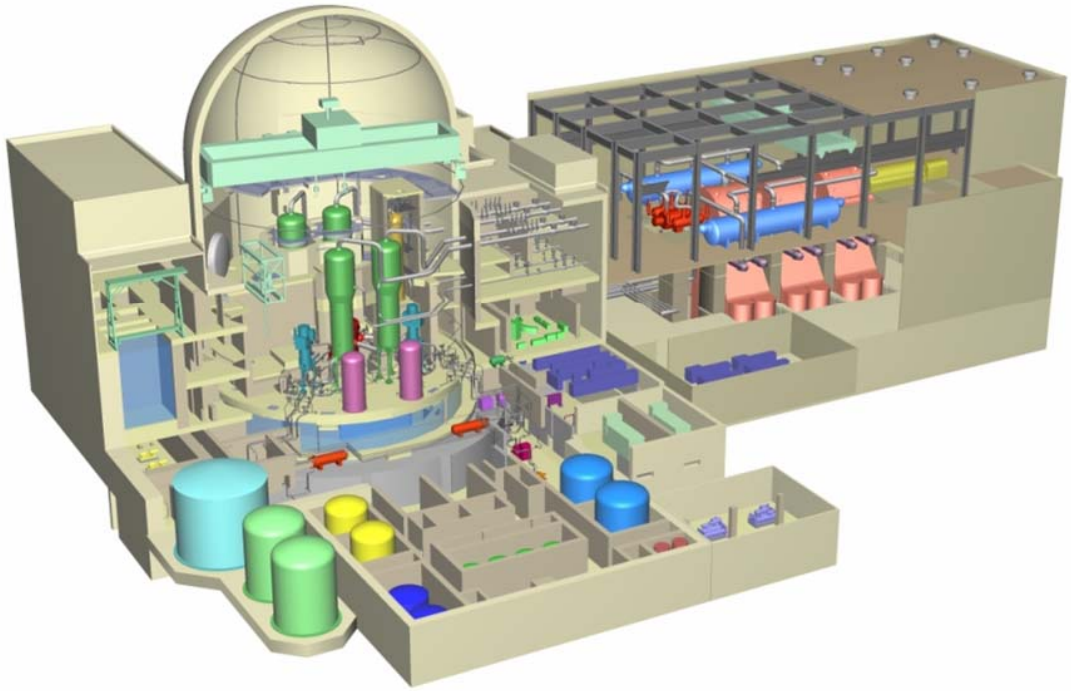
MITSUBISHI NUCLEAR ENERGY SYSTEMS, INC.

MITSUBISHI HEAVY INDUSTRIES, LTD.

US-APWR

MITSUBISHI

US-APWR



Digital I&C Key Licensing Issues

August 18, 2010

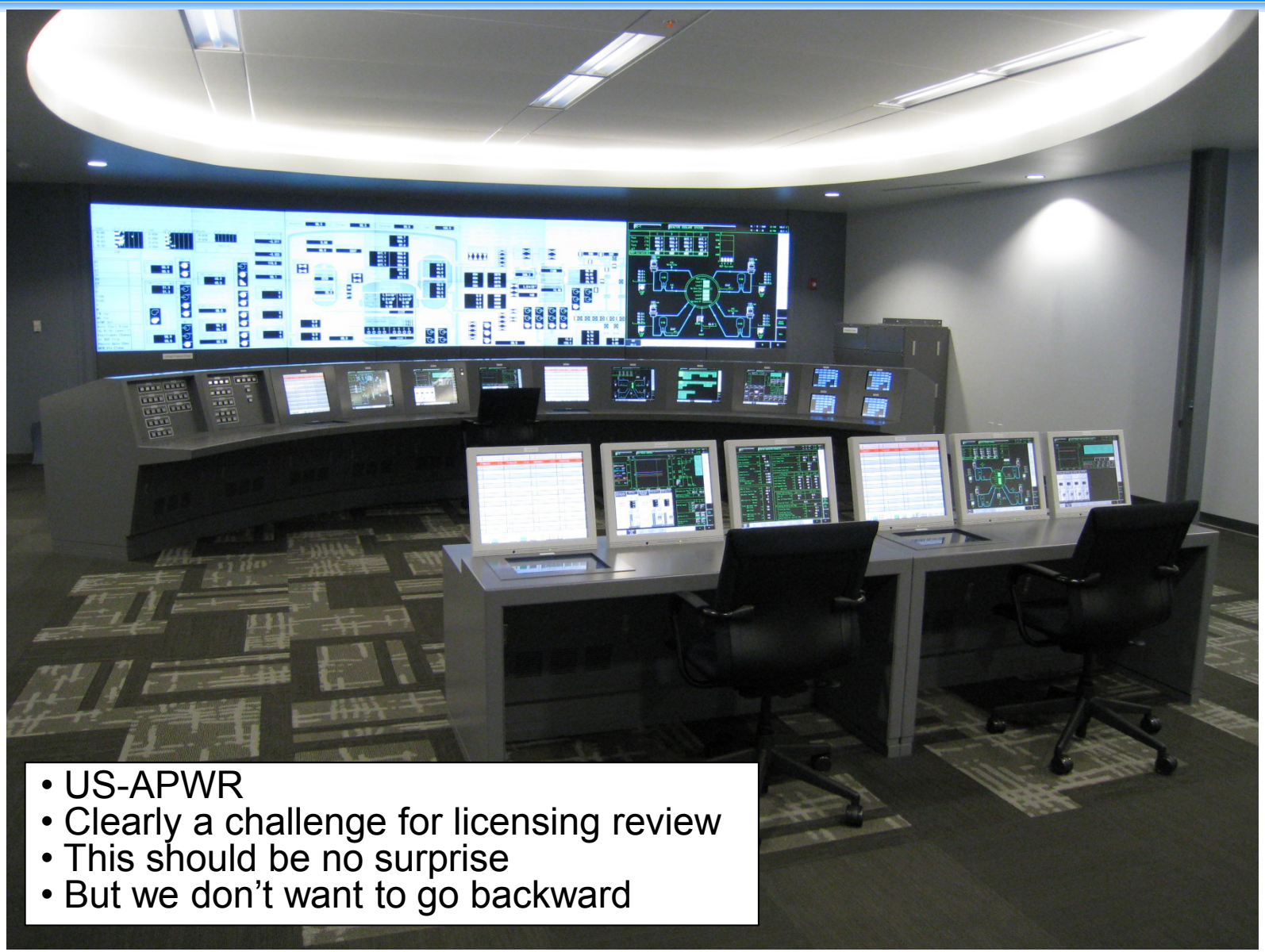
Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Nuclear Industry Analog Reference

- Most US operating plants today

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Analog to Digital Transition



- US-APWR
- Clearly a challenge for licensing review
- This should be no surprise
- But we don’t want to go backward

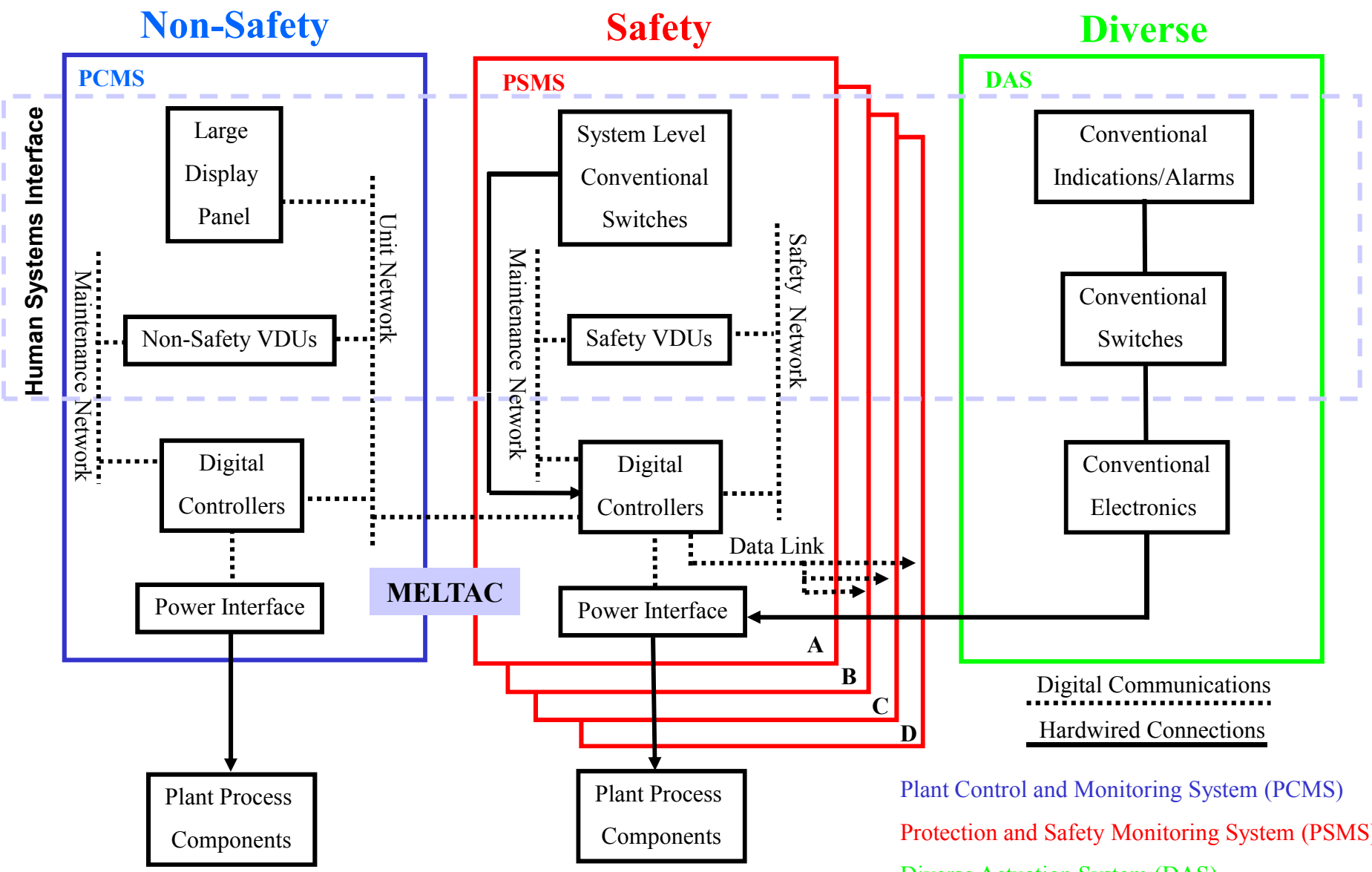
Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Topics

- **Part 1**
  - ✓**Digital I&C overview**
  - ✓**Key licensing open issues overview**
- **Part 2**
  - ✓Details of each issue
    - Inter-division Communication
    - MELTAC Quality Assurance
    - Software Life Cycle Process

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Digital I&C System



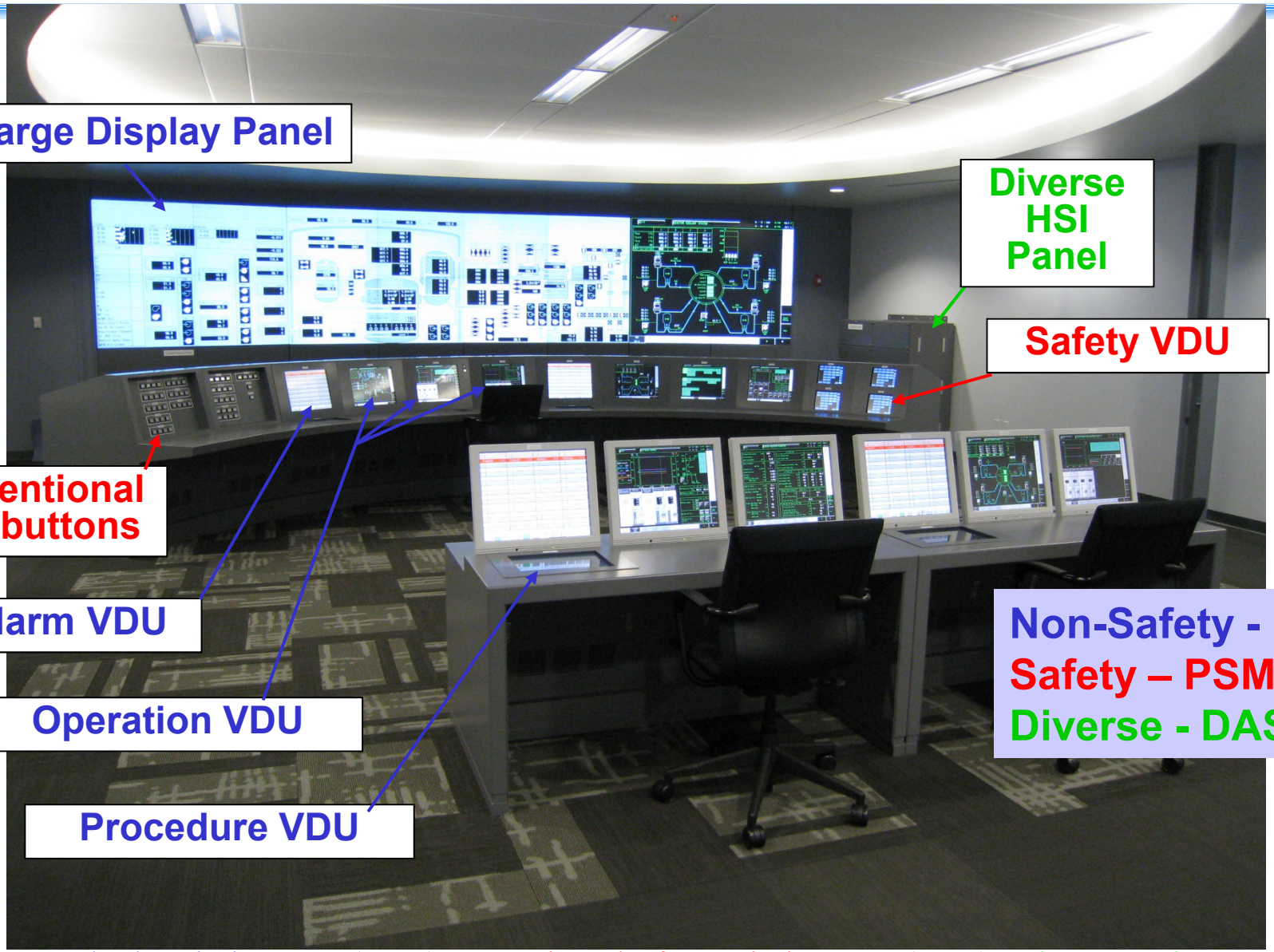
Plant Control and Monitoring System (PCMS)

Protection and Safety Monitoring System (PSMS)

Diverse Actuation System (DAS)

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Digital HSI System

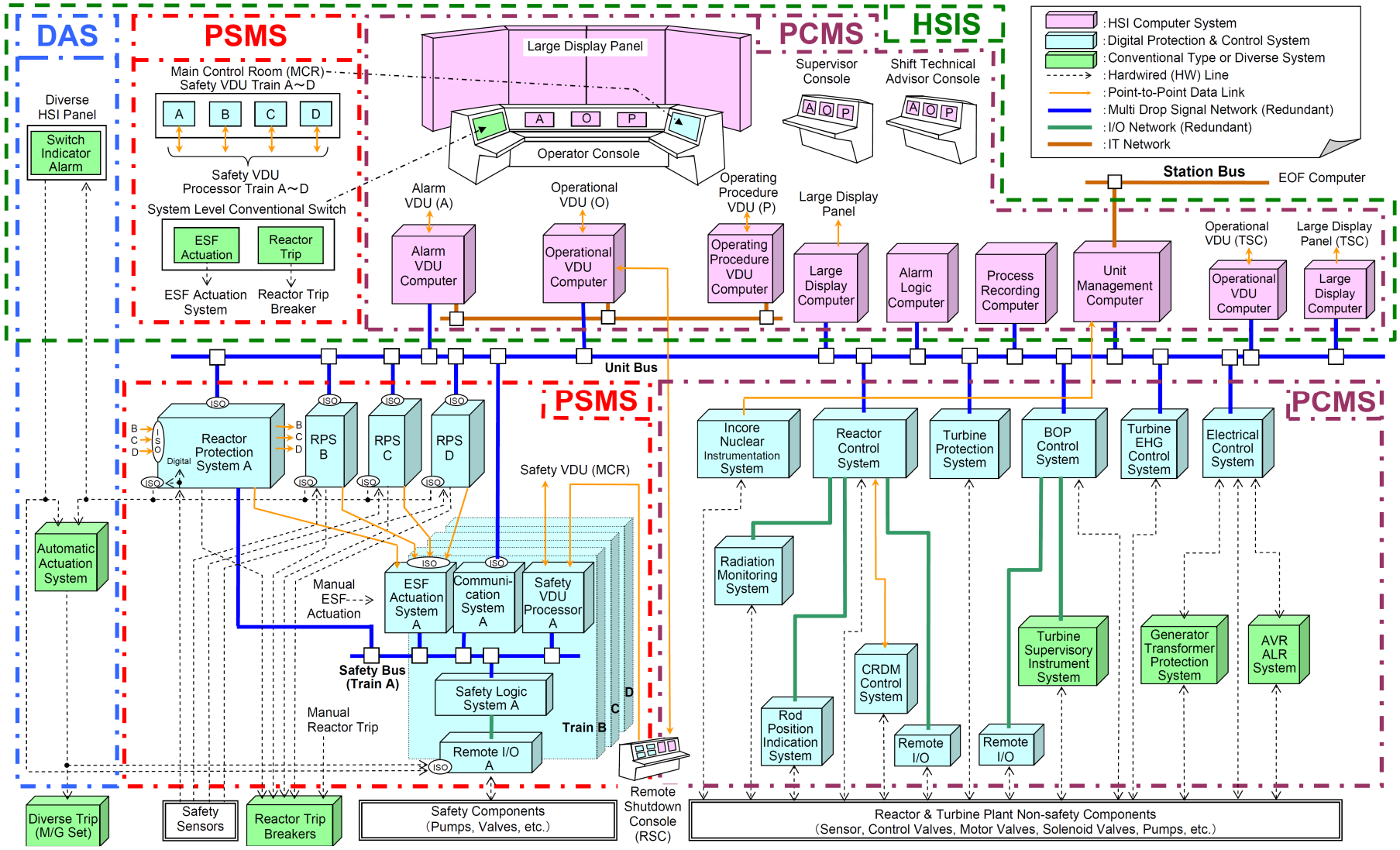


Non-Safety - PCMS
Safety – PSMS
Diverse - DAS

Plant Control and Monitoring System (PCMS) Protection and Safety Monitoring System (PSMS) Diverse Actuation System (DAS)

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Digital I&C System



DAS : Diverse Actuation System PSMS : Protection and Safety Monitoring System HSIS : Human System Interface System PCMS : Plant Control and Monitoring System

MITSUBISHI HEAVY INDUSTRIES, LTD.
Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

History of Mitsubishi Digital I&C

- First Japanese installation for non-safety 1991
- Applied to all non-safety I&C at 5 operating plants in Japan
- 2009 applied to total I&C/HSI at 3 operating plants
- Over 20 million hours total operating experience
  - ✓ ***No system malfunction caused by S/W or H/W failure***
- The same basic architecture and key design features are applied to the US-APWR
  - ✓ MELTAC Controllers
  - ✓ Control Network communications
    - inter-division and intra-division
  - ✓ Maintenance Network communications
  - ✓ Multi-division Operational VDUs
  - ✓ Diverse Actuation System

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

US Licensing

- **Four topical reports submitted to NRC April 2007**
  - Safety I&C System Description and Design Process
  - Safety System Digital Platform - MELTAC
  - HSI System Description and HFE Process
  - Defense-in-Depth and Diversity (D3)
    - SER for D3 issued 6/2009
- **Numerous other I&C technical reports have been submitted for NRC review**
  - ✓ Software program manuals, response time analysis, setpoint methodology, software safety analysis, commercial grade dedication report, QA audit reports, V&V reports, function assignment analysis
- **Numerous other I&C design documents have been audited by the NRC**

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Key Licensing Open Issues

- **NRC has stated MHI has not submitted a sufficient "level of detail" or the "right information" to demonstrate compliance to NRC regulations in three key areas**
  - Inter-division Digital Communication
  - MELTAC QA
  - Software Life Cycle Process
- ✓ ***As a result NRC has stated at the July 27 public meeting they consider the review of these areas complete and therefore cannot generate an SER***
  - ***MHI understands this to mean the review has been suspended for these areas***

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Inter-Division Digital Communication

Non-Safety

Safety

Diverse

PCMS

PSMS

DAS

Human Systems Interface

Large Display Panel

Unit Network

Maintenance Network

Non-Safety VDUs

Digital Controllers

Power Interface

Plant Process Components

MELTAC

System Level Conventional Switches

Maintenance Network

Safety Network

Safety VDUs

Digital Controllers

Data Link

Power Interface

Plant Process Components

A

B

C

D

Conventional Indications/Alarms

Conventional Switches

Conventional Electronics

Digital Communications

Hardwired Connections

Plant Control and Monitoring System (PCMS)

Protection and Safety Monitoring System (PSMS)

Diverse Actuation System (DAS)

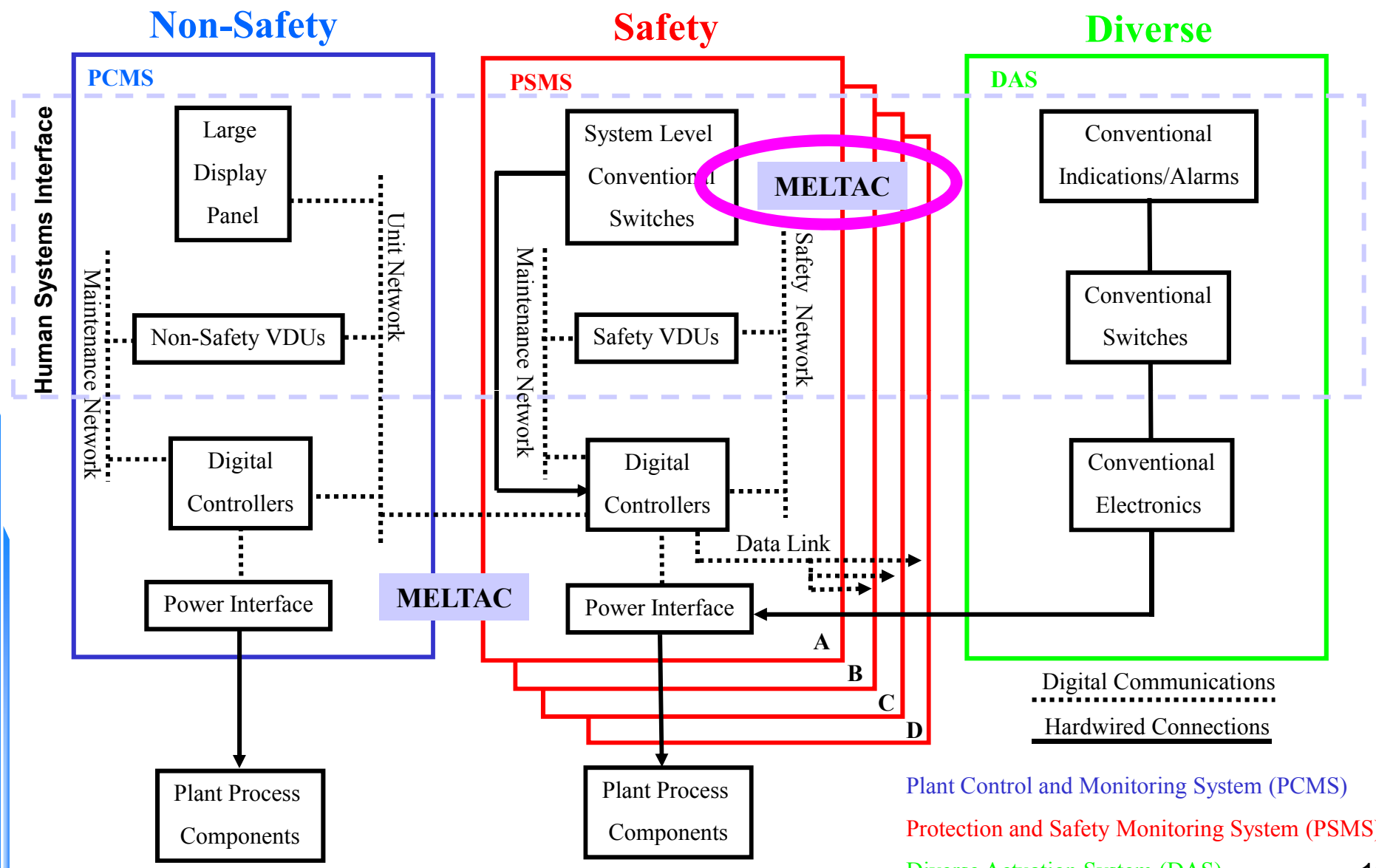
Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Inter-Division Digital Communication

- **MHI understanding of Staff concerns**
  - Unit Network – Operational VDUs (O-VDU)
  - Maintenance Network – MELTAC Engineering Tool (ET)
  - ✓ Have not been shown to support the safety function
  - ✓ The design is too complex
    - This complexity will require excessive review effort
  - ✓ Some specific areas of non-compliance with ISG-04
- **MHI will discuss**
  - ✓ How the design is consistent with NRC guidance regarding support for safety functions and complexity
  - ✓ Specific changes that can be made to more easily demonstrate compliance with ISG-04
  - ✓ **Additional information that may be needed by the Staff to complete the review**

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

MELTAC Quality Assurance



Plant Control and Monitoring System (PCMS)

Protection and Safety Monitoring System (PSMS)

Diverse Actuation System (DAS)

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

MELTAC Quality Assurance

- **MHI understanding of Staff concerns**
  - ✓ MELTAC FPGAs were developed as hardware, not software
  - ✓ Some MELTAC Basic Software did not have independent V&V
  - ✓ MELCO's QAP does not fully comply with 10CFR50 App. B
  - ✓ MELTAC was not originally developed under 10CFR50 App. B
- **MHI will discuss**
  - ✓ Compensatory measures taken for FPGAs and Basic Software
  - ✓ Corrective actions to establish QAP with full compliance to 10CFR50 Appendix B
  - ✓ Commercial grade dedication for MELTAC
  - ✓ The ITAACs that have removed this from the critical path of DCD review and MELTAC Topical Report review
  - ✓ **Additional information that may be needed by the Staff to complete the review**

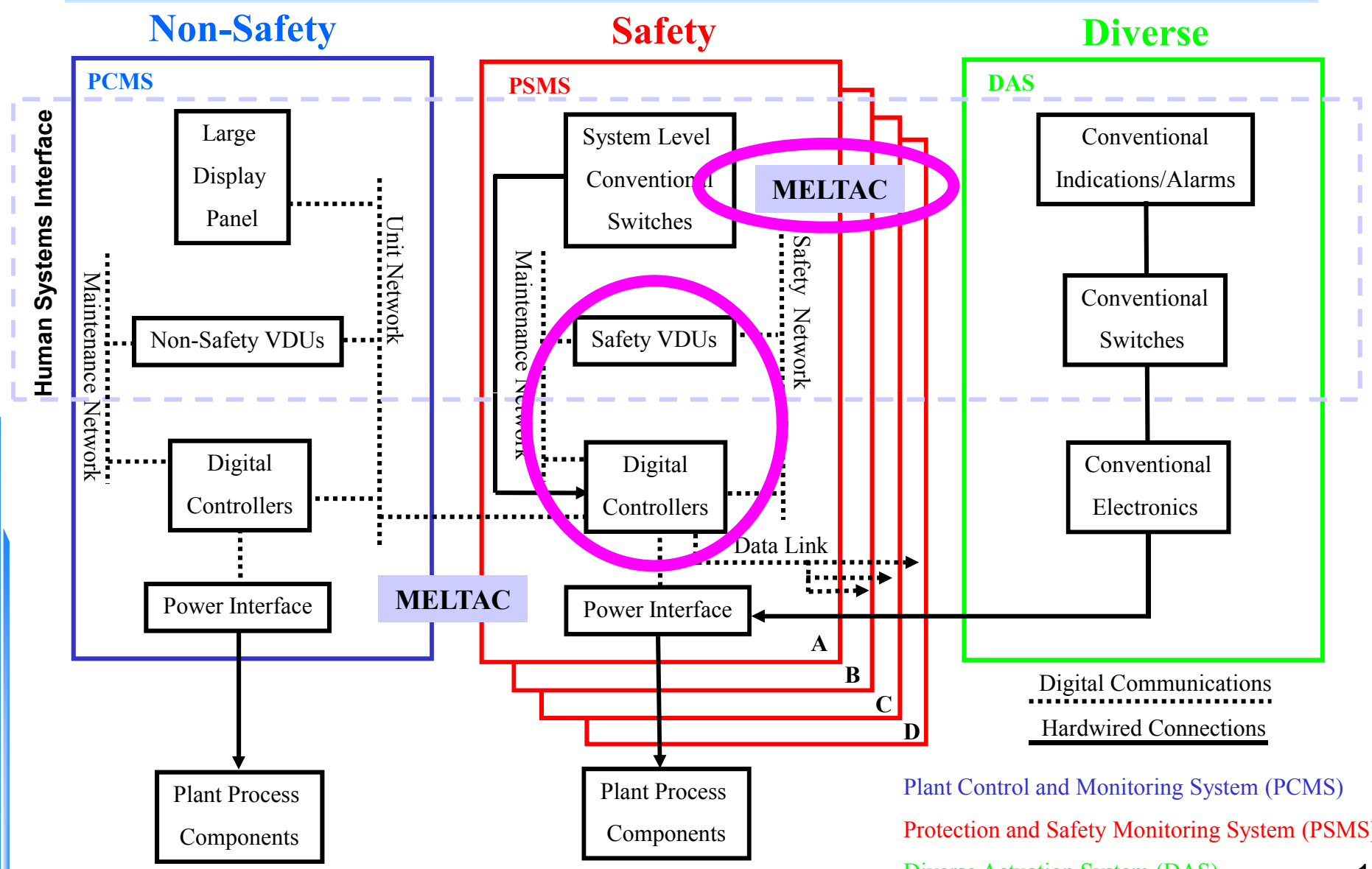
Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

MELTAC Quality Assurance

- **NRC Audit Report documents the high quality of MELTAC, 2008**
  - ✓ "Almost all of the original QA Program for the existing platform meets the requirements of Appendix B."
  - ✓ "The exception … Appendix B, Criterion I-4, "persons and organizations performing quality assurance … sufficient independence ..."
    - This is the same exception identified by MELCO and compensated for by the original Commercial Grade Dedication (CGD) activity (2006-2007), which MHI will discuss
  - ✓ "The software documentation is of high quality …The process can be followed by a knowledgeable lay person which is a primary test of documentation."
  - ✓ "The determination of software qualifying for Category 2 was more rigorous and better documented than indicated in the topical report."
  - ✓ "The testing documentation was sparse but sufficient for review."
  - ✓ "The Category 2 software also appears to be very high quality software. Review by a design review board or comparable V&V should be considered before accepting the Category 2 software."
    - Additional independent V&V was conducted 2009-2010, which MHI will discuss

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Software Life Cycle Process



Plant Control and Monitoring System (PCMS)

Protection and Safety Monitoring System (PSMS)

Diverse Actuation System (DAS)

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Software Life Cycle Process

- **MHI understanding of Staff concerns**
  - ✓ Software Program Manuals (SPM) do not address all areas of BTP 7-14 and referenced industry standards
  - ✓ SPMs do not demonstrate a "secure development and operational environment, as described in RG 1.152"
- **MHI will discuss**
  - ✓ The challenge of providing a balance between docketed and audited material
  - ✓ Compliance to existing security guidance (BTP 7-14 and RG 1.152)
  - ✓ Compliance to draft security guidance
    - "Secure development and operational environment" is initially addressed in DG-1249, which was issued for comment June 2010
    - From our perspective it does not seem appropriate for the NRC to suspend the Phase 2 US-APWR I&C review based on compliance with unreleased guidance
  - ✓ Additional information that may be needed by the Staff to complete the review

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Resolution of Open Issues

- **MHI has been working with the NRC to resolve these issues for ~18 months**
  - ✓ The following documents submitted April to July 2010 address these issues:
    1. Safety System Technical Report MUAP-07004 Rev 4
    2. MELTAC Platform Topical Report MUAP-07005 Rev 5
    3. Response Time of Safety I&C System MUAP-09021 Rev 1
    4. Instrument Setpoint Methodology MUAP-09022 Rev 1
    5. Function Assignment Analysis for Safety Logic System MUAP-09020 Rev 1
    6. [Application] Software Program Manual MUAP-07017 Rev 1
    7. MELTAC Platform Basic Software Program Manual JEXU-1012-1132 Rev 0
    8. MELTAC Platform FPGA V&V Final Report JEXU-1025-3009 Rev 0
    9. MELTAC Platform Category2 Additional V&V Final Report JEXU-1021-6301 Rev 0
    10. MELTAC Platform Re-evaluation Program Report JEXU-1022-6301 Rev 0
    11. MELTAC Platform Basic Software Safety Report JEXU-1015-1009 Rev 0
    12. MELCO 10CFR50 Appendix B QAP Phase 2 Audit Report PQG-HD-22021
  - ✓ We are awaiting NRC feedback on these documents
  - ✓ We can identify the specific information that addresses specific NRC concerns

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Resolution of Open Issues

- **July 27 public meeting NRC stated they consider the review of these areas complete and therefore cannot generate an SER**
  - ✓ MHI and NRC reached agreement on a plan to close these issues, February 2010
    - MHI has executed the plan
    - The submitted documents contain the information to close these issues
    - We are awaiting NRC feedback on the submitted documents
  - ✓ It is not uncommon for the NRC and suppliers/licensees to have difficulty reaching an acceptable "level of detail" or the "right information" in docketed material
  - ✓ We would like to continue working closely with the NRC to resolve these issues

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Resolution of Open Issues

- **We continue to believe a favorable safety determination depends only on reaching agreement on the detailed documentation the Staff needs docketed, and when that is needed**
  - ✓ Since the digital design submitted for the US-APWR is currently operating at 3 nuclear power plants in Japan, MHI can provide all the information necessary to resolve the information gap issue
  - ✓ We hope to continue working with Staff to identify that information for each area of concern
- **MHI will demonstrate how the documentation submitted to date addresses Staff concerns and MHI will make every effort to assist the Staff to ensure the documentation is well understood**
  - ✓ A design familiarization program at MEPPI in Pittsburgh has been planned for new I&C reviewers
- **We will expeditiously provide additional documentation where needed and work with the Staff to ensure it is well understood**

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Resolution of Open Issues

- **To facilitate expeditious NRC acceptance and thereby maintain the current US-APWR I&C review schedule MHI will propose design changes**
- **Through the information provided to date, through additional submittals, and through additional face-to-face review, we believe the NRC will have the information needed to write a near term SER**
  - ✓ With open issues <u>only for detailed implementation reviews</u>
  - ✓ Detailed implementation reviews can be conducted in Phase 4 or taken off the DCD critical path with additional ITAAC

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.