is not clear how this technical position is met.

Response

The following note will be added to Table 4.1-1 Scale and Capacity in Section 4.1.1.3:

> The value between 20msec to 1sec is set in the application software F-ROM. This value is determined based on the application requirements. During the design phase, the system response time is predictably determined through analysis, as described in Section 4.4. This analysis confirms the ability of the system to execute all functions within the allowed software cycle time. In the Integration Test phase, the system response time is confirmed by measurement.

And Section 4.1.3.1 will be revised as follows:

> The processing time from No.2 to No.8 is based on the application logic and the input/output signal quantity of each system. Since the controller operates cyclically, the processing time can be 100% of the application requirement (ie. there is no application margin required for the system). However, to allow future system expansion, during the system design phase, the approximate processing time from No.2 to No.8 is calculated as described in Section 4.4 Response Time. If the processing time exceeds about 80% of the processing cycle required for the system, the application is divided into two or more controllers, as necessary.

RAI-30

Section 4.2.1.1, "CPU Module (PCPJ-11)," states the Futurebus+ will be used for data transmission using the Bus Master and Control Network Modules. Briefly describe the features of this bus architecture. Include if the data transfer is asynchronous and if all components will have separate clocks therefore not requiring time stamps to be provided by identified sources. The staff believes IEEE Std 603 Criterion 5.6, Independence, will be adequately met if asynchronous operation can be proven and the safety division is not dependent upon any information or resource originating outside its own safety division to accomplish its safety function. This is discussed in staff position 1.1 of DI&C-ISG-04.

Response

Futurebus+ is a bus standard defined by IEEE 896 1991. In the MELTAC platform, Futurebus+ is adopted as the back plane bus that connects between modules in the same subsystem in the CPU chassis.
The following will be added to section 4.1.2.1.1:

> The data transfer between the CPU module and other modules (ie, bus master module, control network I/F module, system management module) is asynchronous. All modules have separate clocks.

RAI-31

The topical report, in Section 4.1.2.1.6, should identify how the Status Display Module connects with the controller(s) and other devices giving it the capability to display the mode and alarms of the other subsystems. The topical report should indicate what and how it is displayed. Criterion 5.8.2, System Status Indication, of IEEE std. 603 states; "Display instrumentation shall provide accurate, complete, and timely information pertinent to safety system status.

Response

The status display panel is mounted on the same chassis as the CPU module, and is connected with the CPU module by wiring on the back plane. The status display panel displays the mode and the alarms of the same subsystem, and there is no connection with the other subsystems.

RAI-32

In Section 4.1.2.7.3, identifies a "fan stop detection circuit." Does this detect fan rotation or loss of power? MHI is requested to identify this in the topical report.

Response

The following description will be added to the Topical Report.

A fan stop detection circuit detects the decrease of fan rotation frequency by converting fan rotation frequency into a voltage pulse and monitoring the pulse length. If the pulse length reaches the length equivalent to the detected rotation frequency limit, the fan stop detection circuit de-energizes a relay, which generates a contact closing signal. Also, the same relay is deenergized if there is a power loss to the fan. Therefore, fan failure can be detected.

RAI-33

For Section 4.1.2.8, Power Supply Module, the staff has the following concerns that should be addressed directly in this section of the topical report:

1) Each of the different power supplies, identified within the different types, should be identified, explained and appropriately noted on Figure 4.1-8.
2) The question of the independent sources being different divisions of DC power is answered in 4.1.2.10. But what is meant by "as independent as practical" as explained in 4.1.2.10?
3) PS-1 & PS-2 are noted as mounted outside the chassis. A figure should be provided as to how and where they are mounted and why that is the case.
4) It is stated that overcurrent protection lowers the output voltage level but does not trip the unit. Is this always the case?
5) When AC power is lost, an alarm signal is sent to the Subsystem. Explain;
   (i) How this is done with no input power
   (ii) What the subsystem is?
   (iii) Where the subsystem is physically located in Fig. 4.1-8?

Response

The response is as follows.

1) In the Topical Report, we will identify all power supplies and add descriptions, and provide notes on Figure 4.1.8.
2) "As independent as practical" described in 4.1.2.10 means that the two power sources, should not have a realistic single malfunction point that would result insimultaneously failure. It is important to note that power redundancy is only for system available. There is no credit for this power redundancy in complying with the Single Failure Criteria of IEEE 379, since compliance to IEEE 379 is achieved by having separate trains.
3) PS-1 and PS-2 are mounted on the panel cut parts that are set right and left of the cabinet chassis as shown in the Figure 4.1-8. This mounting location was selected, rather than mounting them within the chassis for three reasons (1) this leaves space in the chassis for additional modules, (2) external mounting allows DC power to be supplied to the chassis from two redundant Power Supply Modules, (3) this location keeps the heat from the power supplies away from the modules, thereby improving module reliability.
4) The Power Supply Module lowers the output voltage level when an overload or output short-circuit occurs. The Power Supply Module provides a contact output alarm signal when an output shutdown occurs.
For a Redundant Standby Controller Configuration and a Redundant Parallel Controller Configuration, each Subsystem monitors the output condition of the other Subsystem's Power Supply Module.
For a Redundant Standby Controller Configuration, when there is a shutdown of the power supply module of the Subsystem in the Control Mode, the Subsystem in the Standby Mode shifts to the Control Mode. When there is a shutdown of the power supply module of the Subsystem in the Standby Mode, the Subsystem in the Control Mode generates an "Alarm".
For a Redundant Parallel Controller Configuration, each Subsystem warns "Alarm" if there is a shutdown of the power supply module of the other Subsystem.
5) As defined in Section **4.1.1.1.1,** "A Subsystem consists of a CPU Module, System Management Module, Status Display Module, Control Network I/F Module and Bus Master Module." For redundant controller configurations, there are two subsystems.

When the AC power input is lost, it is detected by the AC power reduction detection circuit within the power supply, and an alarm signal is output to the CPU Module. When the CPU Module receives an alarm signal for loss of AC power from its own Subsystem's Power Supply Module, the CPU module shifts to the "Failure" Mode before the Power Supply Module output voltage level becomes lower than the operable voltage of the CPU Module.
For a Standby Redundant Configuration, when the Subsystem in the Standby Mode detects the loss of AC power of the Subsystem in the Control Mode, the Subsystem in the Control Mode changes to the "Failure" Mode and the Subsystem in the Standby Mode shifts to the Control mode. When the Subsystem in the Control Mode detects the loss of AC power of the Subsystem in the Standby Mode, the Subsystem in the Standby Mode changes to the "Failure" Mode and the Subsystem in the Control Mode warns "Failure" of the Subsystem in the Standby Mode.
For a Redundant Parallel Configuration, when each Subsystem detects the loss of AC power of the other Subsystem, the Subsystem warns "Failure" of the other Subsystem.

RAI-34

For Section 4.1.2.9, Controller Cabinet, the staff has the following concerns that should be addressed directly in this section of the topical report:
1) The listing that identifies what is stored in the Controller Cabinet should all be identified in and consistent with Figure 4.1-8
2) Does each chassis consist of multiple modules and do these pullout to provide access to each module for replacement?
3) What modules can be replaced at power (i.e. hot swappable?). Describe the basis and system functional impact of the lack of hot swap capability, including any limiting conditions of operation, for any MELTAC system modules designed as such.
4) Does the configuration shown in Figure 4.1-8 represent the one which was seismically qualified? Or the configuration to be seismically qualified?

Response

1) The Optical Switch and Distribution Panel will be added to the list in Section 4.1.2.9 (a). The Isolation Chassis, which houses the isolation modules, and the Power Interface Chassis, which houses the PIF modules, will be added to Figure 4.1-8.
2) Each chassis consists of multiple modules. Each module pulls out and can be replaced without pullout of the chassis. This will be clarified in Section 4.1.2.9 (a).
3) The I/O modules can be replaced at power. The modules in the CPU chassis cannot be replaced at power. This will be stated in Section 4.1.2.9 (a). For redundant subsystem configurations power down of the CPU chassis for module replacement has no effect on the system operation, since the other subsystem remains operable.
4) Figure 4.1-8 shows an example of the rack up in the controller cabinet. Therefore, it doesn't completely agree to the one which was seismically qualified. The configuration of the qualification test specimen is shown in the Qualification Test Report **[ ]** which was provided at the MELTAC audit.

RAI-35

In Section 4.1.5, Self-Diagnostics, the staff has the following questions:

1) This section states "When the error is severe, the Controller makes a transition from the Control or Standby mode to the Failure mode." Completely discuss what errors are "severe", what errors do not require a transition, and how they are identified to the operator?
2) Each description of the three types of self-diagnostic features ends with an "etc." This apparently means there are other checks done but not identified here. MHI is requested to complete the list consistent with the current MELTAC platform basic software. If there are additional features to be added, will the reliability analysis be affected per IEEE 7-4.3.2? Will the cycle time calculation be affected?
3) In part 2) Alarm, states "The minor abnormality with which the system can continue" The topical should state specifically what these "minor abnormalities" are that the system can continue with.
4) In part 3) I/O Alarm states "the input values are kept as they are in the normal state" This section does not states what cause an I/O alarm. What is kept at normal state? And what is normal state?
5) At the January 22,23 meeting with the staff, MHI agreed to provide a description of how sself-diagnostics are checked during manual surveillance tests – memory and I/O. Also, a history of self-diagnostics success or failure (either factory or field data – field data is preferable) should be added. The topical report should demonstrate that manual tests 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

IEEE Std 7-4.3.2 provides the reasoning for types of diagnostics to be used and in when they should be used. It is not clear to the staff the full extent of the diagnostics that MHI is proposing and if the guidelines of this standard are met.

Response

1) The descriptions of all detected errors are in sections 4.1.5.2 to 4.1.5.5. Each description identifies the categorization in parenthesis. For example, Section 4.1.5.2.1a Watchdog Timer is identified as "(Failure)". To clarify this, Section 4.1.5 will be revised as follows: Each detected error is categorized into the three types (Failure, Alarm and I/O Alarm) as described below. Detailed error descriptions are provided in Sections 4.1.5.2 thru 4.1.5.5. The categorization of each error is shown in parenthesis, for example "Clock check (Failure)".
   All errors in Section 4.1.5.2 and 4.1.5.3 are severe and are therefore categorized as "Failure". These errors stop the main CPU operation, and generate signals that can be used for alarms. All other errors (those identified in Sections 4.1.5.4 and 4.1.5.5) generate signals that can be used for alarms, but do not stop the main CPU operation . All error signals are identified on the Engineering Tool. The specific grouping of error signals into operator alarms is application specific. Since most applications have redundant CPUs, typically all error signals are grouped to a single operator alarm and then the Engineering Tool is used for diagnosis of specific error conditions.

2) The descriptions of all detected errors are in sections 4.1.5.2 to 4.1.5.5. The self-diagnostic features are considered in the reliability analysis of each system at the application level. For safety systems the reliability analysis is typically included in the PRA. All self-

diagnostics are considered in the response time calculation method described in Section 4.4. Self-diagnostics that need a long processing time are conducted within the "remaining time" after application program execution, and are distributed over multiple cycles, as necessary, to ensure the application cycle time remains constant.

3) The descriptions of all detected errors are in sections 4.1.5.2 to 4.1.5.5. Each description identifies the categorization in parenthesis. Errors identified in Sections 4.1.5.4 and 4.1.5.5 do not stop the processor. Section 4.1.5.4 will be clarified as follows:

   4.1.5.4 Self-diagnosis of the Communication System

   See Section 4.3.2.4 and 4.3.3.3. Communication System errors are categorized as "Failure" or "Alarm", depending on the redundancy configuration of the controller.

   This is explained further in the response to RAI 43.

4) Failures that result in an "I/O Alarm" are identified in Section 4.1.5.5. Section 4.1.5.(3) will be modified as follows to clarify the failure mode:

   When the I/O Alarm occurs in the Single Input Module, the last good input values are retained and the Application Software is informed of the abnormal state of the input signals. For digital inputs, the input values are kept at the last value (1 or 0) before the error occurred. For analog inputs, the input values are kept at the last engineering value before the error occurred. Based on the error flag, the Application Software can be programmed for a predetermined control action.

5) In the next revised Topical Report, MELCO additionally describes the details of manual surveillance tests, the test result of self-diagnosis function in the factory test, and MELTAC failure records in the field. That record shows that the failures were correctly detected by self-diagnosis in operating plants. MELCO also additionally describes when and how the self-diagnosis is executed in the next Topical Report.

RAI-36

Also with regards to the guidelines provided in IEEE Std 7-4.3.2 on Fault detection and self-diagnostics, in Section 4.1.5.2.1, CPU Module, the staff has the following questions:

1) It is stated that the controller shifts to Failure mode "by a hardware mechanism" when the WDT is activated. What is this mechanism?
2) In the CPU health check, "pre-selected" operations are performed. What is the scope of those pre-selected operations?
3) In the "Software checks," it is stated that "an illegal software operation in the software or a malfunction in the hardware can be detected." Is this with the assumption that all illegal operations exceed the processing time? If not how are other "illegal operations" detected?
4) The clock check, as all others should as well, does not indicate what happens on failure.
5) The "Loop Back Check" describes the "The Bus Master module has four communication channels. The fixed data is transmitted from each channel to the Bus Master module." Provide a figure, or revise an existing figure in the topical report, that shows the four communication channels of the Bus Master module.

Response

The response is as follows.

1. The WDT timer output is hardwired to an interrupt control input of the CPU.
2. In the CPU health check, [

   ]
3. In the "Software check", the assumption is that all illegal operations exceed the processing time. This is a reasonable assumption because the process is completely cyclical and, as stated in Section 4.1.5.2.1[

   ]
4. Each self-diagnostic error is labeled as "Failure", "Alarm" or "I/O Alarm". The result of each condition is described in Section 4.1.5 items 1, 2 and 3, respectively. [

   ]
5. As described in Section 4.1.2.1.3, each of the four communication channels on the Bus Master module can be individually configured for I/O or data link communication. Figures 4.1-1, 4.1-2 and 4.1-3 show various configurations of the Bus Master module communication channels for I/O communication. Figure 4.3-5 shows the four channels of the Bus Master module configured for data link communication.

RAI-37

In the Power Source Check Section, Section 4.1.5.3 a), an error is detected when AC power input is interrupted. How is this tested? Is there an error message triggered when the output drops to a certain level but the AC power is still present?

This, again, leads to the staff's understanding of the MELTAC platform meeting the guidelines of IEEE Std 7-4.3.2 section 5.5.3, Fault detection and self-diagnostics.

Response

[

]

RAI-38

Section 4.2.1.2.1, Configuration of the Safety VDU Processor, part c) Control Network Interface should specifically state, and it should be shown on Figure 4.2-1, if the Control Network is inter or intra divisional.

Response

The Control Network to be connected to Safety VDU Processor is intra divisional.
It receives plant data from the controller within the same division and transmits plant control data to the controller within the same division.
Section 4.2.1.2.1 (c) will be clarified to explain that the Control Network and Safety VDU are both intra divisional.

RAI-39

In Section 4.2.2.1, Basic Software, it is stated "With fixed cycle control and no-interrupts, the Basic Software provides high reliability, and deterministic processing." Per Section 4.1.3.1, Basic Software, "Interrupts are not employed for any processing other than error processing." MHI is requested to revise the topical report to clarify the apparent contradiction. It should be further explained, in the topical report, what types of errors do cause an interrupt.

One of the purposes of BTP-21, Guidance on Digital Computer Real-Time Performance, is to assist the reviewer, and the applicant, in the extensive efforts required to verify techniques, such as interrupts. Use of interrupts can be a risky design practice, as this guidance suggests, MHI is requested to thoroughly explain the interrupt technique mentioned here.

Response

We will revise the description of 4.2.2.1 in the next revision of Topical Report, as follows:

> With fixed cycle control and no-interrupts (except processing of self-diagnostic errors detected by the hardware within the CPU Module and the Power Supply Module and categorized as "Failure" (see Section 4.1.5)), the Basic Software provides high reliability, and deterministic processing.

[

]

Section 4.1.3.1(b) will be clarified as follows:

> Interrupts are not employed for any processing other than processing of self-diagnostic errors detected by the hardware within the CPU Module and the Power Supply Module and categorized as "Failure" (see Section 4.1.5).

RAI-40

Section 4.3.2, Control Network states the network "can also be used to communicate data between different divisions including non-safety systems." Is the verb "can" the same as "is"? The following sentence supports the non committal claim by stating "This may be between multiple Controllers in different divisions." How is communication accomplished to all non safety systems in lieu of only "predetermined data size and structure" is used? Is there a dual port memory buffer to each interface between safety and non safety?

Response

The MELTAC Topical Report is intended to define the capabilities of the platform. The actual configuration of the platform for specific applications is described in other licensing documents. For example the configuration of the PSMS is described MUAP-07004. Therefore, the word "can" is used, rather than "is", since not all applications will utilized the inter-division communication capability of the Control Network.

All controllers connected to the Control Network, whether safety or non-safety, are equipped with Control Network Modules. All Control Network Modules have a dual port memory buffer. All nodes on the Control Network (safety or non-safety) utilize the same data structure. The data size for each node may be different. But once the data size is configured it is always the same for each node and for each communication cycle.

It is noted that the MELTAC Control Network is the name of a MELTAC communication technology. For the PSMS (see MUAP-07004) the MELTAC Control Network technology is used for each of the four separate Safety Busses which are each used only within the same division for safety related functions. The MELTAC Control Network technology is also used for the Unit Bus which is used for communicating non-safety functions between the safety and non-safety divisions (ie. between PCMS and PSMS). Inter-division communication for the safety functions of the PSMS uses only the MELTAC Data Link technology.

RAI-41

Table 4.3-1, Configuration of Control Network, needs to be further described beginning with resolution of the following staff comments:
1) What is meant by "needs of the application" for selection of the speed setting? Is this designed in? Is the speed setting configurable by the user? What makes the setting faster?
2) With regards to the section on the "communication signal";
 a) Why are analog signals listed?
 b) What is meant by "process signal" vs. "operation signal"?
 c) Is the term "system" a smaller subset of the entire control network?

In IEEE Std 1012-1998, which is endorsed by Reg Guide 1.168, performance criteria that includes attributes such as speed and critical configuration data should be included in the design life cycle. How the control network is configured and described needs to support how the guidelines of Reg Guide 1.168 is met.

Response
[

]

[

]

MELCO will revise the description of the topical report in this regard.

RAI-42

Section 4.3.2.2, Specifications, states: 1) "The optical G-bit Ethernet is used for the physical layer." How is the data throughput assured? What specifications are used for specification and testing? 2) "Each Control Network I/F Module is connected point-to-point to the adjacent Control Network I/F Module, as shown in the Table 4.3-1." MHI is requested to:a) Verify the reference to Table 4.3-1b) Since this is the only reference to point-to-point, it is assumed that this is the inter divisional communication reference. A figure should be referenced that shows the divisional boundaries.c) What types of information is sent between divisions? What is it used for?

Response

[

]

2-c) The specific inter-divisional communication data is application specific. The typical types of inter-divisional communication between safety and non safety are as follows:

- Operation signal from non-safety Operational VDUs to manually control the Safety components of each train
- Alarm or Status information from the Safety components or Safety instrumentation to Alarm VDUs, Operational VDUs, or non-safety controllers.
- Signals from non-safety control systems that control safety related equipment during normal operation, such as signals from the pressurizer level and pressure control systems to control Charging Pumps and Backup Heaters.

Inter-divisional communication for safety related functions is not implemented in the Control Network. For this application only data link communication is used.

RAI-43

In Section 4.3.2.4, Self Diagnosis, MHI is requested to identify in Table 4.3-3;

1) Which of the Items are fatal errors?
2) Which of the Specifications, if not met, represent a fatal or tolerable error?
3) How is the operators notified when any listed specification is exceeded?
4) When the transmission data error is checked by CRC, how many bits is it?
5) One specification states "The receiving-side Control Network I/F Module also detects a reduction light quantity in the optical communications." How is this done? What device doe this? Is this used anywhere else?

Response

In MELTAC, a Fatal error is defined as "Failure" and a tolerable error is defined as "Alarm" (see Section 4.1.5.). For Failure conditions, the main CPU stops operation; the main CPU continues operating for Alarm conditions. The application software determines the response to Alarm conditions. For loss of input data, options include using predefined values or the last good values. The categorization of self-diagnostic errors detected for the Control Network I/F module, as defined in Table 4.3-3 Self-Diagnosis Functions of Control Network, is described below:

[

]

[

]

2) See explanation for item 1. A "Failure" will stop the main CPU. An "Alarm" will not stop the main CPU, therefore function processing will continue. The handling of "Alarm" conditions by the main CPU is application dependent.

3) Failure notice is provided to the plant monitoring system for the three types of errors, "Failure", "Alarm", and "IO Alarm" (see Section **4.1.5 Self-Diagnosis)**. These error signals are typically grouped into system trouble alarms, however the method used to present this information to the operator from the plant monitoring system is application dependent and not within the scope of the MELTAC platform.

Detail information for diagnosis of all error conditions is provided on the Engineering Tool.

4) 32 bit CRC calculation is executed.

[

]

MELCO will revise the Topical Report to reflect the explanations described above.

RAI-44

In Section 5.1.2.2 states "The test conditions and test methods are based on industry standards in Japan." MHI is requested to identify, at a minimum, the comparable U.S. standards and preferably provide the comparison and any differences. This information is needed to confirm conformance to IEEE Std 603 criterion 5.4, Equipment Qualification and the associated standards.

Response

The U.S standard for environmental qualification is IEEE 323-2003. But IEEE- 323 does not define clear testing conditions nor the test methods. In addition, there are no qualification requirements for equipment located in mild environments. So for the temperature test, humidity test, temperature cycle test, hot-start test, and cold start test we referred to the Japanese Industrial Standard. The test methods and conditions are described in section 5.1 Environmental Test.

RAI-45

In Section 6.1.4, [

]

Response

[

]

RAI-46

In Section 6.1.5.7, Reviews, the Existing Platform Assessment states that [ ] How was this determined? Per BTP-14, "Of particular interest is the method by which the output of software tools, such as compilers or assemblers, will be verified to be correct. The criterion from IEEE Std 7-4.3.2-2003 is that software tools should be used in a manner such that defects not detected by the software tool will be detected by V&V activities. If this is not possible, the tool itself should be safety-related." Is there any evidence that the output of the complier was verified? If not, did V&V activities find defects that could not be detected by the complier?

Response

[

]

RAI-47

Section 6.1.5.7, Reviews also states that "The test data and test programs have not been under configuration control. However, they can be reconstructed by following the procedures in the test specifications, which are under Configuration Management." 1) If this is the case, all test results would only be available if the tests were redone?2) If this is the case, were they? 3) Could all failed test results be reconstructed? 4) Is there record of the reconciliation of the failed tests results?

These are only some of the attributes of what constitutes software test documentation. At a minimum the information that should be included to meet regulatory requirements as applied to software test documentation can be found in regulatory position C.1, Software Testing Documentation, of Reg Guide 1.171, Software Unit Testing. MHI is requested to address all the attributes of documentation required by the 8 bullets in position C.1. As per stated in this position "Any of the above information items that are not present in the documentation selected to support software unit testing must be incorporated as additional items." Therefore, MHI is requested to address the information that was not present in this manner, accordingly.

Response

[

]

RAI-48

In section 6.1.7.3, the Category-2 software units are only based on one operating cycle or more. No attempt to assure complete coverage of all input conditions is part of the evaluation of the operating experience. Why? In order to consider this to the fullest extent possible all input conditions should be addressed.

IEEE Std 7-4.3.2, endorsed by Reg Guide 1.152, in Annex C, (which is informative only), "Dedication of Existing Commercial Computers," does discuss the crediting of operating experience. However, as identified by Reg Guide 1.152, the NRC does not endorse Annexes B-F of IEEE Std 7-4.3.2. Operating experience is a consideration as part of the dedication process as identified in the staff's SER on EPRI TR-106439.

Response

[

]

RAI-49

Table 6.1-9, Software Upgrades Relation, discusses changing the basic software UV-ROMs and loading the application software using the Engineering Tool with the system on line. Regardless of the fact that there may be redundant controllers within the same division, the staff considers this in conflict to the guidance provide by ISG-04

Response

Section 4.3.4.2 Isolation already states:

[

]

For completeness, the following will be added to the Software Loading section of Table 6.1-9:

[

]

RAI-50

Section 6.1.12, Software Safety Plan, briefly discusses hazards and the V&V team ensures that these hazards are described in the system documents. However, it does not explain the type of hazard analysis that was done or if it was done at all. MHI is requested to explain this in the topical report.

BTP 7-14, Section B.3.1.9 describes the management, implementation, resource characteristics and the review guidance the staff uses with regards to Software Safety Plans. MHI is requested to address BTP-14 with regards to the Software Safety Plan in the topical report.

Response

[

]

RAI-51

Section 6.2.2.2, Troubleshooting Summary, discusses the information received on issues from the field on the MELTAC platform. Are there any time requirements for completion of the issues raised?
Is this implemented as part of or separate from a corrective action program as required by 10 CFR 50, App B?

Response

All activities described in Section **6.2.2 Failure and Error Reporting and Corrective Action are governed by MELCO's** 10 CFR 50, Appendix B quality program.

As stated in Section **6.2.2.2 (d) Monitoring the Progress Situation:**

> The resolution of complaints is monitored by using the fault database explained earlier. The Assigned Section expedites the evaluation and corrective actions process to promptly complete the correction.

There is no specific time requirement because it depends on the safety significance or operations significance of the problem and the complexity of the correction, including the required regression of life cycle activities.

RAI-52

Table 7.5-1, List of Periodic Replacement Parts, lists the frequency to replace the parts. How or what was the basis for the replacement cycle?
IEEE Std 603, Criterion 5.3, requires "Components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates."

Response

For the power supplies, the estimated lifetime of the internal electrolytic capacitor was calculated based on the Arrhenius equation. For the fuses in the fan assemblies, the estimated lifetime was determined by experience for the condition under which the fuse is actually used. The replacement interval of all of the above components was determined based on applying a 20% conservatism factor to the estimated lifetimes of these subparts.

RAI-53

Section 4.3.4.2 Isolation indicates electrical isolation of the Maintenance Network from the System Management Module as required by IEEE 603-1991, Clause 5.6 for independence of the Class 1E system. IEEE Std 384 provides methods that are acceptable for electrical isolation of Class 1E and non-Class 1E circuits.
Section 4.3.4.2 indicates that MELTAC platform was qualified in the configuration shown in Figure 4.3-8. This isolation method as shown would be in compliance with the requirement for independence and the regulatory guidance for electrical isolation. However, no device for electrical to optical isolation of an Ethernet connection is indicated in Table A.7. Also, the system demonstrated at the audit in Kobe, March 2-6, 2009 was not configured with any electrical isolation between the safety system and the Maintenance Network. Please identify the electrical isolation module by part number and indicate its qualification records and verification and validation testing that should be considered as part of the MELTAC platform. This information should include:

- The unit tests for verification and validation of the Ethernet isolation devices.
- Integration tests for both hardware and software of the MELTAC platform showing the proposed configuration of safety system connection to the non-safety Maintenance Network with electrical isolation.
- Seismic qualification reports of the Ethernet optical isolation device.
- Environmental qualification of the Ethernet optical isolation device.

Please provide English translations of these engineering records for audit purposes.

Response

Engineering records that include the following information will be available for audit by January 2010.

- Seismic qualification reports of the Ethernet optical isolation device which include the configuration of the safety system connection to the non-safety Maintenance Network.
- Environmental qualification of the Ethernet optical isolation device which include the configuration of the safety system connection to the non-safety Maintenance Network.

It is noted that since the only safety function of the Ethernet optical isolation device is to prevent electrical fault propagation, the Seismic qualification and Environmental qualification tests are conducted only to demonstrate there are no failures in the isolation device that cause adverse interaction with the safety system. In addition, since the Ethernet optical isolation device is a hardware component, there are no additional unit tests for V&V of the isolation device.

RAI-54

Figure 6.1-4 indicates the security measures for the software development. No engineering procedure for this process is indicated. During the March 2-6, 2009 audit, no clear procedure was cited for the configuration management, and it seemed not to be a formal procedure but the process was an undocumented customary practice (other than the figure generated for the topical report). The use of a formal procedure would strengthen the reliability of the process and ensure continuity of the configuration management process if personnel change.
Please provide appropriate references to engineering procedures for the configuration management of the controlled copy of the MELTAC basic software that ensure that the controlled copy stored in the CEAS has completed all require qualification and resolution of anomalies in development and that the actual final version. Please indicate the positions of the persons responsible for each step so that a clear chain of responsibility for configuration management is established for the controlled copy of software.

Response

[

]

RAI-55

During the March 2-6, 2009 audit, a review of the MELCO system for tracking and resolving problems with hardware and software was performed. The database serves a dual purpose: first to provide a computerized mechanism to track problems to their resolution and second for long term storage of reliability data. The database is used to track individual problems that have been reported, to follow average performance of the problem resolution process, and for tracking trends in reliability of components. The data that are retained are a relatively simple group of fields but offers a useful collection of information on the MELTAC hardware and software.
The data in this reliability database system are apparently part of the engineering data being used for justifying Category 2 software in the MELTAC basic software that is not subjected to independent V&V in Chapter 7 of the topical. To fully credit the use of historical performance in the MELTAC software qualification, considerably more information about the reliability database and the procedures used by MELCO to ensure its integrity. Please document the MELCO reliability database, its uses in MELTAC software reliability, and summary data on the software and hardware failures that have been recorded.

Response

[

]

RAI-56

As per 10 CFR 50.47(a)(9), Content of Applications; technical information, in part, states an evaluation shall be provided to include all differences in the design and those corresponding SRP acceptance criteria.

In Section 3.0, "Applicable Code, Standards and Regulatory Guidance, many Branch Technical Positions are listed which do not have statements of conformance or, more importantly, to direct where statements of conformance can be found. Also, statements are made that there is conformance to a Reg. Guide. This can not imply conformance to the Standard Review Plan. Example; item 43 is BTP HICB-14, "Guidance on SW Reviews for Digital Computer-Based I&C Systems" states "see conformance to RG 1.168 thru 1.173." MHI is expected to provide and substantiate conformance to the standard review plan, or if the MELTAC process does not conform, then the differences should be identified, evaluated and presented to the staff.

Response

The next revision of the Topical Report will include statements of compliance for all Branch Technical Positions. In most cases where a statement of compliance was not previously included, it is because compliance is achieved at the application level, not by the MELTAC basic platform. This will be clarified in the next revision.

RAI-57

At the Jan 22, 23 meeting, MHI committed to provide more detail on the I/O bus. Explanation, in the topical report, should be provided of how all I/O bus communications are the same including communications with the PIF module. Figures should label the type of communications used (e.g. Future bus (backplane), control network, I/O bus, data link etc)

Response

The networks outside the controller, such as controller network, datalink, and maintenance network, are described in the Section 4.3 of the Topical Report.
The following will be added to Section 4.1.6 of the Topical Report to describe the communication within the controller:

4.1.6 Bus inside the controller

Table 1 shows the two busses used inside the controller.

Table 1 Bus inside the controller

Item	Application
Futurebus+	Backplane bus in the CPU chassis. It is used to connect modules in CPU chassis and transfers other module data in the CPU chassis.
I/O bus	A bus that connects the CPU chassis and the I/O module. See Table 2 for detail.

Table 2 I/O BUS specification

Item	Specification
Protocol	1:N master poling
Configuration	Maximum 64 I/O modules can be connected to one I/O bus. (Up to 16 I/O modules can be mounted on one I/O chassis and up to six chassis can be connected to one I/O bus.). There are four I/O busses on each Bus Master module and each controller can have eight Bus Master modules.
Interface	RS-485 transformer isolation.
Baud rate	1Mbps
Error detection method	CRC check
Operation	The bus master module and the I/O modules are connected to the I/O bus. The bus master module sends output data and input data requests to the I/O module and the I/O module responds to that. This communication method is common in to all I/O modules, including the PIF module.

RAI-58

10 CFR 52.47(a)(22) requires applicants to incorporate into their plant designs relevant operating experience. Information Notice 2005-25 describes an event at the Millstone plant where a tin whisker resulted in a reactor trip. Although the risks of tin whiskers increases with the use of lead-free solder material, the electronics industry is moving away from lead-based solder material due to the environmental concerns with such material. At the recent audit in Kobe, Japan, inspection of the manufacturing process yielded these concerns which the staff is requesting a response to:
1) The staff questioned how much of the MELTAC production process is leadfree,
2) If any part is still lead based will the availability require change to all lead free in the near term.
3) The staff requested what the mitigation strategy that MELCO is currently using and will use in the future as the lead free process becomes predominate.
4) At the Jan 22, 23 meeting with the staff, MHI agreed to provide a summary for history of changes of the MELTAC platform in the topical report including reason for change (eg. Software error, functional performance improvement, etc.)

Response
[

]

4) The summary for history of changes of the MELTAC platform will be provided in the topical report in Section 7.

RAI-59

For the staff to further assess compliance of the MELTAC platform to Criteria 5.6, Independence, of IEEE Std. 603, the following must be addressed in the topical report with regards to the synchronization activities between CPUs. [

]

Response

The following will be added to Section 4.1.1.1.2 Redundant Parallel Controller Configuration:

> The Redundant Parallel Controller Configuration is shown in Figure 4.1-2. This configuration can only be used within the same division (ie. the redundant subsystems cannot be in different divisions), because there is no electrical or functional independence between subsystems.

RAI-60

The topical report should describe what happens if the installed hardware and software do not match (eg. the wrong hardware module is installed – input, output, CPU, communication, etc, or the wrong software is installed that does not match the installed hardware).
Evaluation of computer system hardware integrity should be included in the evaluation against the requirements of IEEE Std. 603-1991. Computer system software integrity (including the effects of hardware-software interaction) should be demonstrated by the applicant/licensee's software safety analysis activities.

Response

Section 4.1.5.6 of the Topical Report will be added to explain the operations when the hardware and software do not match, as follows:

Mismatch of the module configuration in the CPU chassis:
The CPU module detects the error and the subsystem turns to failure mode.

Mismatch of the module configuration in the I/O chassis:
The CPU module detects the mismatch and notifies the application software logic that the I/O signals have bad quality, as explained in Section 4.1.5. Currently, the subsystem does not transfer to Failure, Alarm, or I/O Alarm and does not give an alarm. However, the MELTAC basic software will be modified to add an I/O Alarm for this condition. This modification is being executed as a design change, because this I/O Alarm was not required by the original MELTAC specification.