MEETING MINUTES

February 3, 2010, Meeting with Mitsubishi Heavy Industries, Ltd. to discuss Safety Instrumentation and Controls Description and Design Process Topical Report, Safety Systems Digital Platform - Mitsubishi Electric Total Advanced Controller (MELTAC) Topical Report and the United States - Advanced Pressurized Water Reactor (US-APWR) Design Control Document (DCD) Chapter 7.

<u>SAFETY INSTRUMENTATION AND CONTROL (I&C) SYSTEM DESCRIPTION AND DESIGN PROCESS</u>

The U.S. Nuclear Regulatory Commission (NRC) staff opened discussions by stating that the Office of Nuclear Reactor Regulation (NRR) will discontinue review of the Safety I&C Topical Report for Operating Reactors because the topical report doesn't contain sufficient information to make a safety determination. The Office of New Reactors (NRO) staff also recommended that the Safety I&C Topical Report be withdrawn and resubmitted as a technical report.

The NRC staff presented technical issues with the Safety I&C topical report, including safety functions, priority logic, protection actions, engineering tool, quality assurance, and supporting documents.

The following action items are the result of discussion:

1. NRR will not review the Safety System Topical Report, and Mitsubishi Heavy Industries, Ltd. (MHI) accepted.

2. The NRC recommended that the Safety I&C Topical Report be withdrawn and resubmitted as a technical report. MHI agreed to resubmit the Safety I&C Topical Report as a technical report.

3. MHI will add that Safety Video Display Units (VDU) is the credited Human Systems Interface (HSI) for manual operator actions.

4. For Safety VDU, MHI will clarify the meaning of "can have priority"; explain that Safety VDU can cut off commands from Operational VDU at the train level, and explain that automatic safety signals always have priority; identify exceptions.

5. MHI will explain that Figure 5.1-3 is a typical logic diagram, which represents priority of safety commands over non-safety automatic commands and explain that only some components have non-safety automatic commands and that unused functions will not exist in actual software.

6. MHI will modify Section 4.2.2 to explain that all Engineered Safety Feature Actuation System (ESFAS) functions are latched at the train level, and that the ESFAS must be reset at the train level before components can be repositioned at the component level.

Enclosure 2

Explain that Pull-Lock is an exception to this, since Pull-Lock allows the component position to be changed at any time (i.e., prior to reset at the train level). Also explain that Pull-lock allows the ESFAS to be blocked.

7.   The NRC staff presented that Section 3.5.1.2, identifies logic that prioritizes the signals from the Operational VDU and Protection and Safety Monitoring System (PSMS) is contained in the PSMS application software, which may be reprogrammed while in the CPU module. In ISG 04, Staff Position 2, Point 7, Nonvolatile memory should be changeable only through a removable memory device. It should not be reprogrammable as with the application software. MHI will address this in the revision of the Software Safety Report, which will be referenced by the MELTAC Topical Report.

8.   MHI will modify the compliance statement in Section 3 for Branch Technical Position (BTP) 7-18 to explain that commercial grade dedication is a non-recurring activity that applies only to the MELTAC past development design. Future MELTAC life cycle activities, including production, and all application level life cycle activities are under Title 10 of the *Code of Federal Regulations* (10 CFR), Part 50, Appendix B Quality Assurance Program (QAP). This change is also applicable to Section 3 of the MELTAC Topical Report and Table 7.1-2 of the DCD.

The related reference, NUREG-6421, is also applicable and should be noted as such in Section 3 of both topical reports.

9.   MHI will, with regards to the Diverse Actuation System (DAS), remove "or digital" from Section 4.1.d. These words conflict with the Defense-in-Depth and Diversity (D3) Topical Report. If this document is only applicable to the US-APWR; they were originally added to allow an alternate DAS design for operating plants.

10.   MHI will submit the performance history of MELTAC self-diagnostics, by the end of March, 2010.

11.   MHI will clarify, in the Safety Topical Report and the MELTAC Topical Report, what standard technical specification surveillances are being eliminated or modified and the basis for these changes (i.e., what is credited to eliminate or modify these tests). MHI will complete the response to Request for Additional Information (RAI) 63.

The NRC (I&C Branch and Technical Specifications Branch) staff needs to reach an agreement on the acceptance of these changes.

12.   MHI will remove credit for the leak detection. This may also need to be removed from other documents.

13.   MHI will add a reference to the Application Software Program Manual (SPM) (MUAP-07017) in Section 6 to provide a sufficient level of detail for the NRC to review.

MHI will explain that Sections 6.1 through 6.4 provides only an overview of the software life cycle process or remove them completely.

14.   MHI will add a reference to the Instrument Setpoint Methodology (MUAP-09022) in Section 6 to provide a sufficient level of detail for the NRC to review.

Explain that Section 6.5.4 provides only an overview of the setpoint methodology or remove the section completely. If the section is retained, ensure it is consistent with the report.

15.   MHI will revise Appendix C to explain why this section credits three distinct operator actions, while the HSI Topical Report (MUAP-07007) describes only two.

16.   The NRC staff still has a concern that a single software error generating an erroneous signal, of a valid data structure and content, can lead to a multiple valid erroneous commands (Reference RAI 54 response). The NRC staff also explained that the issue with regards to the enhanced QAP for the Operational VDUs, which will limit or prevent these erroneous commands, needs to be revisited by MHI in RAI 55. The reference here does not adequately describe the "enhanced" QAP for the Operational VDU. MHI will submit a failure analysis that identifies each type of command that can be initiated from an Operational VDU. For each command explain how the safety of the plant is maintained, if that command were to be initiated spuriously.

17.   MHI will provide a date for submittal of the revised Safety Topical Report and submittal of failure analysis.

US-APWR FUNCTIONAL ASSIGNMENT ANALYSIS FOR SAFETY LOGIC SYSTEM REPORT

The NRC staff discussed the following issues with the report:

-       No reference back to the Safety I&C Topical Report.
-       No reference section included in the report.
-       Timeline of submission.
-       Does not identify or follow any Institute of Electrical and Electronics Engineers (IEEE) standards, or the NRC staff guidance.
-       Revision and resubmission of the report was expected by the NRC staff, addressing each of these items.

The following additional action items are the result of discussion:

1.   MHI will remove "Failure Modes and Effects Analysis (FMEA)" from all sections of this document and replace with "function assignment analysis".

2.   MHI explained to the NRC staff that FMEAs for the Reactor Protections System (RPS) and the ESFAS are in the DCD in Table 7.2-8 and 7.3-7.

3.   MHI will correct Section 6.5.1 of MUAP-07004 to include PSMS in the fifth bullet and add Functional Assignment Analysis for Plant Control and Monitoring System (PCMS) and PSMS to Table 7-1.

4.   The NRC staff does not understand the timeline of submission for this document. RAI 07.03-8 stated that the "FMEA report will be submitted by September 2009." The NRC staff asked if this document is the one identified in the RAI. MHI answered that this document is identified in the RAI, and the name of this document will be changed to Functional Assignment Analysis, not FMEA. The FMEAs for RPS and ESFAS are not included in the DCD, Tables 7.2-8 and 7.3-7, respectively.

5.   MHI will provide a date for submittal of the revised Functional Assignment Analysis Report.

US-APWR RESPONSE TIME OF SAFETY I&C SYSTEM REPORT

The NRC staff pointed out that the calculation formula in the Safety I&C Topical Report does not match the formula in the Response Time Report.

The following action items are the result of discussion:

1.   MHI will clarify in MUAP-07004, that response time figure includes both the I&C and mechanical components (i.e., control rods) and clarify in MUAP-09021, that response time is only the I&C portion.

2.   MHI will provide a date for submittal of the revised Response Time Report.

MELTAC TOPICAL REPORT

Since NRR is no longer reviewing the MELTAC Topical Report, the NRC staff stated that references to operating reactors should be removed. The NRC staff also discussed the following issues:

- Topical Report addressing requirements and of IEEE standards on the identification, and the method of such, of safety related documents and equipment.
- Engineering tool connection and communication.
- Interim Staff Guidance (ISG)-04, Digital Communications, and the NRC staff positions it identifies with regards to the Engineering Tool.
- QAP procedures; the old "Q" vs the new "N" procedures.
- Topical report conformance to BTP 7-14, Software Life Cycle Process
- Critical Characteristics of the MELTAC Commercial Dedication.

The following action items are the result of discussion:

1.   MHI will revise applicability of BTP 7-18 and associated NUREG 6421; see same item above for the Safety I&C Topical Report.

2.   The NRC and MHI will resolve topical report revision/withdrawal issues (e.g., Does the topical report need to be revised to remove the reference to "operator reactors" or can it be treated similarly as the D3 Topical Report?).

3.   MHI will clarify what end user documentation will be marked "Nuclear Safety Related" per IEEE 494. The NRC staff does not consider that this meets the requirements of IEEE Std 603 Criteria 5.11, which states associated documentation shall be distinctly identified in accordance with the requirements of IEEE Std 494. Methods of identification will be identified as an Application Specific Action Item in the MELTAC Safety Evaluation.

4.   MHI will correct Sections 4.1.4.2 and 4.5.2 to state that the Engineering Tool is permanently connected.

5.   MHI will revise section 4.3.4.2 to clarify that there is only unidirectional data, but there are bidirectional message requests.

6.   The NRC staff identified that the changes or differences between the old, Q procedures, and the new, N procedures, are not identified. The NRC staff has reviewed the Q software quality assurance procedures and found significant issues. MHI will clarify that old quality assurance procedures apply to original MELTAC development and the United States Conformance Program (UCP) activities; new quality assurance procedures apply to all life cycle activities after the completion of the MELTAC Re-Evaluation Program (MRP).

7.   MHI will submit the MELTAC SPM for the basic software by the end of April, 2010 to address the guidelines of BTP 7-14, Guidance for Software Reviews.

8.   The NRC staff recommended that MHI will add a section to the introduction to identify the SPM for the basic software and the Software Safety Report (SSR) (JXAU-1015-1009) as "incorporated by reference." MHI took the action to evaluate this request.

9.   The NRC staff presented that a list of characteristics is necessary in the commercial grade dedication (CGD) of MELTAC. MHI stated that the critical characteristics are all of the platform's technical characteristics described in the topical report. Therefore, the MRP provides a table that lists and reassesses all of those characteristics. When the CGD (MRP for MELTAC) is eventually audited, the NRC staff will look for a composite list and this may be an audit finding.

10.   MHI will provide a date for submittal of the revised MELTAC Topical Report.

SOFTWARE SAFETY REPORT

The NRC staff stated that this report provides useful information with regards to the ISG-04 Review, but is not a SSR. The specific issues with the SSR are as follows:

- The report is titled "US-APWR" but the MELTAC submittal is generic.
- No reference section is provided. The SSRs should reference BTP 7-14, Regulatory Guide (RG) 1.173, and IEEE 1228.
- New Structures and buses are mentioned but not described.
- Failure modes not identified.
- Effects not analyzed.
- No definition of hazard identification.
- The SSR does not identify the platform and application level failures.
- The NRC staff expects each of these items to be addressed in the next revision of the SSR.

The following additional action items are the result of discussion:

1.   MHI will add a description of module busses that are not described in MELTAC Topical Report.

2.   MHI will, for compliance to ISG-04, Staff Position 2, Point 7, modify Section 3.4.7 of the MELTAC SSR to explain that PSMS over PCMS prioritization is in memory that can be reprogrammed without removing. MHI will also explain that this is acceptable because:

    a.   The memory is continuously checked to ensure it has not changed,
    b.   The memory is checked periodically during technical specification surveillance using a diverse method, and
    c.   The memory can only be changed by enabling the write permission switch, which requires the controller to be taken out of service.

3.   MHI will submit the Software Safety Plan that is identified in the SSR. All plans including the Software Safety Plan will be included in the SPM for the basic software that will submit by the end of April, 2010.

4.   The NRC will provide to MHI. an example of a typical Software Safety Analysis (SSA) that meets their expectations; the NRC staff believes this is a good document for addressing ISG-04 guidance. However, they do not accept this document as a SSA. MHI explained that a SSA that meets the guidance of BTP 7-14 is only appropriate for the Application Level. MHI believes this is an appropriate analysis for the platform level. MHI's further comments to the meeting included that other platform level software safety activities are within the scope of verification and validation (V&V). This includes review by the V&V Team of each of the principal design documents to ensure identification and traceability of critical platform functions The unique activity addressed in this SSA is identification and analysis of potential hazards that may adversely affect the critical platform functions.

    This analysis assesses the effectiveness of mitigating design features which ensure the hazards are correctly detected and the platform responds as specified.

The NRC staff will review these issues once they are presented on the docket in both the SSR and the SPM as exceptions to the NRC staff guidance.

5.   MHI will provide date for submittal of revised SSR.

SOFTWARE PROGRAM MANUALS AND BRANCH TECHNICAL POSITION 7-14

The following action items are the result of discussion:

1.   The NRC staff expects the SPM to address all "should" guidance within the Acceptance Criteria section of BTP 7-14; this includes all "shall" guidance in the IEEE Standards reference by this Acceptance Criteria. The NRC staff has requested MHI to analyze their documents to the guidance of BTP 7-14, as required by 10 CFR 51.47(a)(9), and in the RAI in the topical reports as well as the DCD. MHI explained that based on the original RAIs plus our response to new RAIs received in January, 2010, MHI believes that all BTP 7-14 "should/shall" guidance is addressed. MHI will verify that all "should/shall" guidance is addressed.

DESIGN CONTROL DOCUMENT REVIEW ISSUES

The NRC staff stated that the issues presented on the reports and how they are resolved will have a major impact on the evaluation of the DCD and the design certification (DC) for Chapter 7. If the base issues in the reports are not resolved, the problem may impact the DCD by additional inspections, test, analysis, and acceptance criteria; Design Acceptance Criteria or an open item in Phase 2 of the DC. The content in the resolved RAI's must be included in the next revision of the DCD. Any current or future RAI's not resolved by the close of phase 2, will become open items.

The NRC staff also requested that MHI address the supplemental criteria for instrument sensing lines provided in RG 1.151 in the endorsement of American National Standards Institute/Instrumentation Systems and Automation (ANSI/ISA) S67.02.

The following action items are the result of discussion:

1.   MHI will add justification for the single tap design for reactor coolant system flow high tap and describe backup protection function (Delta T), effect of breakage (trip) and detectability of plugging (through periodic surveillance). MHI will also include the effect of plugging on dynamic response.

INSTRUMENT SETPOINT METHODOLOGY MUAP-09022

The NRC staff explained that for an increasing setpoint, the Allowable Value (measurable uncertainties) cannot be higher than the Analytical Limit minus the sum of the squares of all unmeasurable uncertainties.

The following action items are the result of discussion:

1.   MHI will revise the definition of Allowable Value; this affects several sections of the document, several figures and several tables.

2.   The NRC (the Technical Specifications Branch and the I&C Branch) will reach an agreement on the acceptability of allowable value surveillance method for digital functions.

3.   MHI will provide a date for the submittal of the revised Setpoint Methodology Report.

CONCLUDING REMARKS

Both the NRC and MHI have action items to complete in order to resolve issues with documents submitted in support of the DCD and the topical report review. The NRC and MHI will establish a routine conference call that will be held to update the list of action items, obtain clarifications from the NRC and discuss submittal options, if necessary. MHI proposes the first routine conference call will be held on the week of February 22, 2010. At the first routine conference call, MHI will define the submittal dates for all reports which are identified in the actions above. For more details, see presentation materials.