MHI Position on Basic SPM withdrawal Issue

MHI Position

MHI proposes to withdraw the Basic SPM (MELTAC Platform Basic Software Program Manual, JEXU-1012-1132) from the DCD Chapter 7 review, with the following conditions.

1. The NRC provides SER for the DCD Chapter 7 which identifies the contents of the Technical Report, MUAP-07005 "Safety System Digital Platform – MELTAC" including the existing software life cycle process description in Section 6, the inspection report for the MRP and the inspection report for the Basic SPM as described below.

2. The Basic SPM is withdrawn from the DCD Chapter 7 review, but MELCO keeps the B-SPM as an internal procedure, and the Basic SPM is referred to from the Technical Report, MUAP-07005 "Safety System Digital Platform – MELTAC", and the Technical Report, MUAP-07017 "US-APWR Software Program Manual" as follows:

   For MUAP-07005 "Safety System Digital Platform – MELTAC"
   The existing description of the basic software life cycle process (Section 6) is retained, and JEXU-1012-1132B "MELTAC Platform Basic Software Program Manual" will be referred from Section 6 of this Technical Report for applicability to any revision of the MELTAC legacy basic software or any new MELTAC basic software.

   For MUAP-07017 "US-APWR Software Program Manual"
   The Purpose and Scope of this Technical Report will be revised to clarity that this document encompasses not only for the PSMS Application Software, but also MELTAC Basic Software.
   Following description will be added to appropriate sections of this Technical Report;

   To verify that the as-built Basic Software of the MELTAC Platform for the US-APWR plant is developed and supplied under control by JEXU-1012-1132B "MELTAC Platform Basic Software Program Manual".

3. The Basic SPM will be inspected by the NRC during the MRP inspection, and the NRC will include the Basic SPM inspection report results in the inspection report.

4. Following ITAAC-30b is deleted.

DC	ITA	AC
After commercial grade dedication, the PSMS digital platform is managed by a life cycle process that meets the regulatory requirements for Class 1E safety systems. The Class 1E product life cycle management encompasses manufacturing, configuration management, design change management, error reporting and corrective actions, and cyber security.	Inspections of the post-development life cycle documentation of the PSMS digital platform will be performed.	The PSMS digital platform is managed by a life cycle process that meets the regulatory requirements for Class 1E safety systems.

5. ITAAC 24 has been revised for the PSMS Application and Basic Software.

DC	ITA	AC
The PSMS hardware and software are developed and managed by the Basic and Application Software Program Manuals ~~a lifecycle process~~ that meet the regulatory requirements for Class 1E safety systems, and which encompasses the entire product life cycle including software V&V and configuration management.	Inspections of the as-built hardware and software life cycle documentation of the PSMS will be performed	The as-built PSMS hardware and software are developed and managed by the Basic and Application Software Program Manuals ~~a lifecycle process~~ that meet the regulatory requirements for Class 1E safety systems, and which encompasses the entire product life cycle including software V&V and configuration management.

This ITAAC will be expanded for each lifecycle phase.

Staff Comments on Withdrawal of Basic SPM review

a. Overall, the NRC staff does not have an issue with, and plan to accept the proposal at the public meeting in April.

b. For Condition 2, the phrase "… for applicability to any revision of the MELTAC legacy basic software or any new MELTAC basic software" needs to be clarified. The Basic SPM is for the Appendix B-based QAP for all activities related to the Basic MELTAC Platform conducted after the MRP (as stated in the Basic SPM). The NRC staff needs to understand this discrepancy clearly.

c. For Condition 2, where does MHI plan to put the statement "**To verify that the as-built Basic Software of the MELTAC Platform for the US-APWR plant is developed and supplied under control by JEXU-1012-1132B**?" Has MHI considered placing it in the DCD?

d. For Condition 5, "**A report exists and concludes that the basic and application software of the PSMS are developed in accordance with the US-APWR SPM"**   Is there more details to the acceptance criteria other than what is stated there? For example, details such as (BTP 7-14) design or implementation outputs for each life cycle phase would be more specific to evaluate if the acceptance criteria have been met or not.

e. As a general comment on the Basic SPM, the NRC staff has identified issues, as indicated by several RAIs (some of which MHI has already seen).

03/18/2011

Additional Description on Augmented Quality Issue
(Item 5 of Action Item List)

1. Scope of the Augmented Quality Sysetms

Attachment-1 will be added in DCD Chapter 7.

2. Classification for I&C Systems

Attachment-2 will be added in DCD Chapter 3.

3. Software Lifecycle Requirements for the augmented quality systems

Attachment-3 will be added in the US-APWR SPM, MUAP-07017.

Attachment-1

Table 7.X: Scope of the Augmented Quality Systems

Items	Specific requirements for non safety-related system	DCD Commitments for Augmented Quality Systems
Safety Functions Controlled by O-VDUs	DI&C-ISG-04	Required
Safety Parameter Display System (SPDS)	10 CFR 50.34 (f)(2)(iv), “Additional TMI-Related Requirements” regarding the SPDS Control	Required
	NUREG 0737 Supplement 1, “Clarification of TMI Action Plan Requirements - Requirements for Emergency Response Capability”, with respect to SPDS	
Alarms for Credited Manual Operator Actions	SECY-93-087, Item II. T, “Control Room Annunciator (Alarm) Reliability”	Required
Signal Selection Algorithm (SSA)	RG 1.153, “Criteria for Safety Systems”	Required
	IEEE 603-1991, Clause 6.3 “Interaction between the Sense and Command features and other Systems”	
Bypass and Inoperable Indication (BISI)	10 CFR 50.34(f)(2)(v) “Additional TMI-Related Requirements” regarding the bypassed and inoperable status indication	N/A (There is no augmented quality requirement.)
	RG 1.47, “Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems”	
	BTP 8-5, “Supplemental Guidance For Bypass And Inoperable Status Indication For Engineered Safety Features Systems”	
	IEEE 603-1991, Clause 5.8 “Information Displays”	
Diverse Instrumentation and Control System	BTP 7-19, “Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems”	Required
	Generic Letter 85-06, “Quality Assurance Guidance for ATWS Equipment That Is Not Safety-Related”	
Post Accident Monitoring Instrumentation	10 CFR 50, Appendix A: GDC 13, 19 and 64, for specific requirement to provide adequate instrumentation to monitor PA condition(s)	N/A (Type A, B, C and D are implemented in the PSMS and there is no augmented requirement for Type E.
	10 CFR 50.34 (f)(2) “Additional TMI-Related Requirements”	
	RG 1.97, “Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants”	
	BTP 7-10, “Guidance on Application of Regulatory Guide 1.97”	
	IEEE Std 497-2002, “IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations”	
Leak Detection System	RG 1.45, “Guidance on Monitoring and Responding to Reactor Coolant System Leakage”	N/A (Seismic required systems are implemented in the PSMS and there is no augmented requirement for others.)

Attachment-2

Table 3.X Classification of I&C systems (Sheet 1 of 3)

System	Equipment Class	Location	IEEE 603 Class	Quality[1] Assurance	Equipment[2] Qualification	Seismic[3] Category	Notes[4]
1. PSMS							
Reactor Protection System	3	R/B	Class 1E	1	1	I	
ESF Actuation System	3	R/B	Class 1E	1	1	I	
Safety Logic System	3	R/B	Class 1E	1	1	I	
Safety VDU Processor	3	R/B	Class 1E	1	1	I	
Communication System	3	R/B	Class 1E	1	1	I	
Safety Bus	3	R/B	Class 1E	1	1	I	
2. PCMS (DCS)							
Reactor Control System (SSA)	5	A/B	N/A	2	1	NS	4
Reactor Control System	9	A/B	N/A	2	2	NS	
CRDM Control System	9	A/B	N/A	2	2	NS	
Radiation Monitoring System	9	A/B	N/A	2	2	NS	
Rod Position Indication System	9	PCCV	N/A	2	2	NS	
Incore Nuclear Instrumentation System	9	A/B	N/A	2	2	NS	
BOP Control System	9	A/B	N/A	2	2	NS	
Turbine Protection System	9	A/B	N/A	2	2	NS	
Turbine EHG Control System	9	A/B	N/A	2	2	NS	
Electrical Control System	9	A/B	N/A	2	2	NS	
Unit Bus	5	R/B, A/B	N/A	2	1	NS	1, 2, 3, 4

Table 3.X Classification of I&C systems (Sheet 2 of 3)

System	Equipment Class	Location	IEEE 603 Class	Quality[(1)] Assurance	Equipment[(2)] Qualification	Seismic[(3)] Category	Notes[(4)]
3. PCMS (HSIS)							
Alarm VDU Computer	5	A/B	N/A	2	1	NS	3
Operational VDU Computer (for OC)	5	A/B	N/A	2	1	NS	1, 2
Operating Procedure VDU Computer (for OC)	10	A/B	N/A	3	2	NS	
Large Display Computer (for LDP)	10	A/B	N/A	3	2	NS	
Alarm Logic Computer	5	A/B	N/A	2	1	NS	3
Process Recording Computer	10	A/B	N/A	3	2	NS	
Unit Management Computer	10	A/B	N/A	3	2	NS	
Operational VDU Computer (for TSC)	10	AC/B	N/A	3	2	NS	
Large Display Computer (for TSC)	10	AC/B	N/A	3	2	NS	
Supervisor Console	10	R/B	N/A	3	2	NS	
Shift Technical Advisor Console	10	R/B	N/A	3	2	NS	
Large Display Panel	10	R/B	N/A	3	2	NS	
Station Bus	10	A/B	N/A	3	2	NS	
4. PSMS/PCMS							
Operator Console	3	R/B	Class 1E	1	1	I	
Remote Shutdown Console	3	R/B	Class 1E	1	1	I	

Table 3.X Classification of I&C systems (Sheet 3 of 3)

System	Equipment Class	Location	IEEE 603 Class	Quality[1] Assurance	Equipment[2] Qualification	Seismic[3] Category	Notes[4]
5. DAS							
Diverse Actuation System	5	R/B	N/A	2	1	II	5
Diverse HSI Panel	5	R/B	N/A	2	1	II	5
6. Local							
Reactor Trip Breaker	3	R/B	Class 1E	1	1	I	
M/G Set	5	R/B	N/A	2	1	NS	5

Notes:

(1) Identification number for “Quality Assurance”

1. The QA requirement of 10 CFR 50, Appendix B is applied.
   For application software, “Software Program Manual” (MUAP-07017) is applied.
2. The pertinent QA requirement of 10 CFR 50, Appendix B is applied.
   For application software of Class 5 systems, Appendix D of “Software Program Manual” (MUAP-07017) is applied.
3. Industry Standards, ISO 9001, etc, are applied.

(2) Identification number for “Equipment Qualification”

1. “Equipment Qualification Program” (MUAP-08015) are applied.
2. Industry standards are applied.
   For EMC/RFI emission, RG 1.180 is applied so that safety-related I&C equipment has no adverse EMC/RFI impact.

(3) Following augmented qualification requirements are applied concurrent with SSE, and IEEE 344-1987 is applied.

- Reactor control system shall retain the function described in Note (4) 3, 4.
- Operational VDU Processor shall retain the function described in Note (4) 1, 2.
- Alarm VDU Processor and Alarm VDU Computer shall retain the function described in Note (4) 3.
- Unit bus shall retain the functions described in Note (4) 1, 2, 3, 4.
- Diverse Actuation System and Diverse HSI Panel shall retain the function described in Note (4) 5.

(4) Identification number for “Note”

1. Safety Functions Controlled by O-VDU
2. Safety Parameter Display System (SPDS)
3. Alarms for Credited Manual Operator Actions
4. Signal Selection Algorithm (SSA)
5. Diverse Instrumentation and Control System

Attachment-3

Appendix D: Software Program Manual for Augmented Quality Systems

1. Scope

The Basic and Application software of the PSMS is classified as Class 1E based on the definition of IEEE Std 603-1991, and the Basic and Application software is classified as software integrity level (level 4) in accordance with Chapter 1 of RG 1.168 Rev. 1 and comply with this US-APWR Software Program Manual, MUAP-07017.

The Plant Control and Monitoring System (PCMS) are categorized in the non safety-related system, but the several systems in the PCMS have the specific regulatory requirements and these systems are categorized as the augmented quality system. The System Quality Group Classifications are described in Section 3 “Design of Structures, Systems, Components, and Equipment”, and the several digital I&C systems in the PCMS are categorized in the Equipment Class 5 which systems must meet the pertinent QA requirements of 10 CFR 50, Appendix B as described in Section 3.2.2.5 of the DCD.

The equipment classes of all systems are listed in Table 3.X of DCD Chapter 3 (Attachiment-2), and the systems which are categorized as the Equipment Class 5 are required the augmented quality. The actual scopes of the augmented quality systems and the applied regulatory requirements for each system are described in Table 7.X of DCD Chapter 7 (Attachment-1).

2. Software Life Cycle Requirements

The degraded software life cycle processes are required for the augmented quality systems as described in Table D-1.

For the hardware and basic software of the augmented quality systems which are not special for the US-APWR, the pertinent QA requirements of 10 CFR 50, Appendix B as described in Section 3.2.2.5 of the DCD are required same as other SSCs, such as, Equipment Class 5 structures, structural components, non digital I&C and electrical components.

For the application software of the augmented quality systems which are special for the US-APWR, the software life cycle control requirements which are specified by this US-APWR Software Program Manual are applied. Basically, almost software life cycle control requirements for the PSMS are applied to the augmented quality system in the PCMS as described in Table D-1.

Table D-1: Software Plans Applicability

Software Plans	PSMS	Augmented Quality System
Software Management Plan (SMP)	A	A
Software Development Plan (SDP)	A	A
Software Quality Assurance Plan (SQAP)	A	A(1)
Software Integration Plan (SIntP)	A	A
Software Installation Plan (SInstP)	A	A
Software Maintenance Plan (SMaintP)	A	A
Software Training Plan (STrngP)	A	A
Software Operations Plan (SOP)	A	A
Software Safety Plan (SSP)	A	N/A
Software Verification and Validation Plan (SVVP)	A	A(2)
Software Configuration Management Plan (SCMP)	A	A
Software Test Plan (STP)	A	A

Note: A-applicable N/A-not applicable

(1) Based on QA requirements for Equipment Class 5 Systems in Section 3 of DCD Chapter 3.

(2) The V&V activities are conducted by Design Team.

Design change on Safety VDU

1. Background

The US-APWR HSI/HFE Topical Report, MUAP-07007 (Section 4.11 of Reference 1) describes that the loss of the HSI/degraded operating configurations are considered in the HSIS design:

- Degraded HSI systems by single failure
- Loss of all non-safety HSI
- Loss of all digital non-safety and safety HSI (Common cause failure (CCF))
- Loss of MCR

In the US-APWR Phase 1 V&V, a scenario for the loss of all non-safety HSI was simulated and the dynamic validation by using PWR simulator was conducted. As a result of the validation, the human engineering discrepancy (HED) regarding;

- Situation awareness for plant overall status
- Task burden (navigation of in or between safety VDU screens)
- Ability to use soft controls and monitoring in coordination
- Necessity alarms on safety VDU to initiate operator action

were raised for safety VDU design (see Part 3 Section 4.2.5 and 5 of Reference 2).

To resolve these HEDs, MHI considered additional spatially dedicated, continuously visible (SDCV) displays to be added adjacent to the train dedicated safety VDUs.

2. Applicable Regulatory Standards and Guidelines

During the design of the safety VDU, following regulatory requirements and guidance regarding the safety VDU design are applied to the HED resolution.

NUREG-0800 “Standard Review Plan” 7.4 Safe Shutdown Systems

E. Safe shutdown - System conformance to the single-failure criterion on a system basis and operability from onsite and offsite electrical power as required by GDC 34, 35, and 38. Safe shutdown systems that are safety systems according to the definition of IEEE Std 603-1991 should fulfill the requirements of that standard.

NUREG-0800 BTP-18.1; “Guidance for Evaluating Minimum Inventory of Alarms, Controls, and Displays for New Light Water Reactor Plant Designs”, 4. Acceptance Criteria

c. validate that the as-built MCR and RSF minimum inventories support operator performance of those EOP actions and PRA critical operator actions necessary to bring the reactor to a safe shutdown condition and maintain it in a safe shutdown condition.

SRM-SECY-93-087; “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs,” Item II.T, Control Room Annunciator (Alarm) Reliability

the alarm system for ALWRs should meet the applicable EPRI requirements. as discussed above, for redundancy, independence. and separation. In addition, alarms that are provided for manually controlled actions for which no automatic control is provided and that are required for the safety systems to accomplish their safety functions. shall meet the applicable requirements for Class IE equipment and circuits.

DI&C-ISG-05 “Highly-Integrated Control Room-Human Factors Issues (HICR-HF)”, 3. Minimum Inventory

viii. the criteria that will be used to determine which human system interfaces need to be spatially dedicated, continuously visible, continuously available, or accessible by taking only one action.

NUREG-0700 “Human-System Interface Design Review Guidelines”, 4.2.1-4 Use of Spatially Dedicated, Continuously Visible Displays

Spatially dedicated, continuously visible (SDCV) alarm displays should be considered for:

- Regulatory Guide 1.97 Category 1 parameters,
- Alarms that require short-term response,
- The most important alarms used in diagnosing and responding to plant upsets, and
- The most important alarms used to maintain an overview of plant and system status.

Additional Information: Spatial dedication means that the alarm messages always appear in the same position. Continuously visible means a parallel presentation method is used, i.e., the alarm information is always available to the operator, as opposed to serial presentation methods in which the operator must select the information to be seen. A SDCV alarm display (such as is provided by conventional tiles) generally has been found during high-density alarm conditions to be superior to other forms of alarm presentation, such as message lists. SDCV displays provide perceptual advantages of rapid detection and enhanced pattern recognition.

3. Design Resolution

As is described in the Topical Report MUAP-07007 subsection 4.6, the operator console of the US-APWR provides four safety VDUs, which is included in train A to D, which have following functions;

- Monitoring of process value of post accident monitoring categorized to type A and B, and Class 1E component status
- Control of the Class 1E equipments

In order to resolve the HEDs described in Section 1, MHI is planning to add two more safety VDUs, each which is included in train A/D, but both of them have uni-directional serial data link interface with other trains of A to D. The added safety VDUs has ability to display following parameters in SDCV manner:

- Regulatory Guide 1.97 Category 1 parameters
  (IEEE-497 type A, B and C: DCD Chapter 7)
- Plant process indications that would lead operators to take action in SAR of the US-APWR DCD Chapter 15

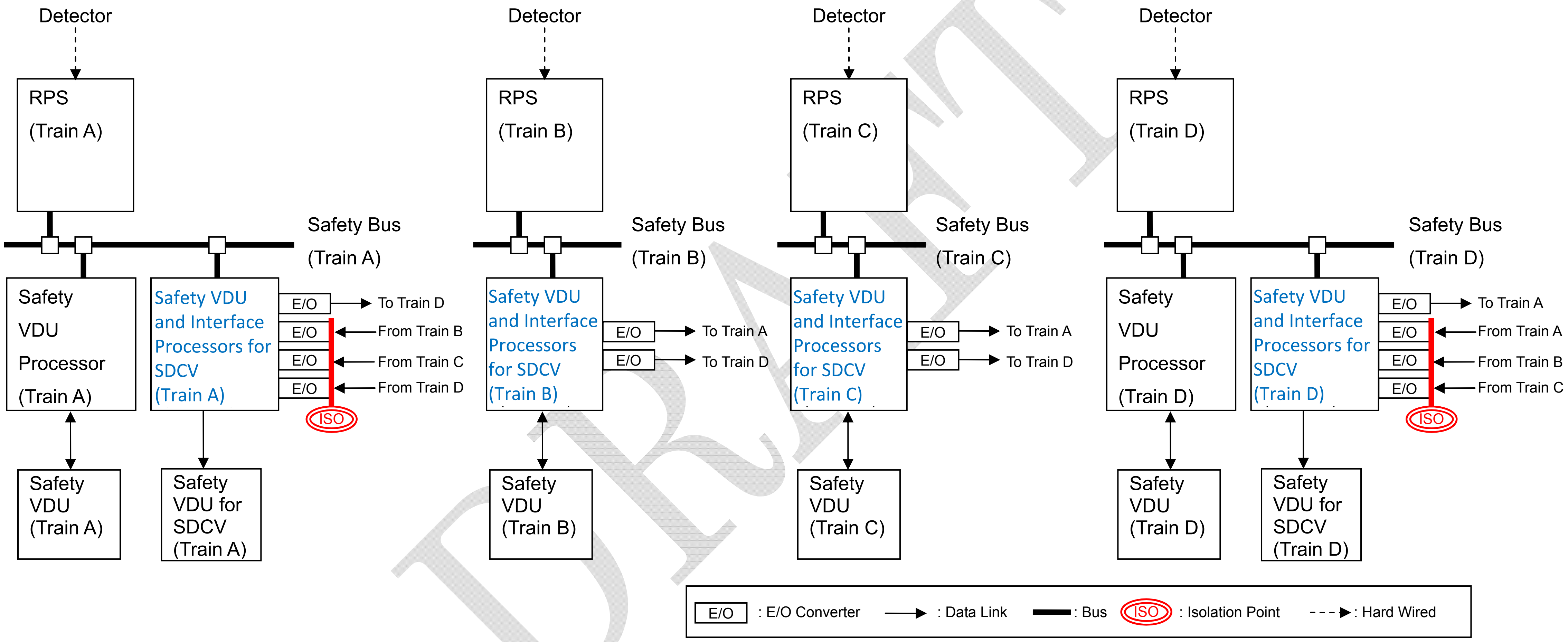
It is noted that the mentioned safety VDUs for SDCV display has no control functions, but has only monitoring function

Using of the safety VDUs SDCV is expected to resolve the HEDs by reducing of operator's task burden to request display screens, and providing continuous display and alerting function to take required actions.

The effect of the added multi train safety VDUs will be verified and validated in the integrated system verification and validation (V&V) test as described in the technical report MUAP-10012 "Verification and Validation Implementation Plan."

4. System description of the multi train Safety VDU

The figure below shows the system configuration of the safety VDUs.



5. References

1 HSI System Description and HFE Process, MUAP-07007-P (Proprietary) and MUAP-07007-NP (Non-Proprietary), Revision 3, October 2009.

2 HSI Design, MUAP-09019-P (Proprietary) and MUAP-09019-NP (Non-Proprietary), June 2009.

3 Verification and Validation Implementation Plan, MUAP-10012, April 2010.

4 Design Control Document for the US-APWR, Chapter 7, Instrumentation and Control System, MUAP-DC007, Section 7.5 "Safe Shutdown Systems," Section 7.5 "Information Systems Important to Safety"

Table F.2-2: Signal List and Functional Independence Design from PCMS to PSMS

Type	Signals	Functional Independence
Non-safety signal from PCMS to SLS via Unit Bus	▪ Closure signal of Steam Generator Blowdown Line and Blowdaown Sampling Line Isolation Valve from Radiation Monitor related signal. ▪ Closure signal of Letdown Orifice Isolation Valve from Pressurizer Water Level Control. ▪ Actuation signal of Class 1E Battery Room Exhaust Fan from Battery Room Exhaust Fan Outlet Airflow Control. ▪ Closure signal of CV Purge Exhaust Line Isolation Valve from CV Purge Exhaust Filtration Fan start ▪ Trip signal of RCP from Non-Class 1E AC Bus under voltage signal ▪ Start permissive signal of RCP from RCP monitor signal.	The priority logic within the application software of the SLS ensures that an automatic safety-related signal generated from within the PSMS has higher priority than any non-safety signals from the PCMS, and all safety-related components cab be actuated correctly at the AOO or PA conditions. Any spurious signals are bounded in the AOO initiating condition of the safety analysis.
	▪ Actuation signal of Pressurizer Back-up Heater from Pressurizer Pressure Control. ▪ Actuation signal of Pressurizer Back-up Heater from Pressurizer Water Level Control. ▪ Actuation signal of Main Steam Relief and Relief Block Valve from Main Steam Line Pressure Control. ▪ Closure signal of Excess Letdown Line and Letdown Line Isolation Valve from Pressurizer Water Level Control. ▪ Closure signal of VCT Outlet Isolation and CHP Suction Alternate Supply Valve from VCT Water Level Control	The priority logic within the application software of the SLS ensures that a manual safety-related signal generated from within the PSMS has higher priority than any non-safety signals from the PCMS, and all safety-related components can be actuated correctly at the safe shutdown operation. Any spurious signals do not cause the AOO.
Non-safety signal from PCMS to ESFAS via Unit Bus	▪ Actuation signal of Emergency Feedwater Pump from Main Feedwater Pump trip signal. ▪ Open permissive signal of Turbine Bypass Valve from Condenser Available signal ▪ Actuation signal of CV Purge Isolation Valve from Containment Radiation Monitor signal	The priority logic within the application software of the ESFAS ensures that an automatic safety-related signal generated from within the PSMS has higher priority than any non-safety signals from the PCMS, and all safety-related components can be actuated correctly at the AOO or PA conditions. Any spurious signals do not cause the AOO.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

03/28/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**NO.702-5518 REVISION 0**
SRP SECTION:	**07.06 – INTERLOCK SYSTEMS IMPORTANT TO SAFETY**
APPLICATION SECTION:	**07.06**
DATE OF RAI ISSUE:	**02/28/2011**

QUESTION NO. : 07-06-25

US-APWR, DCD Tier-2, Section 7.6, lists seven interlocks important to safety. It is not clear if there are non-safety related interlocks that are important to safety. MHI is requested to address in the DCD whether there are non-safety related interlocks that are important to safety. If there are, the staff requests MHI to identify and explain these interlocks to ensure their conformance to applicable regulations including their isolation from the safety systems and to assure that their malfunctions would not impact the safety function.

ANSWER:

SRP Section 7.6 states that “the interlock systems important to safety” are the interlock systems “that operate to reduce the probability of occurrence of specific events, or to maintain safety systems in a state that assures their availability in an accident”. These interlock systems and the interlocks identified in DCD Section 7.6are designed as safety-related.
There are no non-safety related interlocks important to safety.

Impact on DCD

The following sentence will be added to the end of Section 7.6 of DCD: “The interlocks described in this section are safety-related. There are no non-safety related interlocks important to safety.”

Impact on COLA

There is no impact on the COLA

Impact on PRA

There is no impact on the PRA

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

03/28/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**NO.702-5518 REVISION 0**
SRP SECTION:	**07.06 – INTERLOCK SYSTEMS IMPORTANT TO SAFETY**
APPLICATION SECTION:	**07.06**
DATE OF RAI ISSUE:	**02/28/2011**

QUESTION NO. : 07-06-26

US-APWR, DCD Tier-2, Section 7.6.1, states that “The PSMS provides the interlock systems important to safety for the plant, with the exception of electro-mechanical interlocks within the electrical distribution system” without providing further information on the electro-mechanical interlocks and why these interlocks are not included in Section 7.6 of the DCD. MHI is requested to provide information on the electro-mechanical interlocks (or a pointer to another document) and explain why these interlocks are excluded from Section 7.6 of the DCD. In addition, the exception of the electromechanical interlocks has been identified only once and conflicts with other statements in Section 7.6 of the DCD. For example, Section 7.6.2.5 states that “All interlocks important to safety are implemented in the PSMS”; Section 7.6.3 states that “All the interlocks important to safety provide protection for plant mechanical systems or protection to prevent plant accident conditions. All the interlocks are implemented by the PSMS.” MHI is requested to describe the DCD statements with regard to implementation of the interlocks important to safety in a consistent manner.

ANSWER:

"Electro-mechanical interlocks within the electrical distribution system" refers to the self-protection function (overload protection, overcurrent protection etc.) implemented in the electrical distribution equipment such as switchgear and motor control center units, including mechanical interlocks preventing parallel connection of tie line incoming circuit breakers.

Self-protection functions are necessary to prevent component failure including failure of safety-related components. However, the failure of an electro-mechanical interlock can be bounded by a single failure and therefore does not affect the plant safety functions. Therefore, the electro-mechanical interlocks within the electrical distribution system are not included in the scope of “interlock systems important to safety” described in DCD Section 7.6.

Mechanical interlocks preventing parallel connection of tie line incoming circuit breakers is implemented in the breakers and performs its function without the PSMS digital software. Therefore, these interlocks are also excluded from the discussion in DCD Section 7.6.

However, the description in DCD Section 7.6 is confusing as noted in the question from the NRC. Therefore, the description "with the exception of electro-mechanical interlocks within the electrical distribution system" will be deleted from DCD Section 7.6.1.

Interlock systems important to safety realized with digital controllers are implemented in the PSMS, because these interlocks are part of safety related systems as mentioned in response to the RAI 07.06-25. However, there are some mechanical interlocks important to safety such as the mechanical interlock preventing parallel connection of tie line incoming circuit breakers which is configured without the PSMS. For clarification, those descriptions “All interlocks important to…” will be corrected to be read “All digital software interlocks important to safety are implemented in the PSMS.”

Section 7.1.1.11 will be added as included in Attachment 1 to include the evaluation for all types of interlock systems. As a result, the following interlocks are added or deleted as interlock systems important to safety.

Additional Interlocks

- Automatic starting of standby ESWP upon a low pressure signal of discharge line of operating ESWP and automatic starting of standby CCWP upon a low pressure signal of CCW header pressure

These interlocks are categorized as interlock systems important to safety, although they are back up function during normal operation and are not credited to ensure safety function in the event.

Deleted Interlock

- Simultaneous-open block interlock with RHR discharge line containment isolation valve and CS header containment isolation valve

This interlock is an important interlock to prevent that the CS/RHR pump will be loaded beyond its capacity. However, it is not necessary in terms of plant safety function.

[Note]

Attachment 1 will be later. Draft was submitted on March 31st.

Impact on DCD

The description "with the exception of electro-mechanical interlocks within the electrical distribution system" will be deleted from DCD Section 7.6.1.

The description “All interlocks important to…” in Section 7.6.3 will be corrected to be read “All digital software interlocks important to safety are implemented in the PSMS.”

The section 7.6.1.2 will be revised as follows

7.6.1.2 CS/RHR Valve Open Block Interlock

Common CS/RHR pumps are shared between the CSS and RHRS. The CSS and RHRS will not be required at the same time. CSS will be required in the beginning of an AOO or PA to reduce the containment pressure, while the RHR will be employed in the later part of the event to remove decay heat.

~~· Simultaneous-open block interlock with RHR discharge line containment isolation valve and CS header containment isolation valve;~~

~~Valves are provided for CS/RHR pump discharge for each CS and RHR line. If CS and RHR lines are opened simultaneously, the CS/RHR pump will be loaded beyond its capacity. This could lead to a pump run-out condition, which would damage the CS/RHR pumps. To preclude opening both systems valves simultaneously an interlock is provided to block simultaneous opening of the RHR discharge line containment isolation valve and the CS header containment isolation valve. The interlock functions to prevent opening a valve that~~

~~is closed. This interlock prevents CS and RHR system from operating simultaneously to prevent a pump run-out situation. The interlocks for these valves are shown in Figures 7.6-2 and 7.6-3. For RHS-MOV-021A, B, C, D, the piping diagrams for these valves are shown in Figure 5.4.7-2 in Chapter 5, and for CSS-MOV-004A, B, C, D in Figure 6.2.2-1 of Chapter 6.~~

The following description will be added as section 7.6.1.8

7.6.1.8 Automatic Starting of Standby CCWP and ESWP Interlock

The ESWP operation, ESW header pressure signals, and component cooling water pump (CCWP) operation are interlocked to enable automatic start and stop functions of the ESWPs and CCWPs. A low ESW header pressure signal actuates the standby ESWP automatically, ensuring continuous heat removal and protecting RCP seal. In the same manner, a low CCW supply header pressure signal will automatically start the stadby CCWP and corresponding ESWP.

The signal path for these interlocks is from the local pressure transmitters to the RPS, and then SLS, which controls these pumps via switchgears.

Impact on COLA

There is no impact on the COLA

Impact on PRA

There is no impact on the PRA

This completes MHI’s responses to the NRC’s questions.

Appendix 1

7.1.1.11 Interlock Systems

For the US-APWR, interlock systems are summarized as follows:

- Interlock systems included in the reactor trip system
- Interlock systems included in the ESF actuation system
- Interlock systems important to safety
- Interlock systems not required for safety
- Interlock systems related to diverse actuation system

Specific interlocks are listed in Table 7.1-3 based on above category.

Interlock systems included in the reactor trip system includes P-3 to P-13 permissive interlocks. These interlocks provides the permissive condition of the operating bypasses as described in section 7.2 and are implemented in the PSMS.

Interlock systems included in the ESF actuation system includes P-4 and P-11 permissive interlocks, Interlocks to ensure performance of safety components powered by Class 1E GTG and block turbine bypass and cooldown valves interlock. These interlocks are implemented in the PSMS except mechanical interlock which is configured without digital controller. These interlocks are described in sections 7.3 and 8.3.

Interlock systems important to safety are provided to prevent accident conditions and to ensure the availability of safety functions and credited in the safety analysis in chapter 15 or identified as risk significant by the probabilistic risk assessment in chapter 19. These interlocks are implemented in the PSMS and described in section 7.6.

Interlock systems not required for safety are implemented in the PSMS or PCMS and described in section 7.7.

Interlock systems related to diverse actuation system includes DAS actuation block upon P-4, turbine emergency oil pressure or EFW pump actuation. These interlocks are implemented by hardwired logic in the diverse automatic actuation cabinet and described in section 7.8.

Table 7.1-3 Interlock Systems

Interlocks	DCD Sections
Interlock systems included in the reactor trip system	
P-6 Intermediate Range Neutron Flux Above or Below Setpoint	7.2.1.6
P-7 Turbine Inlet Pressure (P-13) or Power Range Neutron Flux (P-10) Above Setpoint or Turbine Inlet Pressure (P-13) and Power Range Neutron Flux (P-10) Below Setpoint	7.2.1.6
P-10 Pressurizer Pressure Above or Below Setpoint	7.2.1.6
Interlock systems included in the ESF actuation system	
P-4 Reactor Trip (RTB open) interlock	7.3.1.5
P-11 Pressurizer Pressure Above or Below Setpoint	7.3.1.5
Trip and prevention from reclosing of the incoming circuit breakers from the offsite power if the Class 1E GTGs are started automatically on the LOOP event.	8.3.1.1
Mechanical interlock preventing parallel connection of tie line circuit breakers	8.3.1.1
Opening of the Class 1E GTG breaker upon the ECCS actuation signal if the Class 1E GTG is operating in parallel with the offsite power source prior to LOCA	8.3.1.1
Block Turbine Bypass and Cooldown valves interlock	7.3.1.11
Interlock systems important to safety	
CS/RHR Pump Hot Leg Isolation Valve Open Permissive Interlock	7.6.1.1
Simultaneous-open Block Interlock with CS/RHR pump hot leg isolation valve and CS header containment isolation valve	7.6.1.2
Primary Makeup Water Line Isolation Interlock	7.6.1.3
Accumulator Discharge Valve Open Interlock	7.6.1.4
CCW Supply and Return Header Tie Line Isolation Interlock	7.6.1.5
RCP Thermal Barrier Heat Exchanger CCW Return Line Isolation Interlock	7.6.1.6
Low-pressure Letdown Line Isolation Interlock	7.6.1.7 (proposed)
a. Automatic Starting of Standby ESWP upon a Low-pressure Signal of Discharge Line of Operating ESWP b. Automatic Starting of Standby CCWP upon a Low-pressure	7.6.1.8 (proposed)

Table 7.1-3 Interlock Systems

Interlocks	DCD Sections
Signal of CCW Header Pressure	
Interlock systems not required for safety	
Over-power and Over-temperature Interlocks	7.7.1.1
Pressurizer Spray Interlock	7.7.1.1
Low Pressurizer Water Level Interlock	7.7.1.1
High Steam Generator Level Interlock	7.7.1.1
Turbine Bypass Interlock	7.7.1.1
Interlock systems related to diverse actuation system	
DAS P-4 Interlock	7.8.1.2
Turbine emergency oil pressure	7.8.1.2
EFW pump	7.8.1.2

7.1.1.1 Scope of Digital System

A unified architecture is applied to the design of integrated digital I&C systems of the US-APWR. The unified architecture provides a high quality and reliable platform for both the safety-related systems and non-safety systems, which simplifies communication between these systems. Maintenance resources are standardized for every system thereby reducing human error. An integrated digital technology is also used for VDU based operation.

Specification of the hardware modules, such as central processing units (CPUs) and I/O modules, used for each subsystem is basically the same throughout the I&C architecture, except for some specific application modules (e.g., rod position interface). This approach allows the total number of required spare parts to be minimized. The configuration of the basic software, POL, and MELTAC engineering tools for specification of the application software, is the same in all digital I&C subsystems using the MELTAC platform. Maintenance procedures and tools (i.e., MELTAC engineering tool) are standardized for all subsystems; therefore, the training effort for the maintenance staff and potential for human error are minimized.

The only digital system applied to safety-related applications is the MELTAC platform. If digital devices other than the MELTAC platform, such as embedded digital device/components, are applied to safety-related SSCs, the COL Applicant is to provide software lifecycle documentation in accordance with the US-APWR Software Program Manual (Reference 7.1-18) or in accordance with a previously approved software lifecycle program, and to perform diversity and defense-in-depth (D3) analysis.

7.1.5 Combined License Information

COL 7.1(1) If digital devices other than the MELTAC platform, such as embedded digital device/components, are applied to safety-related SSCs, the COL Applicant is to provide software lifecycle documentation in accordance with the US-APWR Software Program Manual (Reference 7.1-18) or in accordance with a previously approved software lifecycle program, and to perform diversity and defense-in-depth (D3) analysis.

4.4 PSMS Manual Testing and Calibration Features

Continuous platform and system level self-diagnostic features allow elimination of most manual surveillances required for Technical Specification compliance. Manual testing and manual calibration is only provided for functions with no self-diagnosis. Manual testing overlaps with self-diagnosis to ensure the integrity of the self-diagnosis. The coverage of self-diagnosis and manual testing is shown in Figure 4.4-4.

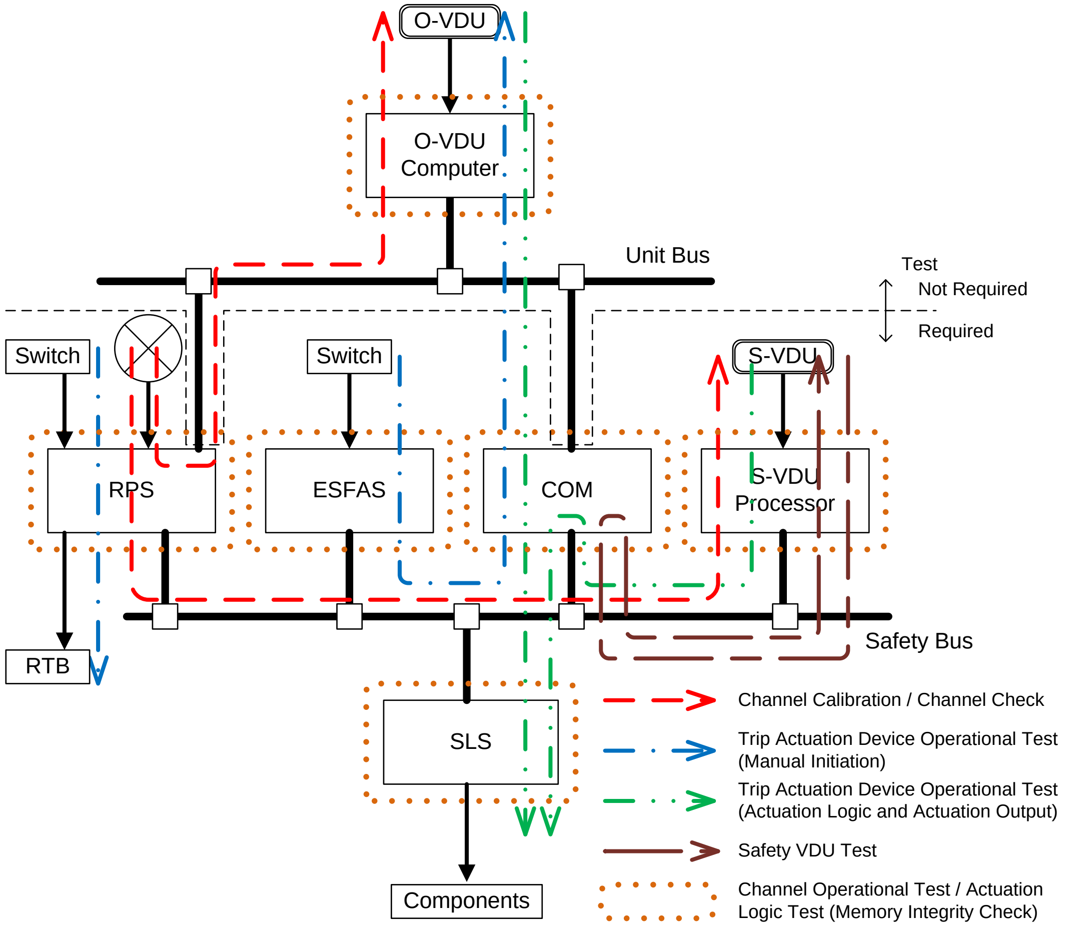

O-VDU
O-VDU Computer
Unit Bus
Test
Not Required
Required
Switch
Switch
S-VDU
RPS
ESFAS
COM
S-VDU Processor
Safety Bus
RTB
SLS
Components
Channel Calibration / Channel Check
Trip Actuation Device Operational Test (Manual Initiation)
Trip Actuation Device Operational Test (Actuation Logic and Actuation Output)
Safety VDU Test
Channel Operational Test / Actuation Logic Test (Memory Integrity Check)

Figure 4.4-4 Coverage of Self-diagnostics and Manual Testing