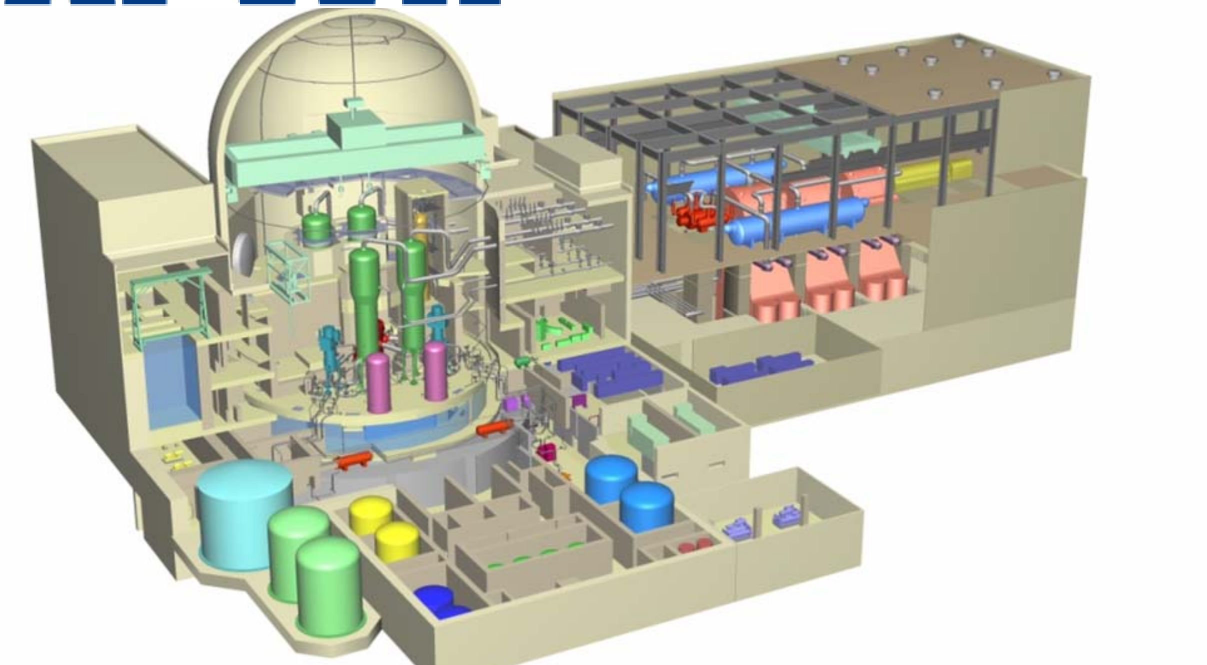
MITSUBISHI NUCLEAR ENERGY SYSTEMS, INC.

MITSUBISHI HEAVY INDUSTRIES, LTD.

MITSUBISHI
US-APWR



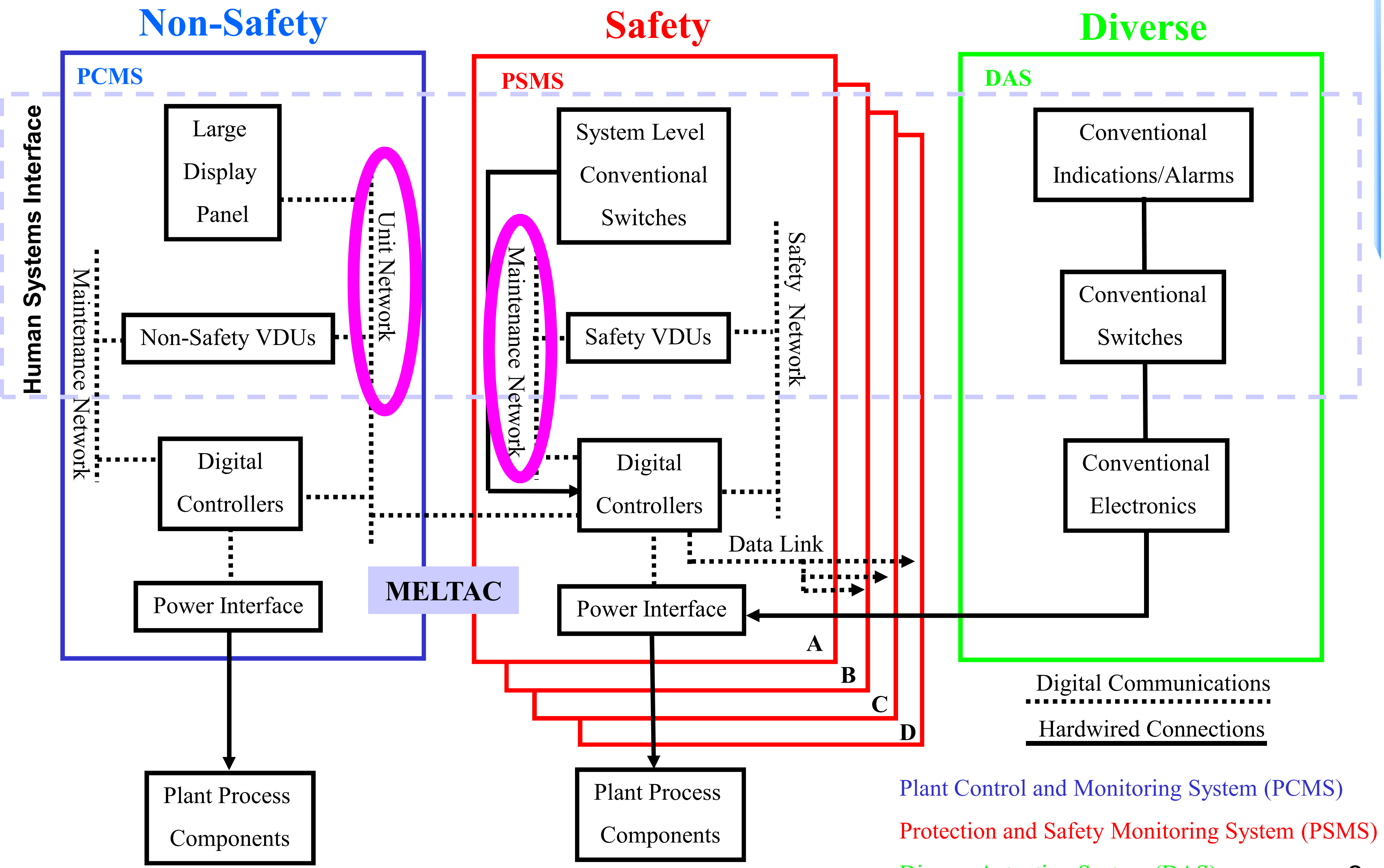
Digital I&C Key Licensing Issues
Inter-division Communication

August 18, 2010

Topics

- ➢ **Part 1**
  - ✓Digital I&C overview
  - ✓Key licensing open issues overview
- ➢ **Part 2**
  - ✓Issue Details
    - **Inter-division Communication**
    - MELTAC QA
    - Software Program Manuals

Inter-Division Digital Communication



Plant Control and Monitoring System (PCMS)

Protection and Safety Monitoring System (PSMS)

Diverse Actuation System (DAS)

Necessity and Complexity

➢ Specific NRC concerns

- ✓ August 11, 2010
  - The bi-directional communication aspects of the design are not necessary to provide the required safety functions, and the resulting increased complexity will require substantially more information to be submitted by MHI and reviewed by the staff.
  - MHI has not demonstrated that the safety divisions need to receive any communication from outside their own safety division. These bi-directional data communication flows have not been adequately justified to enhance or support a safety function.

Necessity and Complexity

- **NRC guidance recognizes the complexity of inter-division data communications, but also recognizes the enhancement to safety functions**
  - ✓ RG 1.152
  - ✓ DI&C Program Plan
  - ✓ ISG-04

Necessity and Complexity

- NRC perspective on enhancements and complexity
  - ✓ RG 1.152 Section B (Revision 2, 2006)
    - – Instrumentation and control system designs that use computers in safety systems make extensive use of advanced technology (i.e., equipment and design practices). These designs are expected to be significantly and functionally different from current designs
  - **"significantly and functionally different" implies NRC recognition that a more extensive review effort is expected**

Necessity and Complexity

- NRC perspective on enhancements and complexity
  - ✓ DI&C Project Plan (May 13, 2009)
    - There are clear potential advantages to the implementation of some types of cross-divisional communication within digital systems…The following types of communication interactions will be addressed by TWG #4…D. Control of safety equipment from a nonsafety workstation…F. Connection of nonsafety programming, maintenance, and test equipment to redundant safety divisions during operation…

- **"advantages" implies cross-divisional communication enhances the safety function for O-VDUs and ET**
  - TWG #4 will give due consideration to the burdens that might be imposed upon both applicants and NRC staff as a result of specific guidance. For example, acceptance of a certain provision might require detailed staff review in an area not presently subject to such review.

- **"burdens" and "detailed staff review" clearly denotes NRC recognition that additional staff review effort would be necessary**

Necessity and Complexity

US-APWR

➢ NRC perspective on enhancements and complexity

✓ ISG-04

» Contains more than 50 detailed criteria applicable to multi-division operator and engineering workstations

– **Clearly demonstrates NRC recognition that inter-division communication is a complex issue that warrants careful design consideration and extensive detailed review**

- **Introduction**

– This ISG describes how controls and indications from all safety divisions <u>can be combined</u> into a single integrated workstation <u>while maintaining separation, isolation, and independence</u> among redundant channels.

– **NRC recognition that O-VDU and ET can be implemented, while complying with current regulations**

Necessity and Complexity

- NRC perspective on enhancements and complexity
  - ✓ ISG-04
    - Section 3
      - This section presents guidance concerning operator workstations used for the control of plant equipment in more than one safety division and for display of information from sources in more than one safety division. This guidance also applies to workstations that are used to program, modify, monitor, or maintain safety systems that are not in the same safety division as the workstation.
    - **Explicit statement that guidance is applicable to O-VDU and ET, indicates NRC recognition that these features enhance the safety function**
      - Even though the use of multidivisional control and display stations is relatively new to the nuclear industry, the concepts to maintain the plant safety contained in this guidance is in line with the current NRC regulations
    - **NRC recognition that multi-division O-VDU and ET can be implemented, while complying with current regulations for independence**

Necessity and Complexity

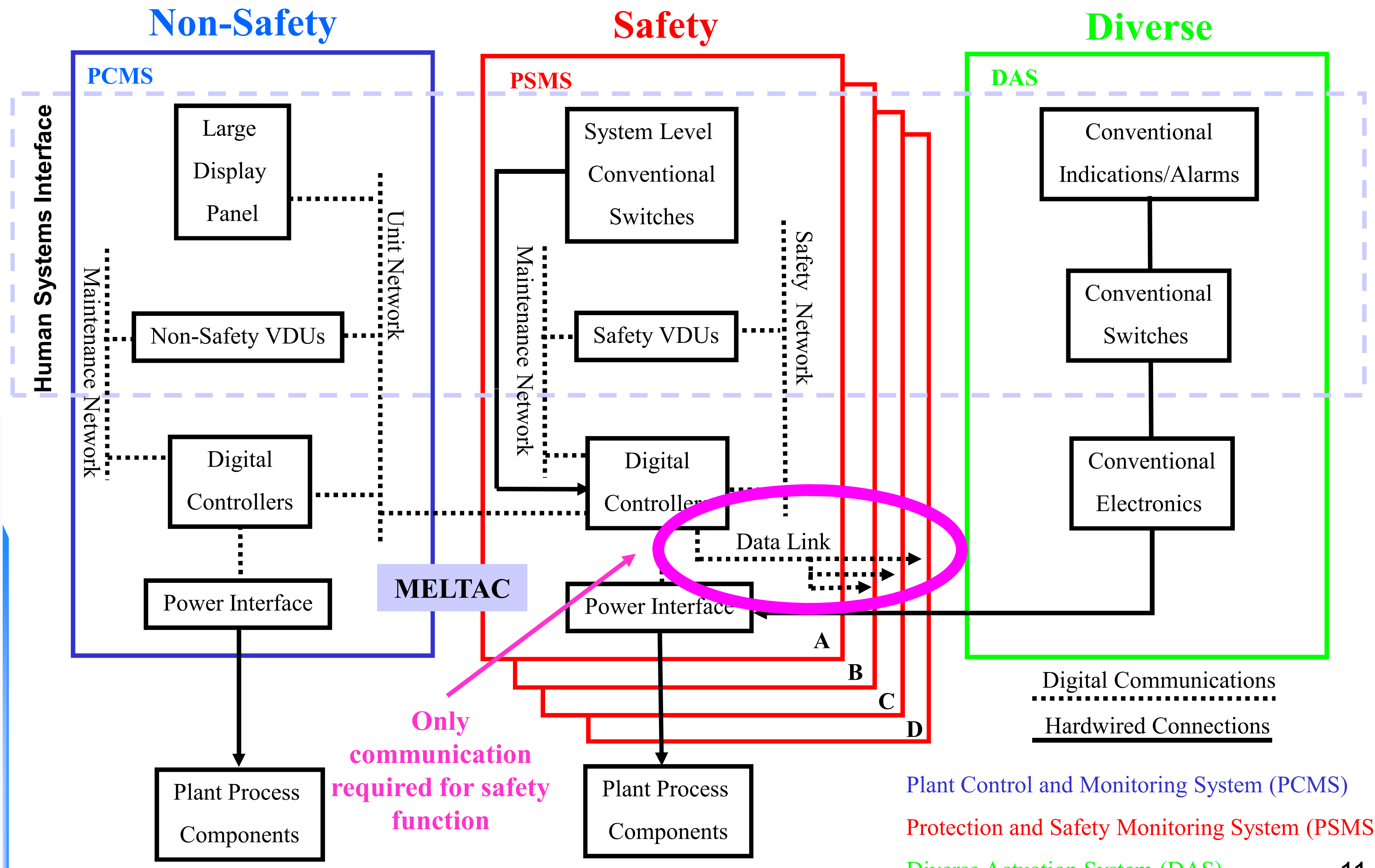
- ➢ NRC perspective on enhancements and complexity
  - ✓ ISG-04
    - Section 3.2
      - Non-safety multidivisional control and display stations may supplement the safety-related control and display equipment that is credited in the plant safety analyses.
    - **“supplement” implies NRC recognition that O-VDU is an enhancement**

Necessity and Complexity

US-APWR

- **MHI Perspective on enhancements to the safety function**
  - ✓ Unit Network and Maintenance Network **are not relied on for any safety functions**
    - Inter-division communication for safety functions is limited to data links for RPS and ESFAS voting logic
    - These data links are the only “vital communications”
      - – They are point-to-point links
        - » In accordance with ISG-04 Section 1.14

Inter-Division Digital Communication



Only communication required for safety function

Plant Control and Monitoring System (PCMS)

Protection and Safety Monitoring System (PSMS)

Diverse Actuation System (DAS)

Necessity and Complexity

- **MHI perspective on enhancements to the safety function**
  - ✓ NRC has stated that MHI has not demonstrated that the Unit Network and Maintenance Network are necessary
    - To comply with IEEE603 and ISG-04 <u>they cannot be necessary</u>
      - If they were necessary, they would need to be considered “vital communications” and would need to be Class 1E
    - Not necessary does not mean they do not enhance the safety function
      - **They do enhance the safety function**

Necessity and Complexity

- ➢ **MHI perspective on enhancements to the safety function**
  - ✓ Multi-division O-VDUs supplement divisionalized switches and Safety VDUs (S-VDUs) to improve operator human performance
    - – Execute EOPs
      - » Component controls
      - » ESFAS system level reset
    - – Control protection system operating bypasses during startup and shutdown evolutions
    - – Bypass failed protection channels to prevent spurious plant trips
    - – Bypass one of N redundancies to allow periodic surveillance testing

Necessity and Complexity

- **MHI perspective on enhancements to the safety function**
  - ✓ US-APWR Phase 1 HFE program confirmed the benefits using a full scope simulator with 13 US operating crews from Comanche Peak.
    - Providing these functions on multi-division O-VDUs allowed a single Reactor Operator (RO) to successfully manage very complex scenarios such as Steam Generator Tube Rupture (SGTR)
      - SGTR typically challenges 2 and 3 ROs in conventional designs, where HSI for each division is physically separated.
  - ✓ The Phase 1 HFE report clearly demonstrates the significant safety benefit of multi-division O-VDUs
    - The HFE Branch is preparing a favorable SER for the HSI Topical Report

Necessity and Complexity

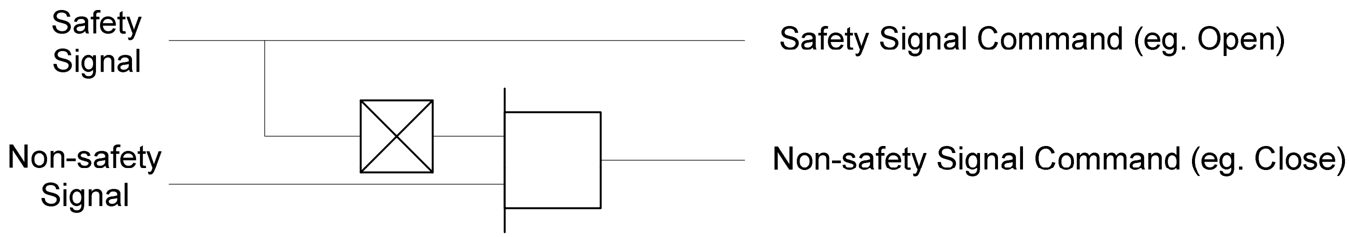
- ➢ **MHI perspective on enhancements to the safety function**
  - ✓ ETs improve the availability of all safety functions
    - Display self-diagnostic data to monitor routine system health prior to reaching alarm conditions
        - eg. communication errors, deterministic cycle times
      - Allows plant personnel to detect degrading conditions before failures occur
    - Display self-diagnostic group alarms with drill down to details of actual fault conditions
      - Allows plant personnel to quickly determine the significance of self-diagnostic alarms
        - Most alarms do not result in safety function INOPERABLE conditions
    - Display dynamic functional logic diagrams for process diagnostics
        - eg. why won't the pump start?
      - This expedites trouble shooting of failure conditions outside the digital system

Necessity and Complexity

- **MHI perspective on enhancements to the safety function**
  - ✓ If ETs are not licensed for permanent connection, the reliability of the safety functions is adversely affected
    - When it is connected the division to which it is connected must be declared INOPERABLE
      - This will result in an LCO
      - The LCO would be very limiting since it is common to have something INOPERABLE in another division
        - Typically return the function to service or achieve hot shutdown in 6 hours when two divisions are inoperable
      - Unnecessarily declaring a safety function INOPERABLE and unnecessary plant shutdown **will have a negative plant safety benefit**
      - **As a result plants are likely to defer alarm diagnosis**
  - ✓ Communication disconnect switches could be added to allow connection of the Maintenance Network to only one controller at a time
      - **This would add complexity and additional points of failure**
      - It would not eliminate the LCO
        - » But would reduce the potential for time limiting conditions

Necessity and Complexity

- **MHI perspective on complexity**
  - ✓ The logic to ensure the safety functions always have priority over the non-safety functions is simple combinational AND-NOT logic


Safety Signal
Non-safety Signal
Safety Signal Command (eg. Open)
Non-safety Signal Command (eg. Close)

- The priority logic is required regardless of the method of inter-division data communication, including hardwires

Necessity and Complexity

➢ MHI perspective on complexity

✓ Non-safety control signals are used to control safety components at many plants today

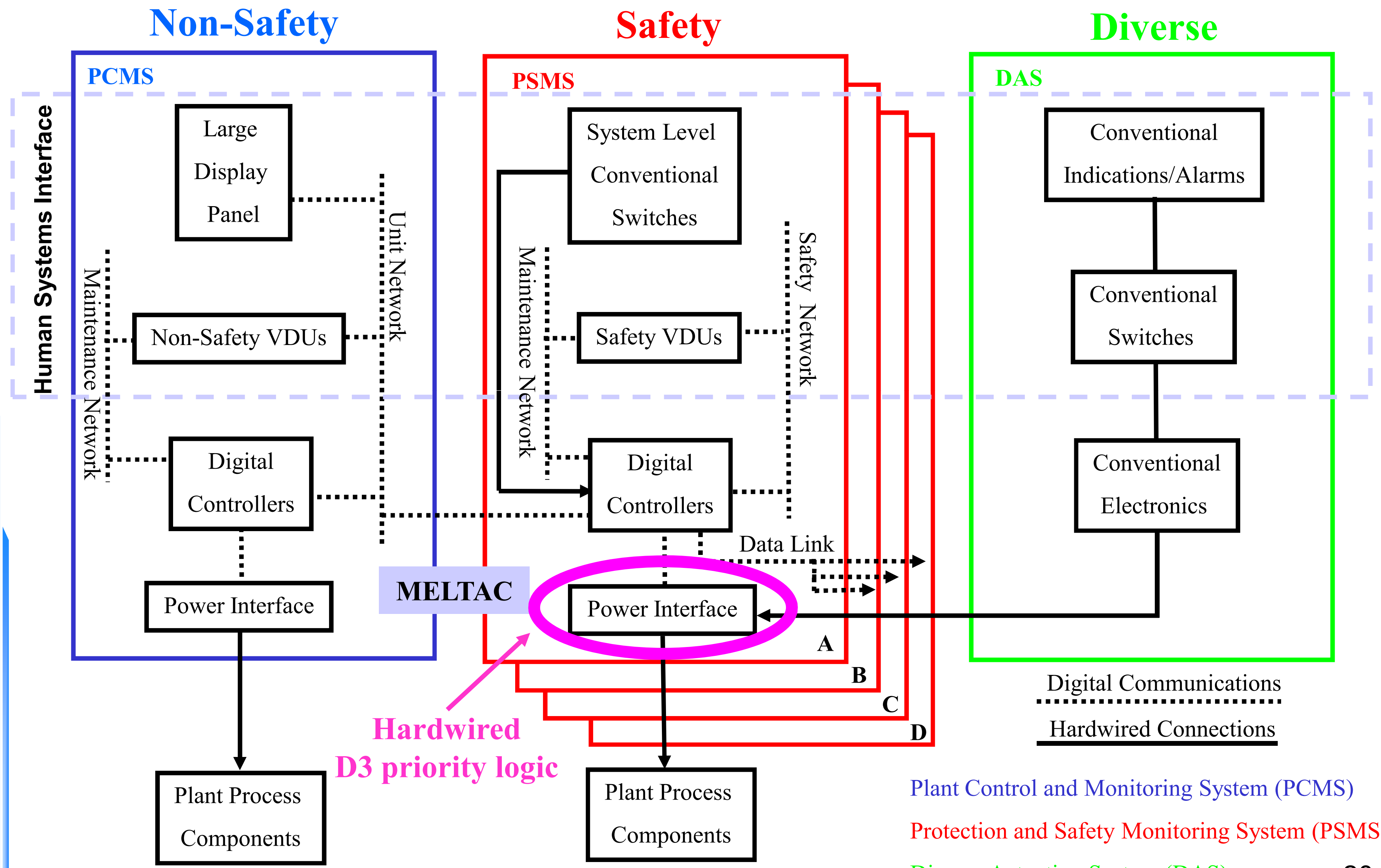
- Class 1E charging pumps are cycled by the non-safety pressurizer level control system and are actuated by Safety Injection Actuation Signal
- Class 1E pressurizer backup heaters are cycled by the non-safety pressurizer pressure control system and are actuated by the emergency load sequencer

✓ As in the US-APWR, simple combinational logic ensures the safety function has priority over non-safety functions

Necessity and Complexity

- **MHI perspective on complexity**
  - ✓ The priority logic to ensure the safety function can always be achieved by either the PSMS or DAS, regardless of software CCF in PSMS or hardware failure in DAS, is in conventional Class 1E hardware

Inter-Division Digital Communication



Plant Control and Monitoring System (PCMS)

Protection and Safety Monitoring System (PSMS)

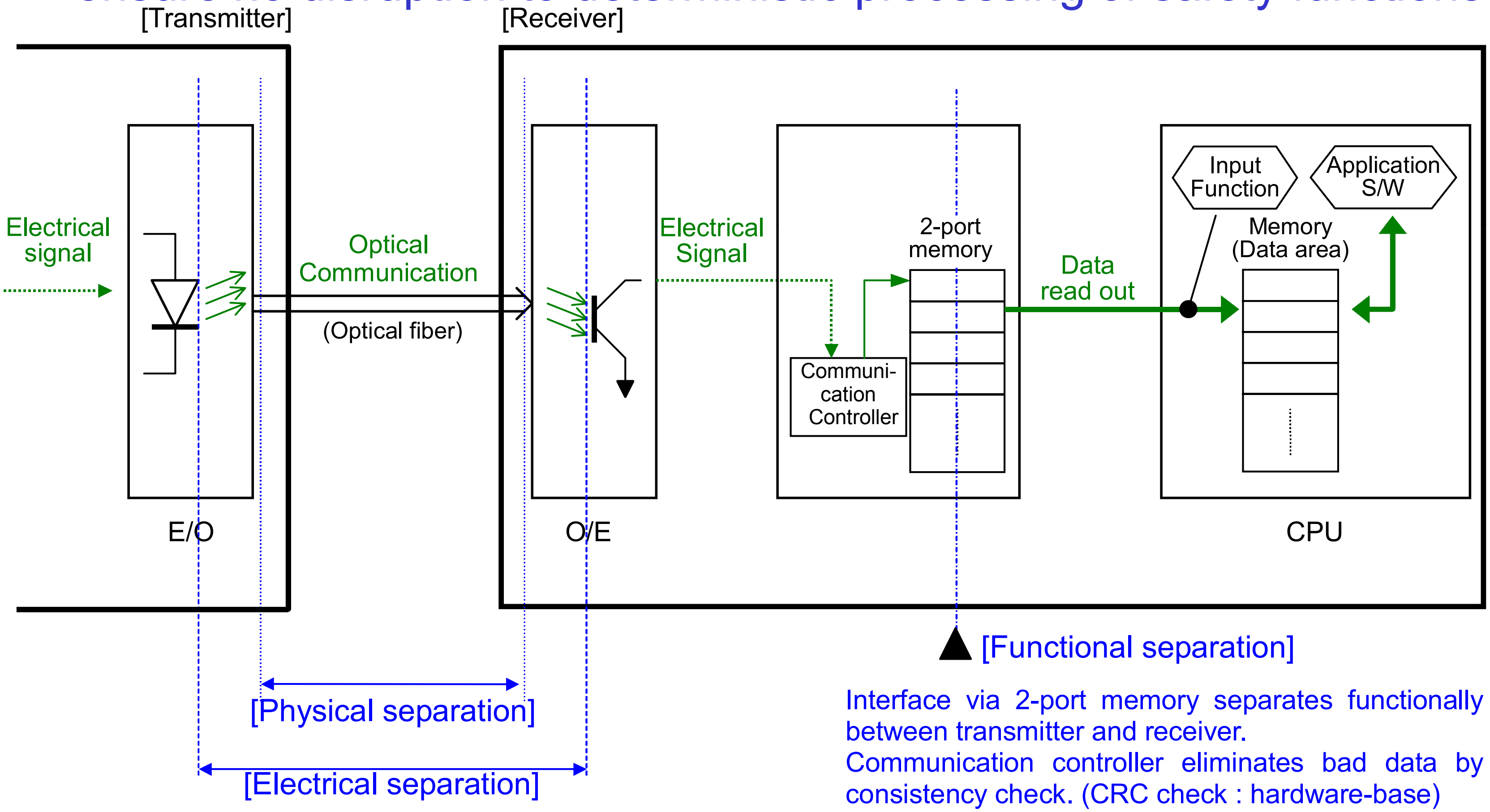
Diverse Actuation System (DAS)

Necessity and Complexity

- ➢ **MHI perspective on complexity**
  - ✓ For digital data communications experts, the design is straightforward
    - ✓ Standard industry communication methods are employed
      - ✓ None of the digital data communication technology is unique to MELTAC or to the nuclear industry
    - ✓ The information sources, destinations and data are fixed
  - ✓ But for the rest of us, whose expertise is not digital data communications, the design might seem complex
    - ✓ Unit Network
      - ✓ IEEE 802.17 RPR topology with IEEE 802.3z 1 Gbit Ethernet transmission medium
    - ✓ Maintenance Network
      - ✓ IEEE 802.3 using CSMA/CD, UDP/IP
  - ✓ The highest complexity is in dual CPUs with shared memory arbitration
      - – But that is the preferred method for computer independence in ISG-04
      - – It is also a long established digital communication technology

Digital Data Communication

- All intra-division or inter-division data communication uses the same method – applies to networks and data links
- In accordance with ISG-04 - Separate Central Processing Units (CPUs) for communications and functions, with shared memory ensure no disruption to deterministic processing of safety functions

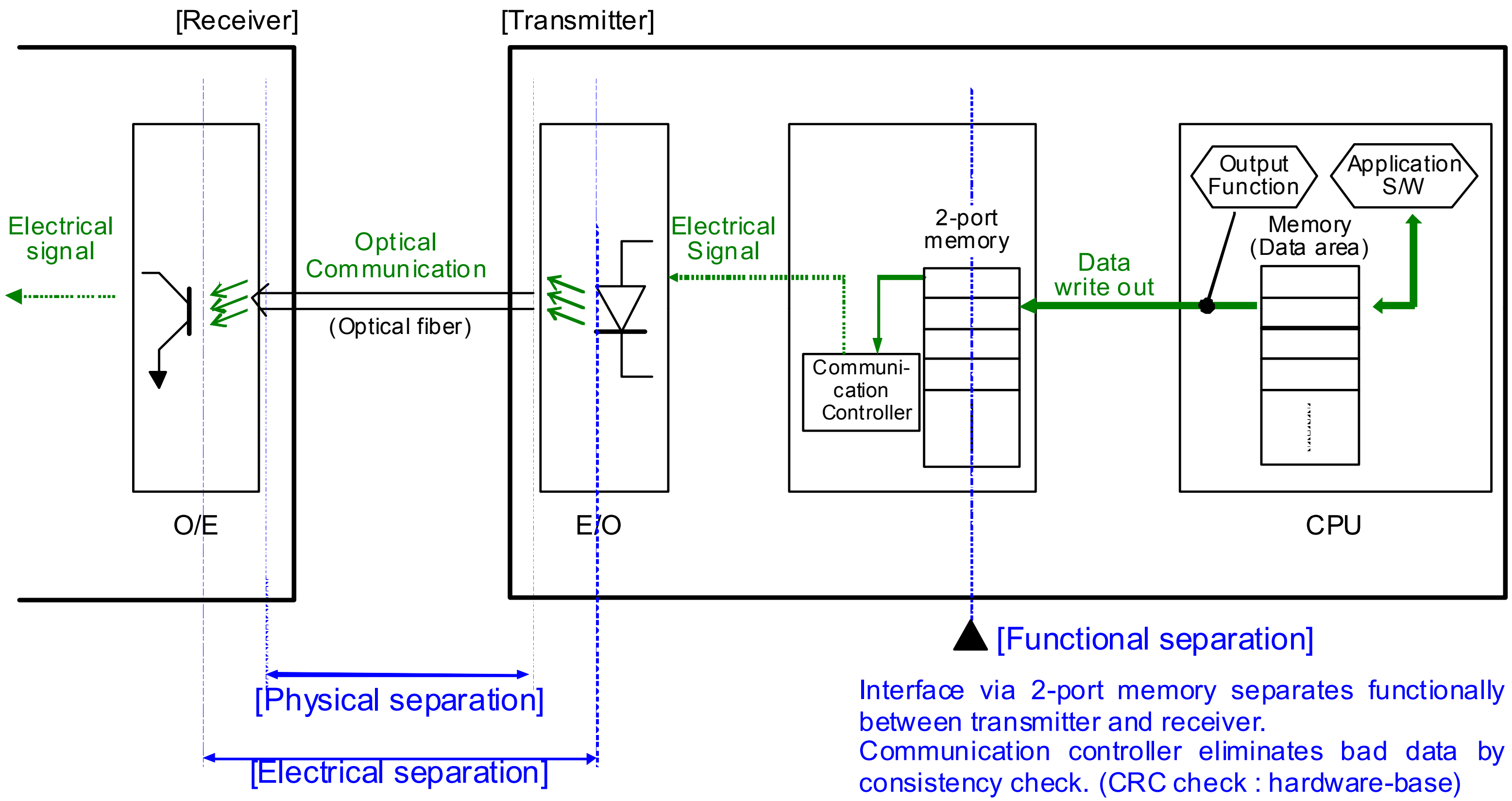


[Functional separation]

Interface via 2-port memory separates functionally between transmitter and receiver.
Communication controller eliminates bad data by consistency check. (CRC check : hardware-base)

Digital Data Communication

- Data is transmitted and received in the same manner
- For either case the deterministic operation of the main CPU is unaffected by data communication, in accordance with ISG-04



Interface via 2-port memory separates functionally between transmitter and receiver.
Communication controller eliminates bad data by consistency check. (CRC check : hardware-base)

Necessity and Complexity

➢ MHI perspective on complexity

- ✓ If all the signals are transmitted by hardwired cable, numerous cables, isolation devices and I/O modules are needed, and all of these interface connections must be manually tested periodically to ensure operability
- ✓ On the other hand, digital communications are completely redundant, continuously self tested, and use fiber optic cable for inherent isolation
- ✓ The total reliability of the digital communication is clearly higher than using hardwired communications

Necessity and Complexity

- ➢ **MHI perspective on complexity**
  - ✓ Unfortunately **“necessity”** and **“complexity”** are very subjective issues for which there is no regulatory guidance
  - ✓ MHI addressed these issues in the current documentation
  - ✓ MHI needs to clearly understand what additional information the NRC requires on the docket
  - ✓ Reaching agreement on subjective issues, such as this, should not be a basis for suspending the regulatory review process

Compliance to ISG-04

- **NRC identified two issues regarding compliance to the specific technical criteria in ISG-04**

1. Protection from Altering Priority Logic
2. Protection from Spurious Actuations

Protection from Altering Priority Logic

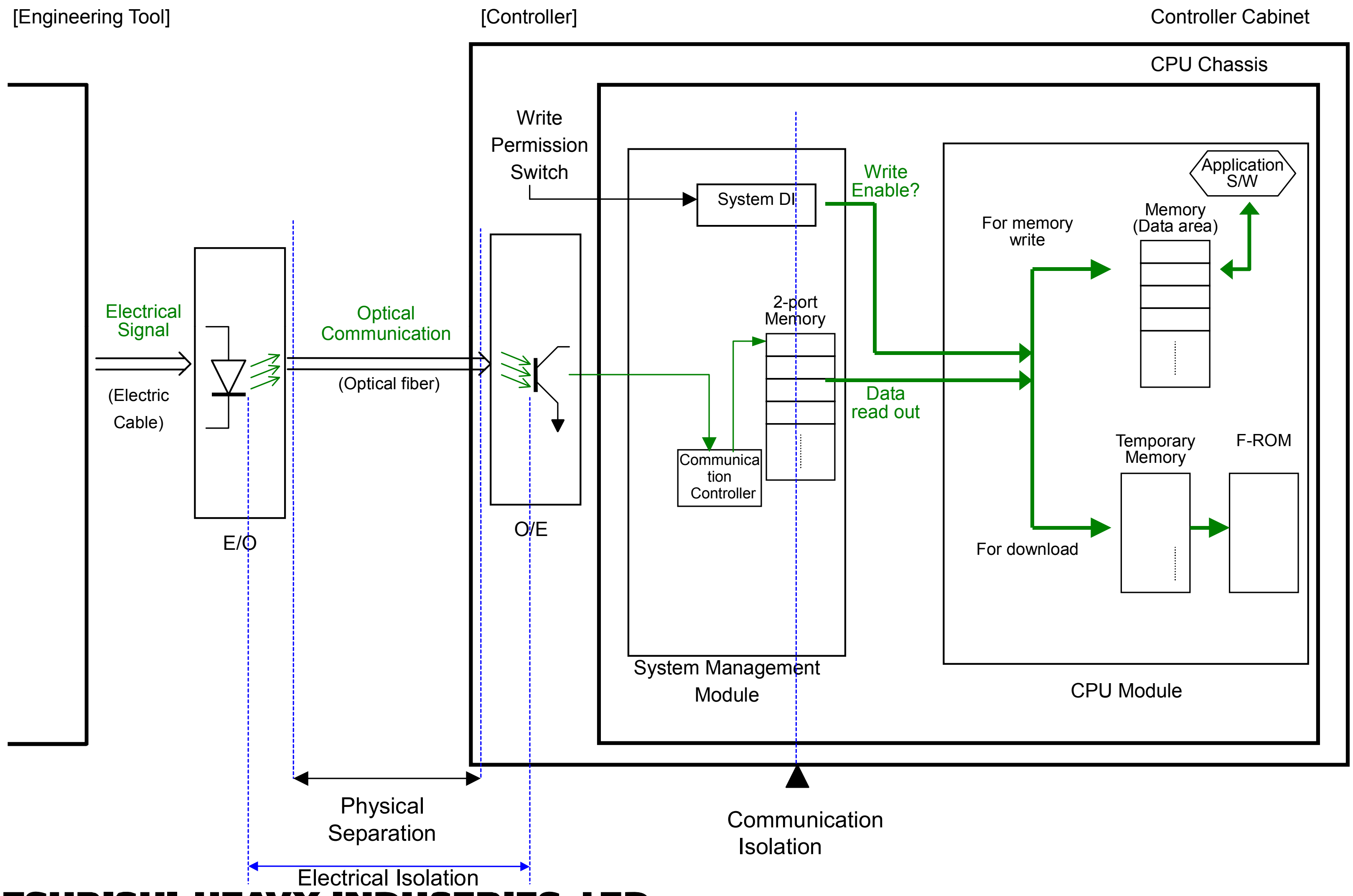
- Specific NRC concern
  - ✓ August 11, 2010
    - MHI has not demonstrated how their priority logic cannot be altered in the field. Staff guidance provides that the contents, such as priority logic, of nonvolatile memory should be changeable only through removal and replacement of the memory device

Protection from Altering Priority Logic

- **ISG-04 Section 2.7 has two requirements:**
  1. "All requirements that apply to safety-related software also apply to prioritization module software"
     - Section 1.10 "Safety division software should be protected from alteration … by means of keylock switch that …interrupts the connection by means of hardwired logic"
  2. "Nonvolatile memory (such as burned-in or reprogrammable gate arrays or random-access memory) should be changeable only through removal and replacement of the memory device"
- **"protected from alteration… by means of hardwired logic" and "changeable only through removal" are conflicting guidance**
- **MHI has justified that the priority logic in MELTAC is "protected from alteration"**
  - ✓ The priority logic is executed from non-volatile F-ROM, not volatile RAM
  - ✓ The F-ROM cannot be altered from the Unit Network interface
  - ✓ The F-ROM can only be altered from the Maintenance Network
    - And only when the Write Permission switch is enabled

Memory Write Permission

- The Write Permission interlock involves both hardware and software



Protection from Altering Priority Logic

- **MHI has identified the design of the Write Permission switch as an alternative to the "hardwired logic" guidance of ISG-04 Section 1.10, with justification based on**
  1. ISG-04 guidance is primarily to provide memory protection for multi-division maintenance networks to ensure a single failure cannot cause inadvertent software changes in multiple divisions
     - For MELTAC there are separate Maintenance Networks and separate ETs for each division, therefore the system architecture provides inherent protection against single failures
  2. The software that controls the interlock is in non-alterable read only memory
     - The ROM must be physically replaced to change this software
  3. All software is continuously checked for unintended alteration by self-diagnostics
  4. Periodic diverse memory integrity tests ensure there has been no unintended software change
  5. The priority logic for D3 functions is hardware based
     - The DAS provides protection against a CCF resulting from any unintended priority logic alteration
- **The NRC has been reviewing this design justification**
  - ✓ MHI has expected the NRC to accept the design, since a hybrid write permission design was previously approved for Oconee
  - ✓ NRC has not identified that the design is unacceptable

Protection from Altering Priority Logic

- **The design can be changed to facilitate expeditious NRC acceptance and thereby maintain the current US-APWR I&C review schedule**

1. The Write Permission switch can directly control the write enable port of the F-ROM that contains all application software, including priority logic
   - The Write Permission function will have no reliance on software
     - The Write Permission switch will interface to the F-ROM through simple interlock logic implemented in an unalterable FPGA
2. For the US-APWR the ET location can be limited to the I&C equipment rooms
   - Currently there are also ETs in the maintenance facility within the vital area
3. For the US-APWR the diverse memory integrity test can be conducted on a staggered monthly basis, with all controllers tested every 24 months
     - If a monthly test reveals any unintended software alteration, all controllers will be checked
   - Current tech specs only require 24 month surveillance

Protection from Altering Priority Logic

➢ Write Permission design change

- ✓ This change requires a minor update to the MELTAC Topical Report which can be made by September 2010
- ✓ The implementation details of this design can be addressed through Tier 1 with appropriate ITAAC, eg.
  - All software and firmware is protected from unintended alteration by physical and hardwired barriers
    - – Confirmed through inspection of digital platform life cycle* and inspection of locks on rooms and controller cabinets
    - – *The life cycle processes that ensure the features above are implemented and maintained with appropriate quality are already addressed in ITAACs 24, 30a and 30b in Table 2.5.1-6.
- ✓ MHI needs to clearly understand what additional information the NRC requires on the docket

Protection from Spurious Actuations

➢ Specific NRC concern

✓ August 11, 2010

- MHI has not adequately defined the potential failure modes associated with bi-directional communication. A software error from a non-safety device producing a valid, but conflicting, command is an example of a failure mode that would be considered credible.
- MHI has not demonstrated that the safety system or operator, by backup safety commands, has sufficient time or indications of communications failures to take appropriate actions and, if necessary, disable the non-safety display unit

Protection from Spurious Actuations

- The potential failure modes of the inter-division communication are identified and analyzed in the MELTAC Software Safety Analysis (Rev 2 March 2010)
- Communication error detection features reject all communication faults identified in ISG-04 Section 1.12
- Other credible faults have been identified and analyzed
  - ✓ Invalid floating point numbers
  - ✓ Out of range values
  - ✓ A range of hardware and software failures for each module
  - ✓ Potential adverse impacts from self-diagnostics
  - ✓ Configuration control errors in each life cycle phase

Protection from Spurious Actuations

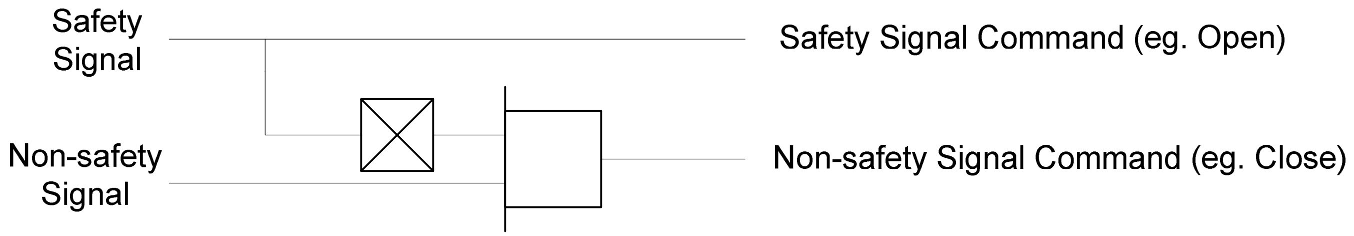
- **Single spurious valid commands are addressed in MUAP-07004 (Rev 0 2007)**
  - ✓ Spurious actuations of non-safety functions are the same as control system failures, which are bounded by the AOOs in the plant's safety analysis
  - ✓ Spurious actuation of safety functions are already analyzed in the safety system FMEA
- **A single failure that results in multiple spurious valid commands is considered incredible, based on compliance with ISG-04 Section 3.1.5 Bullet 4**
    - Two distinct control actions "as described here is to provide protection from spurious actuations, not protection from operator error."
  - ✓ O-VDU requires two distinct control actions to build command messages
  - ✓ O-VDU has augmented quality
    - Independent software V&V
    - Equipment qualification

Protection from Spurious Actuations

- **Regardless of this incredibility, the effect of <u>multiple</u> spurious valid commands on safety functions was added to the Safety System TR Appendix D (Rev4, April 2010)**
  - **Based on NRC request Feb. 2010**
  - ✓ Priority interlocks prevent any adverse affect for Operating Bypasses, Maintenance Bypasses and RPS/ESFAS Reset
  - ✓ Spurious component actuations are overridden by ESFAS priority logic
    - Therefore there is no operator action needed
  - ✓ For safety components without ESFAS, spurious component actuations are self-announcing by Spatially Dedicated Continuously Visible (SDCV) Bypassed or Inoperable Status Indication (BISI) alarms
    - Therefore, corrective actions can be taken quickly by operators prior to AOO or PA
      - Operator action is facilitated by priority logic
  - ✓ We are awaiting NRC feedback
    - An operator time response analysis can be provided
- **MHI needs to clearly understand what additional information the NRC requires on the docket**

Protection from Spurious Actuations

- **The design can be changed to facilitate expeditious NRC acceptance and thereby maintain the current US-APWR I&C review schedule**
  - ESFAS signals with priority logic can be added to all safety components to eliminate the need for manual operator actions


Safety Signal
Non-safety Signal
Safety Signal Command (eg. Open)
Non-safety Signal Command (eg. Close)

✓ This change requires updates to ESF system P&IDs, not Chapter 7 of the DCD

- This change can be made in DCD rev 3

✓ The Safety System Technical Report analysis in MUAP-07004 would also be updated to reflect this change

- This change can be made by September 2010

Inter-division Communication

➢ Level of detail summary

- ✓ The critical technical aspects of the inter-division communication design that ensure compliance to ISG-04 are described in Tier 2
  - Either directly in the DCD or in referenced Topical and Technical Reports
  - Additional technical detail will be docketed where the Staff deems it necessary to make their safety determination
- ✓ However, MHI believes the NRC is primarily concerned about implementation detail, not critical design commitments
- ✓ To take the detailed implementation review off the DCD critical path, additional commitment details, with related ITAACs can be added to Tier 1
  - These ITAACs would allow the detailed implementation of the inter-division data communication features to be reviewed in Phase 4 or after DCD approval