

~~OFFICIAL USE ONLY – PROPRIETARY INFORMATION~~

June 29, 2016

Gilbert W. Remley
Nuclear Systems Department Manager
Mitsubishi Electric Power Products, Inc.
547 Keystone Drive
Warrendale, PA 15086

SUBJECT: REQUEST FOR ADDITIONAL INFORMATION FOR THE “SAFETY SYSTEM DIGITAL PLATFORM – MELTAC – [MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER] TOPICAL REPORT REVISION 0” (TAC NO. MF4228)

Dear Mr. Remley:

By letter dated April 30, 2014 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML14272A382), Mitsubishi Electric Corporation (MELCO) submitted for U.S. Nuclear Regulatory Commission (NRC) staff review the topical report (TR), “Safety System Digital Platform - MELTAC - Topical Report Revision 0” (ADAMS Accession No. ML14121A413). By letters dated September 26 and December 30, 2014, January 30, March 31, and April 28, 2015 (ADAMS Accession Nos. ML14272A382, ML14364A132, ML15033A073, ML15090A620 and ML15118A661), MELCO supplemented the application.

Upon review of the information provided, the U.S. Nuclear Regulatory Commission (NRC) staff has determined that additional information is needed to complete the review. In an email exchange with Mr. Ken Krayvo representing MELCO, it was agreed that the NRC staff will receive your response to the enclosed Request for Additional Information (RAI) by mid-August, 2016. Some RAIs may need a pre-submittal discussion, so it is agreed that the NRC staff will receive response(s) by the submittal dates determined after this discussion.

~~OFFICIAL USE ONLY – PROPRIETARY INFORMATION~~

~~OFFICIAL USE ONLY – PROPRIETARY INFORMATION~~

G. Remley

- 2 -

If you have any questions regarding the enclosed RAI, please contact me at 301-415-7297 or Joseph.Holonich@nrc.gov.

Sincerely,

/RA/

Joseph J. Holonich, Sr. Project Manager
Licensing Processes Branch
Division of Policy and Rulemaking
Office of Nuclear Reactor Regulation

Project No. 751

Enclosure:

1. Nonproprietary RAI questions
2. Proprietary RAI questions

NOTICE: Enclosure 2 transmitted herewith contains SUNSI. When separated from the enclosure 2, this transmittal document is decontrolled.

~~OFFICIAL USE ONLY – PROPRIETARY INFORMATION~~

~~OFFICIAL USE ONLY – PROPRIETARY INFORMATION~~

G. Remley

- 2 -

If you have any questions regarding the enclosed RAI, please contact me at 301-415-7297 or Joseph.Holonich@nrc.gov.

Sincerely,

/RA/

Joseph J. Holonich, Sr. Project Manager
Licensing Processes Branch
Division of Policy and Rulemaking
Office of Nuclear Reactor Regulation

Project No. 751

Enclosure:

- 1. Nonproprietary RAI questions
- 2. Proprietary RAI questions

NOTICE: Enclosure 2 transmitted herewith contains SUNSI. When separated from the enclosure 2, this transmittal document is decontrolled.

DISTRIBUTION:

PUBLIC	RidsACRS_MailCTR	RidsNrrDprPlpb	PLPB R/F
RidsOgcMailCenter	RidsNroOd	RidsResOd	
RidsNrrLADHarrison	RBeacom	RStattel	MWaters

ADAMS Accession No.: Package: ML16124A012; Proprietary RAIs: ML16083A111

Letter and nonproprietary RAIs ML16124A013

NRR-106

OFFICE	DPR/PLPB/PM	DPR/PLPB/LA*	DE/EICB/BC	DPR/PLPB/BC	DPR/PLPB/PM
NAME	JHolonich	DHarrison	MWaters (RStattel for)	KHsueh	JHolonich
DATE	05/10/2016	05/26/2016	06/ 20 /2016	06/ 29 /2016	06/ 29 /2016

OFFICIAL RECORD COPY

REQUEST FOR ADDITIONAL INFORMATION #1
MITSUBISHI ELECTRIC COMPANY- MELCO
SAFETY SYSTEM DIGITAL PLATFORM
MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER- MELTAC
TAC NO. MF4228

Topical Report (TR), JEXU-1041-1008, "Safety System Digital Platform – MELTAC"
(Agencywide Document Access and Management System (ADAMS) Accession
No. ML14121A416):

1. Title 10 of the *Code of Federal Regulations* (10 CFR) Part 50, "Domestic Licensing of Production Utilization Facilities, establishes fundamental regulatory requirements. Specifically, Appendix B, "Quality Assurance Criteria," Criterion II, "Quality Assurance Program," states, in part; "This program shall be documented by written policies, procedures, or instructions." Page 0-6 of the TR states "the information provided in this report covers the life cycle and the Quality Assurance Program (QAP) of the MELTAC platform." In other inferences throughout the document, there are references to "10 CFR Part 50 Appendix B QAP" or just "QAP" or "MELCO QAP." The U.S. Nuclear Regulatory Commission (NRC) staff notes there is also a separate QAP for non-safety items. It is therefore unclear to the NRC staff how this requirement for specific written policies, procedures, or instructions is met and thus the staff is unable to make a regulatory compliance determination. Please provide information to identify each QAP by title, number, date, and revision which is proposed to meet the requirements (or not) as stated by 10 CFR Part 50 Appendix B, Criterion II.
2. On page 2 of the TR, the following General Design Criteria (GDC) are also applicable to the MELTAC platform. Please review criteria provided in these GDC's and describe how the platform satisfies each GDC. If regulatory compliance is dependent on application specific development activities, please state this.
 - a. GDC 13, "Instrumentation and Control," is applicable. MELTAC and the qualified displays, with no identified limitations within the system descriptions, will monitor variables and systems during normal operations, anticipated operational occurrences (AOOs), and accident conditions as well as those which affect the fission process and core pressure boundaries. Include a full explanation applicable to this GDC.
 - b. GDC 20, "Protection System Functions," is applicable. MELTAC will automatically initiate reactivity control systems. Include a full explanation applicable to this GDC.
 - c. GDC 25, "Protection System Requirements for Reactivity Malfunctions," is applicable. The MELTAC platform will be used for safety and non-safety systems for reactivity control systems without limitations identified by the topical report. Also the capability to protect against reactivity control malfunctions is not an exception therefore this requirement should be included.

3. With regard to TR page 17, item d), software is mentioned several times regarding the capabilities of the engineering tool. In each case, identify if this is referring to the application or platform software or both.
4. With regard to TR page 54, a) "Creation of Application Softwar." Criterion III, "Design Control," of 10 CFR Part 50 Appendix B states in part: "Design changes, including field changes, shall be subject to design control measures commensurate with those applied to the original design and be approved by the organization that performed the original design unless the applicant designates another responsible organization." To determine compliance with this criteria, the NRC staff needs to understand whether the MELCO development process described by this application will be used to perform design changes or if a different process to be developed by the licensee would be used. If a different process is to be used, then an application specific action item should be developed accordingly to make clear to the licensee that an appropriate safety-related development process must be established before the engineering tool is used to revise platform software.
5. With regard to TR page 55, e) in order to complete its evaluation of the MELCO platform the NRC staff needs to understand the temporary changes to field changeable process value in data table (Data Set). Please provide a description and examples of temporary changes to field changeable process values.
6. With regard TR Page 54, in Section 4.1.4.1, Function Description, subsection b) states this activity is done with the central processing unit (CPU) module in the re-programming Chassis and therefore the controller status is off line; however; subsections c), d), and e) do not include similar statements. Please provide additional information regarding controller status in relation to performing functions described in subsections c), d), and e).
7. DI&C-ISG-04, Section 1, Interdivisional Communications, Point 6, states the safety function processor should not accept interrupts from outside its own safety division. Page 56, third paragraph, states; [

.] Provide information on how the engineering tool is prevented from disrupting the controller safety functions.
8. Page 76, Section 4.1.7.2, Memory Integrity Check (MIC), describes an activity that is part of the verification program for the MIC software tool. Per ISG-06, Section D.10.4.2.3.2, the information needed for the NRC staff to reach a determination that the software tools are adequate for their intended use should be contained in the documentation for the software tool verification program. Therefore, provide the procedure for the verification of the MIC tool to demonstrate adequacy. In addition, please clarify the following: How far along is the development of the MIC? Is it currently in use by operating plants? Please explain if all of the system memory locations are checked during this activity including data locations and unused memory.

9. Page 214 of the TR discusses the generic redundant parallel controller reliability analysis and a fault tree analysis to support that controller configuration review. The NRC staff needs to review this specific analysis and additional analyses for other controller configurations and modules that are included in the MELCO platform to complete its evaluation in accordance with ISG-06 Section D.9.4.2.1.1. Please provide a description of the criteria used to determine which controller configuration will be used (i.e., single, redundant parallel or redundant standby) as well as documentation to demonstrate compliance of other possible controller configurations to this criteria.

JEXU-1041-1022, "Summary of MELTAC Platform Design" (ADAMS Accession No. ML15033A076):

1. Software Requirements Specification (SRS) and Software Design Specifications (SDS):
 - a. The summary document, JEXU_1041-1022, states the MELCO document which contains the information for a software requirements specification is "MELTAC-Nplus S System Specification," Section 4.1, "System Specification (Platform Specification)." The summary document provides the table of contents of the system specification but not the specification itself. The NRC requires system specifications to support its safety evaluation. The NRC staff has endorsed Institute of Electrical and Electronics Engineers (IEEE) Standard 830-1998, "IEEE Recommended Practice for Software Requirements Specifications," by Regulatory Guide (RG) 1.172. Also, the NRC Standard Review Plan (SRP) Section 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems," Section B.3.3.1 provides acceptance criteria for a SRS. Additional guidance can be found in NUREG/CR-6101, Sections 3.2.1 and 4.2.1. The acceptance criteria using these references is delineated in ISG-06 Section D.4.4.3.1. The summary document points to JEXU-1024-1010, "MELTAC-Nplus S System Specification." Therefore, the staff requests this document be submitted on the docket with an analysis of conformance to the acceptance criteria, or any alternatives, to RG 1.172 and the applicable sections of the SRP, Section 7.14, specifically identified.
 - b. ISG-06, Section D.4.4.3.3, references the acceptance criteria for the software design specification including the SRP Section BTP 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems," Section B.3.3.3, "Design Activities – Software Design Specification (SDS)." This guidance provides functional and process characteristics as well as review guidance of SDSs.

Provide an explanation how the following documents, identified in Table 1 and Appendix A, provide the information for the controller CPU module to conform to the Software Design Specification guidance stated above. Also the NRC staff requests these documents be submitted on the docket:

Hardware Requirement Specification, JEXU-1024-1021,
Hardware Specification, JEXU-1024-1051,
Software Specification, JSX4L400,

FPGA Specification, JEXU-1024-1071.

2. Thoroughly explain the statement on page 1: "Since the development of the MELTAC Platform is ongoing, only auditable documents are listed in Appendix A." The staff needs to understand the extent of the ongoing development process and the limitations of document availability. Please identify by specific type what activities, equipment, and procedures are not complete and why the changes are taking place including those involved in the MELTAC Reevaluation Program. Also include the schedule to complete the development.
3. The MELTAC-N plus S Basic Software Update Project was not scheduled to be finished until after the NRC inspection in 2011, therefore, the NRC inspection team limited its review to completed supporting documents for the requirement, software design, implementation, and maintenance phases. (Note: this did not include testing or the test plans). Identify when this was completed or identify any activities yet to be completed, by procedure, and identify the schedule for completion.

JEXU-1042-1031, "MELTAC Platform Software Tools" (ADAMS Accession No. ML15118A661):

1. Page 4, List of Software Tools Category Used in Each Phase:
 - a. In order for the NRC staff to evaluate software tools for compliance with IEEE 7-4.3.2, Section 5.3.2, we will need to understand what the tools are used for as well as what functions they perform in relation to the MELCO safety software development processes. The software tools listed in Table 1 are not consistent with names of the software tools provided in Section 5.0, Detailed Description of Processes. Please clarify the specific function of the tools and identify what document describes the function of each tool. The response should include a description of what the rules are for using the tool correctly and what configurations or options are recommended or advised against.
 - i. By further example of what the NRC staff needs to understand is the functions of the Engineering Tool. Section 4.1.4.1, Function Description of the TR, states the functional block diagrams are converted to graphical block diagrams by the MELTAC engineering tool. Section 5.7, MELTAC Engineering Tool, does not describe this function. Please explain.
 - b. Please provide an assessment of how each tool conforms to the software tools criteria of IEEE 7-4.3.2, Section 5.3.2 for the tools listed below:
 - i. []
 - ii. []
 - c. Identify the lifecycle phases that the MIC will be used in as was done with the other software tools on Table 1.

- d. Clause 5.3.2 of IEEE 7-4.3.2 specifies that software tools used to support software development are controlled under a configuration management plan. To evaluate compliance with this requirement, the NRC needs to review plans and procedures for establishment and maintenance of tool configuration control. Please provide documentation to show how tool configurations are controlled and Identify procedures used to maintain tool configuration control.
2. Page 15, Section 5.0, of this document, "Detailed Description of Processes," does not identify the procedure used to initially select, track, and maintain the specific software tool suppliers that are identified in this section. BTP 7-14, B.3.1.11.2, states that the a description of the process used to maintain and track purchased items, such as software tools used to make the final product should be provided. BTP 7-14 goes on to state this qualification procedure should be provided, and a method of tracking tool history, bug lists, and errata sheets should enable tracking which design outputs may be affected. Please provide this qualification procedure on the docket for NRC staff review.
3. [], Page 23, Section 5.8.2.2 "Verification & Validation (V&V) Method," of this document states the same V&V process applies to the MIC tool as the safety system software per the MELTAC Platform Software Program Manual (SPM). The NRC staff needs to understand the applicability of the SPM to the MIC and the Appendix B process. Therefore, provide the final V&V Report, per Section 3.10.4.8 of the MELTAC Platform Software Program Manual, which was completed for the MIC tool on the docket. Also, please reference and provide the procedure which includes the instructions for completing the V&V report for software tools.
 - a. Section 5.8.1 of this description identifies the MIC function of the MELENS software is developed and managed under Appendix B but the previous page and Section 5.7 states the MELENS software is developed as non-safety. The NRC staff requests the description of []. How is separation maintained for development and maintenance purposes? Is there a separate sign-on for access to the MIC function?
4. Criterion V of Appendix B of 10 CFR Part 50 requires, in part, "Activities affecting quality shall be prescribed by documented instructions," and this Criterion also states "Instructions shall include appropriate acceptance criteria." (See RAI 2 of JEXU-1041-1008). In this document, Page 24, Section 5.9.2, 2), states: "[]" Provide the V&V procedure that describes the acceptance criteria used to determine the write operation of the tool is successful by reading the result of the tools listed.
5. The NRC staff needs a clear understanding of where 10 CFR Part 50 Appendix B applies and where is it not applicable in order to complete the evaluation. []

JEXU-1041-1018, "Summary of Compliance to the IEEE Std. 603 and IEEE Std. 7-4.3.2"
(ADAMS Accession No. ML15149A310):

1. Regarding page 10, Table 3, of this document, IEEE 603, 5.11, Identification. Does MELCO have an identification system of hardware and software applied during the design and manufacturing of the generic platform? If so this requirement applies and the NRC needs to evaluate how it is implemented. Please provide a description of platform hardware and software identification methods to demonstrate compliance with this requirement.
2. Also on page 10, Table 3, IEEE 603, 5.14, Human Factors. This requirement includes how certain safety system design goals should be met in accordance with IEEE 1023. This includes maintenance of the displays (safety VDUs) which provides assembly/disassembly, tools required and interchangeability of parts as well as features to prevent incorrect assembly. The staff requests information including an explanation of why such an evaluation would not be required on a generic basis (versus application specific) for the safety VDUs.
3. Page 12, Table 3, IEEE 603, 6.6 and 6.7, Operating and Maintenance Bypasses. Confirm for the NRC staff that the generic platform has the capability to complete these two requirements. It is understood by the NRC staff that specific operating bypasses are defined on a plant specific basis as well as plant specific Technical Specifications govern the use of the maintenance bypass feature.

JEXU-1041-1015, "Conformance Analysis to ISG-04" (ADAMS Accession No. ML14269A141):

1. With regards to the response to Staff Position 2; the last sentence of staff position 2 is not addressed, that is "This protection must be sustained despite any operation, malfunction, design error, communication error, or software error or corruption existing or originating outside the division." Please provide additional information to demonstrate compliance with this position.
2. With regards to the response to Staff Position 3; is the "vital communication" division voting logic the only input coming from outside the division (i.e., request for actuation coming from the other divisions)? If not what are the other inputs coming from outside the division that is necessary for the generic platform?
3. With regards to the response to Staff Position 4; this is the only place the communications processor is a "to be determined" processing technology. Discussion within this section and the topical report, such as section 4.3.3.5.1, "Detailed Data Flow," identifies this as a []
]. The NRC staff requires the technology of the communications processor to be determined and consistent with the design, process, and procedures. If this processor is yet to be determined, or is being changed, the NRC staff needs to be notified of the changes.
4. With regards to the response to Staff Position 7, the NRC staff requires additional information on the characteristics of a predefined data set used in MELTAC

communication interfaces to support its safety evaluation. This information should include message formatting and protocol, message identification, status information, as well as signal attributes such as point of signal origin and destination. Include a discussion of how unrecognized messages are handled.

5. With regard to the response to Staff Position 10, the NRC staff requires the following:
 - a. A description of what constitutes a “temporary change”
 - b. The NRC staff requests the procedure describing how user configurable constants, such as setpoints, time delays, or instrument ranges will be changed with the CPU module mounted in the dedicated re-programming chassis.
6. With regard to the response to Staff Position 12, the NRC staff does not have information needed to perform an evaluation of faults 1 through 12 identified in this staff position. Please provide a discussion of how each of these faults as well as any additional identified communications faults will be handled by the MELCO safety platform and identify any application specific features needed to support system response to such faults.

JEXU-1041-1025, “Summary of MELTAC Platform QA,” Rev. 1 (ADAMS Accession No. ML15090A625):

1. Criterion XVIII, Audits, of 10 CFR Part 50 Appendix B states, in part, “audits shall be carried out to verify compliance with all aspects of the quality assurance program.” This Criterion goes on to state “Audits shall be performed in accordance with check lists by appropriately trained personnel not having direct responsibility in the areas of the audit.” Also, the Criterion states: “Followup action, including reaudit of deficient areas, shall be taken where indicated.”

The NRC Inspection (ADAMS Accession No. ML12013A353) was limited to assess MELCO’s compliance to selected portions of 10 CFR Part 50 Appendix B. Also the NRC staff review is not intended to determine compliance of the MELCO ESC QAP program to all the requirements of 10 CFR Part 50 Appendix B or 10 CFR Part 21. Rather the intent of this review is to determine if the elements of the MELTAC Platform hardware and software meet the regulatory requirements necessary to reach a reasonable safety determination. Many of the elements have their basis within the Criteria of 10 CFR Part 50 Appendix B and should be reviewed and identified in Appendix B supplier audits. Since MELCO has not fully developed and manufactured a complete MELTAC platform under its 10 CFR Part 50 Appendix B program the staff must understand the many issues identified during Mitsubishi Heavy Industries (MHI) Appendix B audits of MELCO. Please provide the resulting corrective actions for issues identified during the following MHI Appendix B audits of MELCO:

- a.
 - i. []
 - ii. []
 - iii. []

