



United States Nuclear Regulatory Commission

Protecting People and the Environment

US-APWR

Key I&C Issues and Review Status

Instrumentation, Controls and Electrical Engineering Branch 2
(ICE2)

Division of Engineering
Office of New Reactors

September 30, 2010

The key purpose of this presentation is to provide the staff's:

- Response to the MHI letter on the closure plan for I&C Issues dated August 27, 2010
- Review status of the US-APWR Chapter 7

- Introduction
- Background
- Staff's Chapter 7 review status
- Status of document Submittals
- Staff Response to MHI Closure Plan Letter
- Path Forward/Summary
- Requests for Additional Information (RAIs)
 - Overall RAI Status

- The staff will work closely with MHI to get the issues resolved.
- The staff will be available for clarification of staff RAIs, staff guidance and expected submittals.
- The staff will provide feedback to MHI's responses and submittals in a timely manner.
- The staff will try to be specific relevant to applicable regulations and regulatory guidance when issues are identified.

- The staff expects MHI to provide high-quality, timely responses to staff requests for additional information.
- The staff expects MHI to have a high-quality document configuration control for future changes.
- The staff expects MHI to follow applicable staff guidance and staff's interpretation of the guidance and to understand potential delays in staff review if deviations are made.
- The staff expects MHI to answer the staff's questions and concerns without iteration of RAIs.
 - Interactions with staff to ensure RAIs are well understood and responses meet staff expectations

In the July 27, 2010 public conference call and the August 18 and 19, 2010 public meeting, the staff stated for the following areas the staff cannot produce the safety evaluation report with open items (Phase 2) for several Chapter 7 sections and 14.3.5:

- Data Communications
- Quality Assurance

The staff also identified several examples.

- These issues have been communicated with MHI through audits, meetings and RAIs but the responses have not demonstrated adequate compliance with the applicable regulations.
- The staff emphasized that the examples described are not a complete list as it is the responsibility of the applicant, not of the NRC staff, to perform a comprehensive analysis. It is expected that the closure plan and subsequent details would include the results of the comprehensive analysis.
- The staff's response letter to the closure plan has been issued on September 28, 2010.

Review Status

Section 7.1 I&C Introduction

➤ Existing RAIs: 23

– Closed: 17

– Open: 6 (These open items are related to other technical reports)

➤ Section 7.1 is the place holder to address generic issues discussed in the public meetings. New RAIs may be generated after the staff reviews the MHI's design modification submittal. The staff's review focuses on the following areas:

1. Conformance to Regulations
2. Basic design principles – Independence, Determinism, Redundancy, Diversity & Defense-in-Depth and Simplicity
3. Software development activities
4. Setpoint Methodology
5. Adequacy of ITAAC

Review Status

Section 7.2 Reactor Trip System

➤ Existing RAIs: 2

- Closed: 7.2-01
- Open: 7.2.02 – generic open item

➤ Potential RAIs:

- 13 potential new RAIs are being evaluated for issuance

Review Status Section 7.3 ESFAS

➤ Existing RAIs: 15

- Closed: 5
- Open: 10 – generic open items or items under review

➤ Potential RAIs:

- Several potential new RAIs are being evaluated for issuance

Review Status

Section 7.4 Safe Shutdown System

➤ Existing RAIs: 19

- Closed: 17
- Open: 2
 - Generic open items related to data communications

➤ New RAIs: 3

- Safety I&C System Technical Report (MUAP-07004) - Single Failure
- Periodic Testing of Transfer Switches
- Power Sources – maintenance bypass and reliability

Section 7.5 Systems Important to Safety

➤ Existing RAIs: 18

- Closed: 13
- Open: 3
 - Generic Open Items related to data communications

➤ New RAIs: 2

- PAM variables and DI&C-ISG-04
- Plant Annunciator (Alarm) System environment.

Review Status

Section 7.6 Interlock Systems

➤ Existing RAIs: 16

- Closed: 10
- Open: 6

➤ Recent RAIs: 8

- Recently sent to MHI

Review Status

Section 7.7 Control Systems

➤ Existing RAIs: 27

- Closed: 25
- Open: 2
 - DI&C-ISG 4 – Communication Issues (HICRc) conformance; priority module
 - Single Failure Criterion

➤ New RAIs: 2

- Clarification of inconsistencies on radiation monitor safety classification
- Clarification on number of operator commands

Review Status

Section 7.8 Diverse Systems

➤ Existing RAIs: 5

- Closed: 5
- Open: 0

➤ Staff is reviewing the “Defense-in-Depth and Diversity Coping Analysis” Topical Report (MUAP-07014-P) and the ASAs from the “Defense in Depth and Diversity” Topical Report (MUAP-07006-P-A).

➤ “Defense-in-Depth and Diversity Coping Analysis” Topical Report (MUAP-07014-P) is also being reviewed by other NRC branches including HFE.

Section 7.9 Data Communication

- **Existing RAIs: 18**
 - Closed: 3
 - Open: 15
 - Generic Open Items
 - Independence between safety and nonsafety systems (the use of operational VDUs)
 - Determinism
 - Software quality

- **New RAIs:**
 - Upon the review of the MHI design/submittal changes completed, the staff will determine whether new RAIs are necessary.

Document Submittals Status

- These documents are under staff review with RAIs anticipated. Upon the review of the MHI design/submittal changes completed, the staff will determine whether new RAIs are necessary. The staff plans to issue RAIs for all issues communicated in previous meetings that remain open:
- Safety I&C System Technical Report (MUAP-07004)
 - MELTAC Topical Report (MUAP-07005)

Document Submittals Status

- For these documents RAIs are being created on issues communicated in previous meetings that remain open:
 - Function Assignment Analysis for Safety Logic System Report (MUAP-09020)
 - Software Safety Report (JEXU-1015-1009)

Document Submittals Status

- These documents are under staff review and on track with no major issues at this time:
 - Instrumentation Setpoint Methodology (MUAP-09020)
 - Response Time of Safety I&C System (MUAP-09021)

Document Submittals Status

- Documents below are currently not under staff review as presented at the August 18 and 19, 2010 meeting:
 - Application Software Program Manual (MUAP-07017 Revision 1)
 - MELTAC Platform Documents:
 - Basic Software Program Manual (JEXU-1012-1132)
 - FPGA V&V Final Report (JEXU-1025-3009)
 - Category 2 Additional V&V Final Report (JEXU-1021-6301)
 - Re-evaluation Program Report (JEXU-1022-6301)

Document Submittals Status

- Appendix B QAP Phase 2 Audit Report (PQG-HD-22021)
 - Submitted for information only

MHI Closure Letter Review

- While Staff cannot make any final determination until all design and licensing documents are submitted, the following comments are provided for the three design changes outlined in the MHI Closure Plan Letter:
 - The change to the Maintenance Network, so that the safety controllers are only temporarily connected to the engineering tool, appears to meet the guidance of ISG-04, Staff Position 1, Point 10.
 - The underlying reasons for adding priority logic to all ESFAS safety components, for protection from spurious actuations from the Operational VDU, and adding a hardwired interface to the write enable port of the Flash Read Only Memory (F-ROM) needs to be further understood in detail.

MHI Closure Letter

SDOE Issues - Review

- Within the Closure Plan for US-APWR I&C Open Issues, MHI committed to:
 - Revise the MELTAC commercial grade dedication report to demonstrate that security features of MELTAC, and the security controls applied to the legacy development, are sufficient to be maintained under the security controls defined in the MELTAC Topical Report and SPM.
 - Provide an appendix to the Application Software SPM to document the non-malicious security assessment that encompasses the current lifecycle progression of the PSMS.
- The staff finds that MHI's commitments facilitate the closure of portions of the SDOE review concerns. However, MHI needs to address the following items:
 - Modify Technical Report, "US-APWR Cyber Security Program, (MUAP-08003)" and referenced documents to remove reference to cyber security program and specifically address SDOE as described in RG 1.152.
 - Discussion on how the results of the security assessment will 1) drive the SDOE requirements for the PSMS design and 2) drive development environment and development process controls

MHI Closure Letter

The Regulatory Audit Intent

- By policy a Regulatory Audit is intended to:
 - “Gain understanding and/or to identify information that will require docketing to support the basis of the licensing or regulatory decision” – Office Instruction, NRO-REG-108

- A “thread path” audit is, by definition in BTP 7-14, is a sample of the quality of the software product. It is expected no other errors not already discovered and documented by either the QA organization or the V&V team are found. If one or more errors are found, this indicates a potential weakness in the effectiveness of the QA organization.

- Quality Assurance Program Observation from Arlington audit:
 - “A more thorough review should be performed regarding the UCP with respect to compensating for the inadequacy of the independence of the V&V team.”
- Conclusion of the Arlington Thread Path Audit:
 - “The staff will identify documents translated in this audit, or any additional documents pertaining to the MELTAC platform and the US-APWR application, which may required to be put on the docket, via request for additional information.”

MHI Closure Letter Review Summary

- The closure plan has proposed design changes and the submission of additional information which should address some aspects of the open areas.
- Since the closure plan is written at a high level, the staff will need to see the deliverables committed to in the letter to fully assess the impact on the staff review schedule for the I&C issues.
- The Operational VDU communication with safety systems will continue to be a focus of staff review.
- Software Program Manuals are key for staff's safety findings and have been challenging in other design centers.

- The staff will review the revised design details and documents and will determine staff resources and schedule.
- The staff will continue to review areas that are not covered by the closure plan and work with MHI for resolution for any open issues.
- The staff will use RAIs for all open issues to the extent possible.
- The staff will enforce the Office of New Reactors Phase discipline policy; Phase 2 will be completed only if and when all open items are determined to have a clear success path, and are simple to address, and require no iterations of RAIs.
- The staff will work closely with MHI to resolve all current and future open issues.

Requests for Additional Information - Summary

➤ DCD Review

➤ Total	Closed	Open
143	98	45

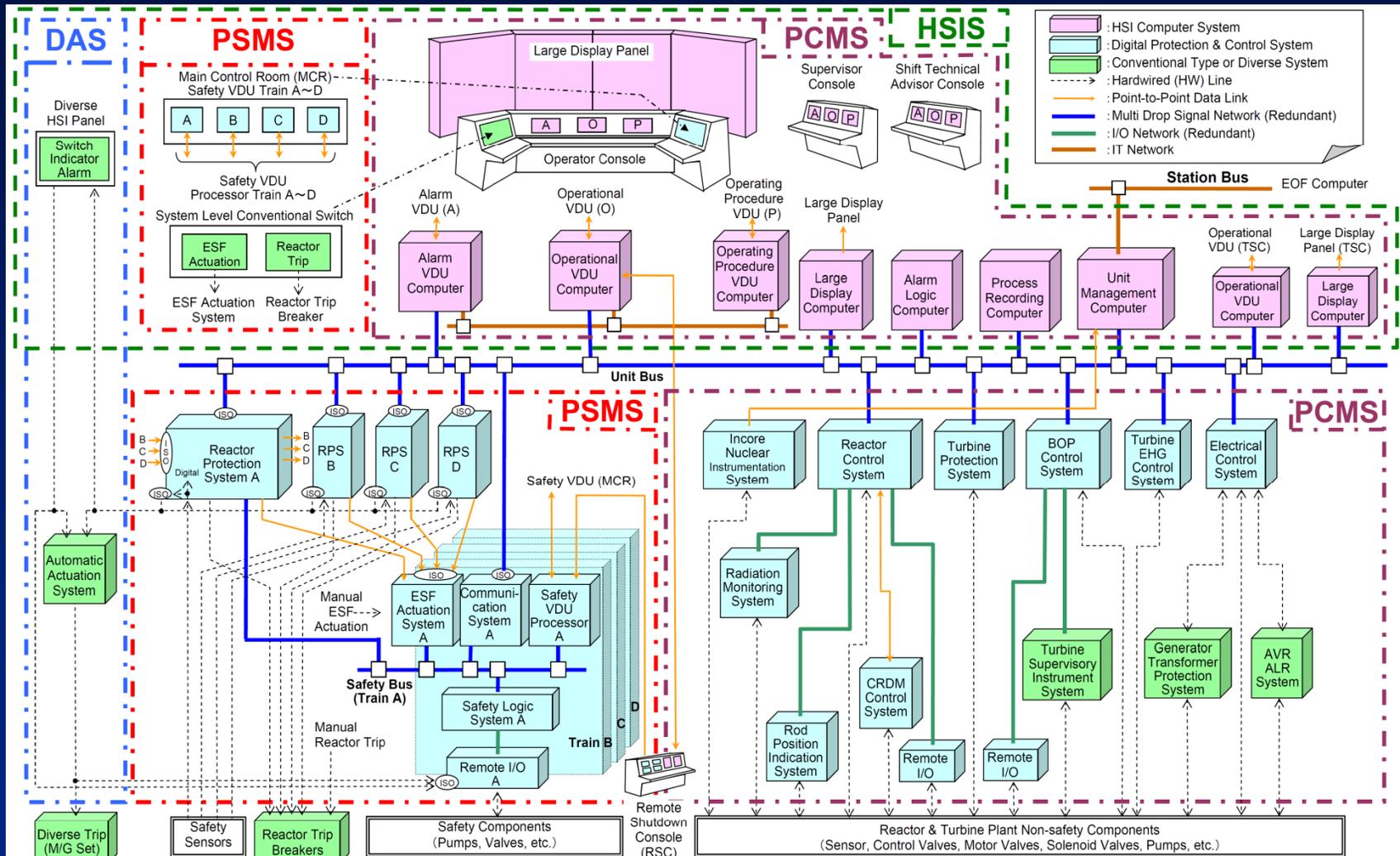
➤ MELTAC Topical Report

➤ Total	Closed	Open
60	24	36

➤ Safety I&C System Design & Process Technical Report

➤ Total	Closed	Open
78	41	37

281	163	118
-----	-----	-----





United States Nuclear Regulatory Commission

Protecting People and the Environment

Acronyms

- CFR Code of Federal Regulations
- BTP Branch Technical Position
- CGD Commercial Grade Dedication
- DCD Design Control Document
- EPRI Electric Power Research Institute
- FPGA Field Programmable Gate Array
- F-ROM Flash Read Only Memory
- GDC General Design Criteria
- HICR Highly Integrated Control Room
- IEEE Institute of Electrical & Electronics Engineers
- ISG Interim Staff Guidance
- ITAAC Inspections, tests, analyses and acceptance criteria
- MELTAC Mitsubishi Electric Total Advanced Controller
- MELCO Mitsubishi Electric Company
- MHI Mitsubishi Heavy Industries, Ltd
- SDOE Secure Development and Operating Environment
- SRP Standard Review Plan
- US-APWR United States Advanced Pressurized Water Reactor
- V&V Verification and Validation
- VDU Video Display Unit