United States Nuclear Regulatory Commission

Protecting People and the Environment

US-APWR
Key I&C Issues

Royce D. Beacom
Instrumentation, Controls and Electrical Engineering Branch 1
Division of Engineering
Office of New Reactors

August 18, 2010

Purpose

The purpose of this presentation is to review the staff's findings, regulatory requirements, examples and summary, with the path forward, of each of the US-APWR I&C key issue areas:

- Data Communications
- Quality Assurance

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

Agenda

- Background
- Data Communications
- Quality Assurance
- Path Forward
- Figure: US-APWR Overall I&C Architecture
- Acronyms

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

Background

- With the exception of the MELTAC Reevaluation Program, these issues have been communicated with the applicant through audits, meetings and RAIs but the responses have not addressed the issues. The February 3, 2010 public meeting presented a comprehensive discussion of these and some of the other issues affecting the US-APWR Chapter 7 Design Certification.
- 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.

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

Data Communications Finding

- Aspects of the US-APWR system design do not comply with NRC requirements on separation between safety and nonsafety systems based on the submitted information to date.
- MHI must demonstrate compliance with the regulations such that the separation design principle is clearly met in order for the staff to reach a reasonable assurance of safety finding.

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

Data Communications Regulatory Basis

- IEEE Std. 603-1991, as incorporated by reference in 10 CFR 50.55a(h), addresses credible failures in and consequential actions by other systems shall not prevent the safety system from meeting other safety criteria.
- 10 CFR Part 50, GDC 24, requires separation between protection and control systems, by limiting interconnections to assure safety is not significantly impaired.

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

Data Communications Examples

- The staff determined that MHI deviated from the current staff guidance in Interim Staff Guidance (ISG)-04 and has not provided sufficient basis and justifications for the deviations to demonstrate compliance with the regulations:
  - Position 1, Point 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. Functions that are not necessary for safety, even if they enhance the reliability, should be executed outside the safety system.*
  - Position 1, Point 10: *On-line changes to safety system software should be prevented by hardwired interlocks or by physical disconnection of maintenance and monitoring equipment.*
  - Postion 1, Point 12: *Communication faults should not adversely affect the performance of required safety functions in any way.*
  - Postion 2, Point 7: *Design provisions should ensure that static memory and programmable logic (i.e. priority logic) cannot be altered while that memory device is installed in the system. Logic should be changeable only when the memory device is physically removed from the system.*

Data Communications Examples

- The staff determined that MHI deviated from the current staff guidance in ISG-4 on command prioritization and has not provided sufficient basis and justifications for the deviations to demonstrate compliance with the regulations.
  - Position 2 Point 3: *Safety-related commands, that direct a component to a safe state, have highest priority and override all other commands.*
  - MHI design that the Safety Video Display Unit (VDU) “can have” priority or the Operational VDU has “equal priority” has been found unacceptable.

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

Data Communications Examples

- MHI's evaluation on conformance to ISG-04 was limited to the basic MELTAC platform and has not addressed application-level (i.e., US-APWR) details.
  - Staff guidance is addressed at the application level.

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

Data Communications Summary

- Aspects of the US-APWR system design do not comply with NRC requirements as MHI deviated from the current staff guidance and has not provided sufficient basis and justifications for the deviations to demonstrate compliance with the regulations.
- Complexity issue is a major concern.
  - A simpler data communication design is expected to be needed to demonstrate sufficient independence between safety and nonsafety systems both to ensure compliance with the regulatory requirements and to establish a more predictable staff review schedule.

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

Quality Assurance Finding

- Aspects of the US-APWR design certification application do not demonstrate compliance with NRC regulatory requirements on quality assurance and quality standards.
- MHI must demonstrate that the I&C design is developed in compliance with the regulations by completing required quality assurance activities. MHI must also provide sufficient information on MELCO compliance with quality assurance and standards.

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

Quality Assurance Regulatory Basis

- 10 CFR 50.55a(a)(1) requires, in part, that systems and components be designed, tested, and inspected to quality standards commensurate with the safety function to be performed.
- 10 CFR Part 50, Appendix B, provides quality assurance requirements for design, construction and operation of safety-related components.
- 10 CFR Part 21 provides, in part, an acceptance process undertaken to provide reasonable assurance that a commercial grade item to be used as a basic component will perform its intended safety function.
- 10 CFR Part 50, Appendix A, GDC 21, provides, in part, that protection systems be designed for high functional reliability.

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

Quality Assurance Examples

- MELCO, in original submittals of the US-APWR Design Certification, was “affirmed” & “in accordance” with 10 CFR Part 50 Appendix B.
- Multiple MHI Audits of MELCO found Findings and Concerns associated with 10 CFR Part 50 Appendix B and 10 CFR Part 21 (such as Software Quality Assurance, Tests & Inspections, and Document Control).
- The reconciliation between the MELTAC Quality Assurance process and the requirements of 10 CFR Part 50 Appendix B and 10 CFR Part 21 has not been demonstrated.

Quality Assurance Examples

- MHI/MELCO has recently submitted the MELTAC Reevaluation Program documents. With regards to their scope and purpose, the staff finds that:
  - MHI has not addressed all required attributes of a 10 CFR Part 21 commercial grade dedication (CGD) process; therefore, the staff finds that MHI has not met the regulatory requirement.
  - For staff guidance on CGD, MHI has addressed only small subsections of relevant staff guidance (e.g., EPRI 107330 & 106439 which have been endorsed by the staff); therefore, the staff finds that MHI has not addressed conformance to applicable guidance or provided acceptable alternatives.

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

Quality Assurance Example

- NRC March 2009 audit found:
  - FPGAs are used in the safety systems.
  - Other technical & quality issues were identified.

And, these issues have not been fully addressed.

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

Quality Assurance Summary

- Aspects of the US-APWR design certification application do not demonstrate compliance with NRC regulatory requirements on quality assurance and quality standards as:
  - MHI has not fully addressed conformance to the applicable staff guidance and has not provided sufficient basis and justifications for the deviations to demonstrate compliance with the regulations.
  - Audits of MHI and the staff identified significant deficiencies with respect to conformance to 10 CFR Part 50 Appendix B and 10 CFR Part 21.

Software Quality Assurance Background

- Standard Review Plan (SRP) Branch Technical Position (BTP) 7-14 and Regulatory Guides describe staff acceptable methods for meeting applicable regulations including 10 CFR Part 50 Appendix B for plans of highly reliable software processes.
- US-APWR acceptance review and schedule is based on DCD Chapter 1 stated "Conformance - with no exceptions noted" for BTP 7-14
- The Software Program Manuals (SPMs) for basic and application software were submitted in May 2010. An SPM is an essential document for the staff to make a reasonable assurance of safety finding with respect to software quality.

Software Program Manuals Finding/Examples

- Both SPMs are not adequate with regards to level of detail, completeness, and conformance to staff guidance:
  - MHI's SPMs contain information on specific software plans that is inconsistent, overlapping, and conflicting with other licensing documents such as Design Control Document and supporting technical reports.
  - The applicable criteria (e.g., the "should" and "shall" in the staff guidance) have not been fully addressed or acceptable alternatives for deviations have not been fully presented in compliance with 10 CFR 52.47(a)(9).
  - The processes described do not include definitions of the activities defined by endorsed IEEE software terminology.

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

Software Program Manuals Examples

- The verification and validation (V&V) efforts are not in conformance with staff guidance, and MHI has not provided acceptable alternatives for the deviation.
- Potential security vulnerabilities in each phase of the lifecycle process in accordance with Regulatory Guide 1.152 have not been assessed, and MHI has not provided acceptable alternatives for the deviation.
- Identification and use of software tools are not adequately addressed in each software plan (e.g., FPGA development tools).

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

Path Forward

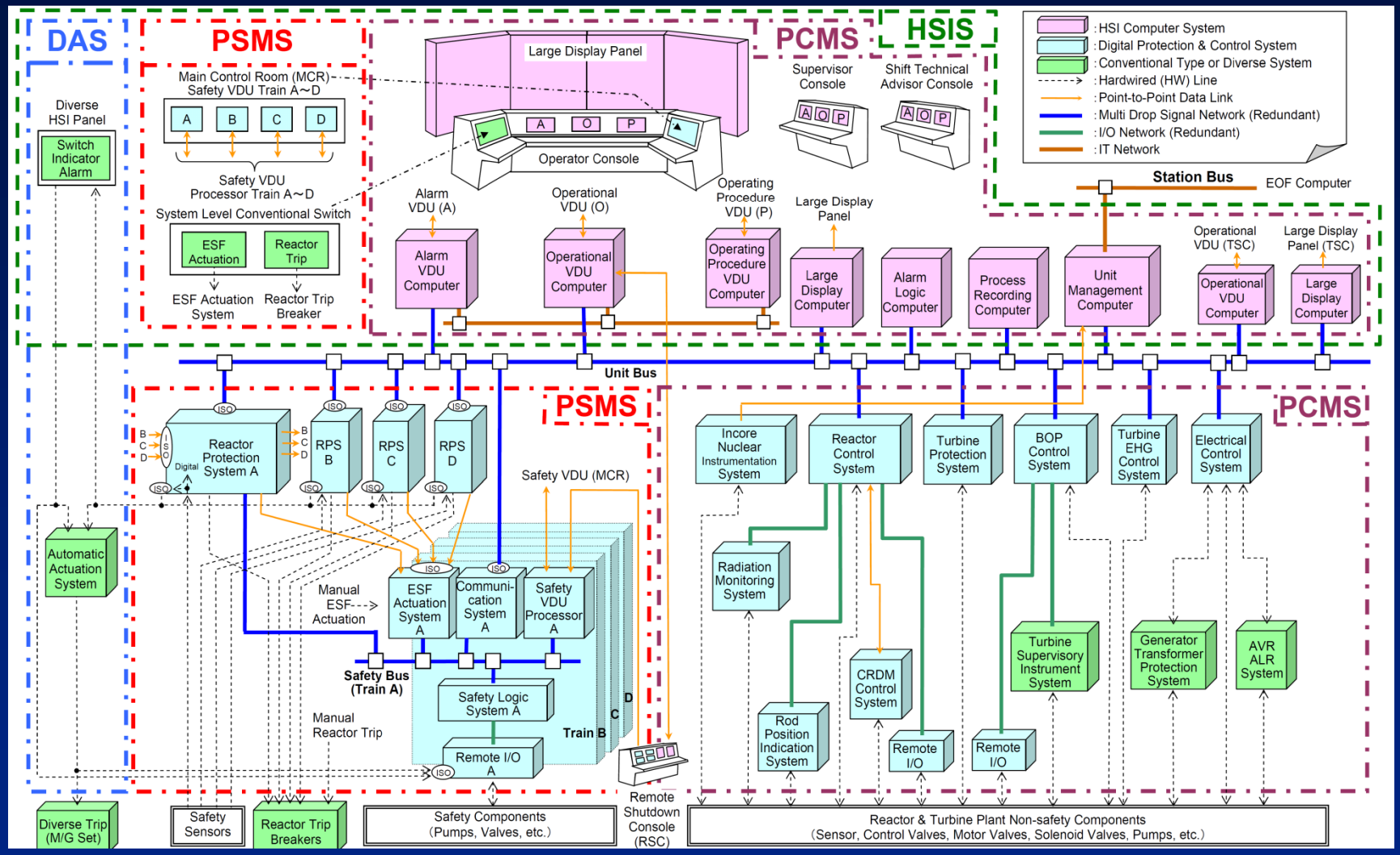
- To ensure that the design presented for this application can be demonstrated to meet communications independence requirements, a simpler data communication design is expected to be needed to demonstrate sufficient independence between safety and nonsafety systems both to ensure compliance with the regulatory requirements and to establish a more predictable staff review schedule.
- MHI must demonstrate that the I&C design is developed in compliance with the regulations by completing required quality assurance activities. MHI must also provide sufficient information on MELCO compliance with quality assurance and standards.

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

Path Forward

- A complete CGD process of the MELTAC system must be implemented in accordance with the requirements of 10 CFR Part 21. This CGD program should fully address applicable staff guidance and endorsed industry documents.
- Revised SPMs should be submitted to the NRC for both the application and basic software. The applicant should ensure all applicable criteria in staff guidance (BTP 7-14 and Regulatory Guides) on software plans are addressed. Acceptable alternatives with sufficient justification should be provided where the submittal differs from guidance for the staff to make a reasonable assurance finding.

US-APWR
Overall I&C Architecture



U.S.NRC
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
- GDC General Design Criteria
- IEEE Institute of Electrical & Electronics Engineers
- ISG Interim Staff Guidance
- MELTAC Mitsubishi Electric Total Advanced Controller
- MELCO Mitsubishi Electric Company

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

Acronyms

- MHI Mitsubishi Heavy Industries, Ltd
- SRP Standard Review Plan
- US-APWR United States Advanced Pressurized Water Reactor
- V&V Verification and Validation
- VDU Video Display Unit