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

December 10, 2010

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Purpose

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

- Feedback on deliverables received in accordance with the MHI closure plan on key I&C issues letter dated August 27, 2010.

- Status of the remaining portions of the US-APWR Chapter 7 Review, (time permitting).

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Agenda

- Background
- Staff Feedback on Key I&C Issues
  - Software Program Manuals
  - Communications Independence
  - Commercial Grade Dedication
- Topics to Support Schedule Improvement
- Staff's Chapter 7 Review Status (time permitting)

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Background

- In public meeting on August 18-19, 2010, the staff stated for the following areas that 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 in each area.

- MHI provided a Closure Plan for these issues by letter dated August 27, 2010

Background

- By letter dated August 18, 2010, MHI submitted three reports related to the MELTAC Reevaluation Program in partial response to the Quality Assurance Key Issue.
- By letter dated September 30, 2010, MHI submitted revisions to the Software Program Manuals as a response to the Quality Assurance Key Issue.
- By letters dated October 13, 2010 MHI submitted various technical report revisions as deliverables to the closure plan.
- By letter dated November 16, 2010, MHI provided an update to the Tier 1 and Chapter 7 of the US-APWR Design Control Document.
- The staff's response letter to the closure plan was issued on September 28, 2010.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Software Program Manuals Regulatory Basis

- 10 CFR 50, Appendix A, General Design Criterion (GDC) 1, "Quality Standards and Records," requires in part that systems and components important to safety be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions.
- GDC 21, "Protection System Reliability and Testability," requires the design to have high functional reliability.
- In Appendix B, to 10 CFR 50, many of the criteria are applicable to life cycle activities as proficiently explained in the six associated regulatory guides and Branch Technical Position (BTP) 7-14 of the Standard Review Plan (NUREG-0800).

Software Program Manuals Safety Significance

- Research and experience have found software cannot be typically proven as error-free.
- Software design & specification errors are the primary credible sources of faults in software dependent safety systems.
- The high quality software design process can reduce these errors and is critical for the defenses where complexity does not allow 100% testing.
- A formal development process, described by the SPMs, is critical to the creation of high quality safety system software.

Software Program Manuals Purpose

- SPMs describe, for the applicant and staff, how the 12 software plans in BTP 7-14, Guidance on Software Reviews, will be written.
- The software plans are based on the IEEE Computer Society Standards where critical functions depend on high integrity software.
  - 7 Regulatory Guides endorse 9 of these standards
    - BTP 7-14 provides guidance taken from these and other standards, NUREGs etc

Software Program Manuals Revision Status

- Basic Software SPM submitted twice.
  - Not progressed beyond the staff's initial assesments.
- Application SPM submitted three times;
  - 41 RAIs and issues raised at three public meetings between revisions over 2+ years – with little progress.
- The significant additions to latest submittals were the BTP 7-14 Compliance Matrix appendices which interpreted, for the staff, how each section of SPMs meets BTP 7-14.
- The NRC has completed an assessment of the extent to which recent submittals addressed the identified concerns. Based on this review, the NRC staff has found the revised SPMs unresponsive to the cited information needs.

Software Program Manuals Completeness

- Examples of SPM Issues with regards to lack of detail, completeness and specificity:
  - Each activity shall be assigned a single "owner" (RG 1.173/ IEEE Std 1074)
    - Basic SPM: "Revise the Project Plan when it is changed. At the time of revising the Project Plan, it should be reviewed and approved as well as its first edition."
    - Basic SPM: "Support software (compiler, test tool, etc) and associated documentation are managed by a list."

Software Program Manuals Organizational Issues

- Examples of Issues with regards to Implementing Organizations:
  - Per BTP 7-14, "One of the most critical items is the independence of the V&V organization. ... Should not be subject to ... pressure from designers or project managers. Second in importance is number and quality of V&V personnel"
    - Application SPM: The V&V group reports to the Project Manager
    - Basic SPM: The V&V budget is acquired from the design group
    - Basic SPM: Number of V&V man-hours is equivalent to Design man-hours. (This is not an equivalence to the number of personnel and the quality of their skills)

Software Program Manuals
Organizational Issues

- Issues with regards to Implementing Organizations (cont.):
  - Per BTP 7-14, a Configuration Control Board (CCB) should exist with the authority to authorize all changes to baselines.
    - The Application SPM identifies a possible "equivalent" group but does not address how each role or function of the CCB, according to staff guidance, is equally performed.
    - The Basic SPM does not identify any type of similar function.
  - Project management planning shall detail the project organization (RG 1.173/ IEEE 1074):
    - Basic SPM does not identify a project organization or a Project Manager.

Software Program Manuals
SPM Terminology Issues

- Examples Issues with regards to SPM Terminology:

– Two sources for terminology are not used by the SPMs: 1) IEEE 610.12-1990, Standard Glossary of Software Engineering Terminology as accepted by the Regulatory Guides; 2) Also the terms used in the standard review guidance such as BTP 7-14.

– Examples of different or missing definitions which create uncertainty that the processes are consistent with staff guidance:

  - Requirements Traceability Matrix, Configuration Control Boards, Software Requirements Specification, Configuration items, Baselines, Interfaces, System Testing etc.

Software Program Manuals Implementing Process Issues

- Examples of Issues with incomplete or missing Implementing Processes:

  - All types of Quality Assurance (QA) audits per IEEE 1028-1997 as endorsed by RG 1.168 – all not identified in the SPMs.
  - All topics to be addressed for each V&V activity per IEEE 1012-1998 as endorsed by RG 1.168 – not addressed in the SPMs.
  - The types of software safety analyses, identified by BTP 7-14, to be completed for each phase of the software life cycle – not addresed in the SPMs.
  - The methodology used for the identification of software metrics per IEEE 1061-1998 – not addressed in the SPMs.

Software Program Manuals Implementing Process Issues

- Examples of Implementing Processes Not included:
  - The MHI "augmented" quality program for systems important to safety. (Ex: O-VDU, Alarms, SPDS, SSA etc.)
  - Identification of the actual lower level software plans, procedures, manuals, etc. that will be used to implement the planning and later phase activities.
  - Addressing hardware attributes throughout various planning activities.
  - Checklists are not included as attachments to the SPM. Merely stating the checklist meets the regulatory guide is not sufficient evidence of conformance.

Software Program Manuals Identification of Regulations

- Examples of Issues with Regulations, Requirements and Standards Identification:

  - The SPMs do not identify the regulations, requirements and standards that form the basis for the plant safety analysis in the development plan or in the software requirements specifications. This example is a critical feature to be included in the planning phase.

  - Requirements shall be specified as completely and thoroughly as is known at the time, even if evolutionary revisions can be foreseen as inevitable. The fact that they are incomplete should be noted. A formal change process per IEEE 830 -1993 as endorsed by RG 1.172 should be developed.

Software Program Manuals
Software Tools

- Examples of issues with regards to Software Tools:

– The SPMs do not list all software tools and activities associated with them. BTP 7-14 discusses the methods, techniques and tools to implement each plan should be described. Examples include:

  - Tools used for Field Programmable Gate Arrays (FPGAs)
  - MELENS and the RAPID CAD Software packages
  - For these and the other tools identified, the SPMs fail to adequately address: 1) the tool qualification processes and when it is done; 2) configuration controls used and when they are done; 3) who has the responsibilities to do this and; 4) what are the implementing procedures.

Data Communication Independence Introduction

- The staff has completed the assessment of the latest MHI submittal of DI&C architecture and data communication scheme.
- The staff recognizes the efforts by MHI in trying to resolve the DI&C issues.
- MHI has made a progress in addressing the staff concerns with regard to data communication independence including the engineering tool.
- However, there are key aspects for which the NRC will needs significant additional information to complete its evalutation to reach a safety finding.

Data Communication Independence Staff Findings

- Maintaining the use of non-safety Operational Visual Display Units (O-VDUs) to perform safety functions does not improve the certainty of the DCD review.
- Utilizing the bi-directional communication between non-safety components and safety systems unnecessarily adds significant complexity; and therefore requires significant additional information and staff's review time and resources

Data Communication Independence Staff Findings

- As more information is required to support the staff's safety finding, the amount of licensing basis document may significantly increase.
- A new set of ITAAC may also be required to confirm the as-built design.

Data Communication Independence Regulatory Basis

- GDC 24 states, in part, that interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.
- 10 CFR 50.55a(h), IEEE 603-1991, Clause 5.6, requires safety systems design be such as credible failures in and consequential actions by other systems shall not prevent the safety systems from meeting the requirements of the standard.

Data Communication Independence
Staff Regulatory Guidance

- ISG-04 provides guidance for interconnections while maintaining IEEE 603-1991 requirements.
  - MHI has claimed that by following ISG-04 guidance, the US-APWR interdivisional communication meets the regulations.

Data Communication Independence
Staff Regulatory Guidance

- The staff's review therefore focuses on ISG-04 to confirm MHI's claim.
- The staff finds that the submittal has not adequately demonstrated that the US-APWR interdivisional communication fully meets ISG-04, and therefore will need significant, additional information to confirm the ISG-04 conformance.

Data Communication Independence
Staff Regulatory Guidance

- ISG-04, Staff Position 1.2 states, in part, that the protection, which protects the safety function of a safety division from influence from outside that division, is sustained despite any operation, malfunction, design error, communication error, software error, or corruption originating outside the division.
- The submittal has not demonstrated that the safety function of a safety division can be sustained despite such potential influence.

Data Communication Independence
Staff Regulatory Guidance

- ISG-04, Staff Position 1.3 states, in part, that the added system/software complexity associated with the performance of functions (1) not directly related to safety function and (2) does not increase the likelihood of the software errors that would affect more than one division.

- Based on the submitted documentation, the staff has not able to reach safety findings with regard to the performance of the safety function by the complex O-VDUs, Unit Bus and associated equipment.

Data Communication Independence
Areas of Additional Information

- As such, to determine whether the US-APWR interdivisional communication conforms to ISG-04, the staff needs additional information including the following:
  - Additional detail of data exchanged between safety divisions and nonsafety components to gain a better understanding of the complexity of the bi-directional communication.
  - Additional information on potential failure modes of interfaces between safety divisions and non-safety components to ensure no design errors and malfunction of the non-safety components impair the safety functions.

Data Communication Independence
Areas of Additional Information

- The quality assurance and configuration controls of the Op-VDUs, Unit Bus, and associated components to ensure they are reliable to sufficiently perform safety functions.
- Additional functional analysis of the O-VDUs and Unit Bus that concludes any malfunction, design error, communication error, software error, or corruption originating from the O-VDUs would not influence the safety function of a safety division
- Additional information on testing and surveillance for Op-VDUs, Unit Bus, and associated equipment to ensure these non-safety components would not impair safety functions.

Data Communication Independence Summary

- MHI has made progress in trying to resolve the data communication independence issues.
- The staff found that utilizing the bi-directional communication between non-safety components and safety systems unnecessarily adds significant complexity, which requires a significant amount of additional information from MHI and the staff's review time and resources.

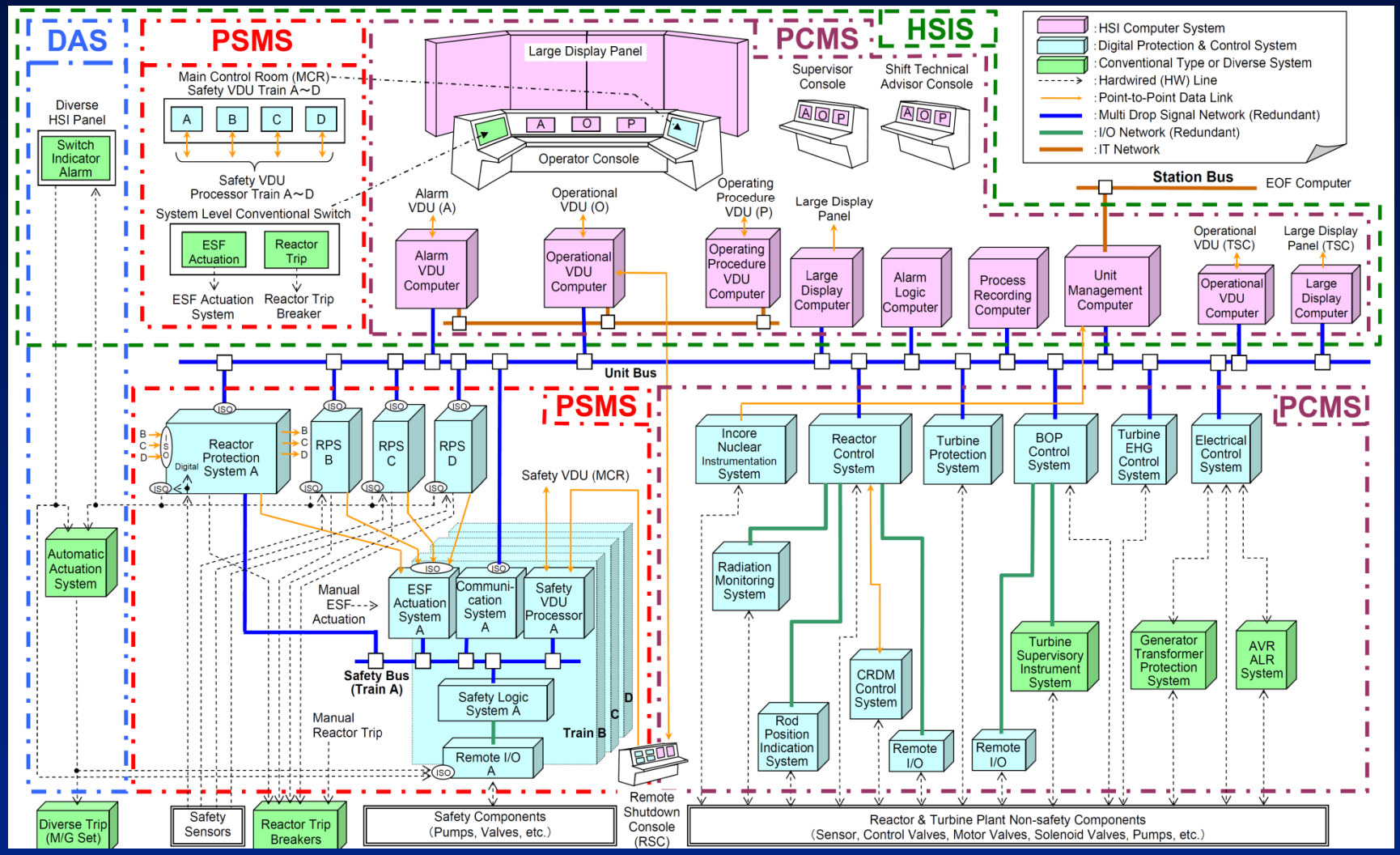
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Topics to Support Schedule Improvement

- SPMs (45+ RAIs)
  - High Quality Submittal of SPM or Plans – essential
- Commercial Grade Dedication (CGD) Plan for "Existing Platform" of MELTAC (6+ RAIs)
  - Software - Process & procedures
  - Hardware - The differences of each
  - US conformance program vs "Existing" platform assessment
- Data Communications (20+ RAIs)
  - Simplify
  - O-VDU & Unit Bus
- Scope of Manual Surveillances (12+ RAIs)
  - Begin with Standard Technical Specification Surveillances
  - Update based on US-APWR Self Testing Operational History – License Action Request (LAR)?

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

US-APWR
Overall I&C Architecture



Acronyms

- CFR — Code of Federal Regulations
- BTP — Branch Technical Position
- CAD — Computer Aided Design
- CGD — Commercial Grade Dedication
- DCD — Design Control Document
- DI&C — Digital Instrumentation and Control
- 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

Acronyms

- MELCO — Mitsubishi Electric Company
- MHI — Mitsubishi Heavy Industries, Ltd
- O-VDU — Operational VDU (Non-Safety)
- SSA — Signal Selection Algorithm
- SPDS — Safety Parameter Display System
- SDOE — Secure Development and Operating Environment
- SRP — Standard Review Plan
- S-VDU — Safety VDU (Safety-Related)
- US-APWR — United States Advanced Pressurized Water Reactor
- V&V — Verification and Validation
- VDU — Video Display Unit