Safety I&C System Description and Design Process

Non-Proprietary Version

November 2013

Revision History

Revision	Date	Page (section)	Description
0	March 2007	All	Original issued
1	July 2007		The following items are revised based on NRC comments or erratum correction.
		xii	List of Acronyms "Design Certification Document" →"Design Control Document"
		5 (3.1)	Erratum correction (b) "Invokes IEEE Std. 603-1991" → "(h) Invokes IEEE Std. 603-1991"
		10 (3.3)	Conformance to RG 1.209 is added.
		17 (4.1)	Figure 4.1-1 is modified. ・ Erratum correction "operational procedure VDU" → "operating procedure VDU" ・ The figure is changed to colored Figures.
		21 (4.1)	(11)"Operation Procedures VDU Processor" →"Operating Procedure VDU Processor"
		22 (4.1)	Description of engineering tool is modified. ・ "portable personnel computer" →"personnel computer" ・ Description for administrative control of engineering tool connection is added.
		27 (4.1)	Description of the input route for DAS signal is added.
		31 (4.2.1)	Description of the sensor inputs signal to PSMS is added.
		34 (4.2.3)	Description of SLS I/O module is modified. ・ "power interface devices" → "Power interface (PIF) modules" ・ Description of PIF modules is added.
		44 (4.2.6)	Figure 4.2-2 is changed to colored Figures.

Revision	Date	Page (section)	Description
1 (continued)		49 (4.5)	Figure 4.4-1 is modified. ・ Erratum correction "Manual RT signal for …" ・ The figure is changed to colored Figures.
		50,51 (4.5)	Figure 4.4-2 and 4.4-3 are changed to colored Figures.
		54 (5.1.7)	Erratum correction in Figure 5.1-1 "conponent" → "component"
		60 (5.2.5)	Composition of Electrical Power is modified. ・ "non-safety AC" → "safety-rerated AC" ・ Description of non-safety AC transfer is deleted. ・ "Emergency Generators through qualified isolation devices" → "Alternate Power Source"
		61,62 (5.2.5)	Figure 5.2-1, 5.2-2 and 5.2-3 are modified. ・ Transformer is changed to Safety Class in Figure 5.2-1 and 5.2-2. ・ "Emergency Generator" is changed to "Alternate AC Power Source" in Figure 5.2-3. ・ "Safety Division" and "Example of UPS for Backup Power Source" is deleted in Figure 5.2-3.
		71 (6.4.1)	Description of Engineering Tools is modified.
		82 (7.0)	Description of document availability is added.
2	December 2008		The following items are revised based on RAI response (UAP-HF-08144), and erratum correction and clarification are implemented.
		xiv	List of Acronyms ・ Balance of Plant (BOP) is added ・ "Combined Licensing" →"Combined License"
		2, 3 (3.1)	Description of conformance to GDC 15 is added to follow the response (UAP-HF-08144) to RAI-01.

Revision	Date	Page (section)	Description
2 (continued)		6 (3.1)	Erratum correction "Commision's" → "Commission's"
		7 (3.3)	The title of RG 1.97 is corrected.
		10 (3.3)	Description of conformance to RG 1.204 is added to follow the response (UAP-HF-08144) to RAI-02.
		10 (3.3)	Description of conformance to RG 1.206 is added to follow the response (UAP-HF-08144) to RAI-03.
		11 (3.4)	Description of conformance to BTP 16 is deleted to follow the response (UAP-HF-08144) to RAI-03.
		16 (4.1)	Diverse Actuation System is added to (3) Non-safety I&C list for clarification.
		16 (4.1)	"Fully multiplexed including class 1E signals" is deleted from (4) Data communication list because this was doubly described.
		17 (4.1)	Figure 4.1-1 is replaced with the one in Revision 1 of US-APWR Design Control Document Chapter 7. In addition, the configuration of communication for Operating Procedure VDU is added to follow the response (UAP-HF-08144) to RAI-10, and the note for maintenance network is added for clarification.
		18 (4.1)	Figure 4.1-2 is replaced with the one in Revision 1 of US-APWR Design Control Document Chapter 7 to ensure figure resolution for NRC electronic submittal. (Contents are not changed.)
		19 (4.1)	Figure 4.1-3 is replaced with the one in Revision 1 of US-APWR Design Control Document Chapter 7.
		21 (4.1)	Description of communication for Operating Procedure VDU is added to follow the response (UAP-HF-08144) to RAI-10.

Revision	Date	Page (section)	Description
2 (continued)		26 (4.1)	C (8) "Turbine Control System" is replaced with "Balance of Plant Control System" in consistence with overall system architecture (Figure 4.1-1).
		33 (4.2.2)	Bypass and override function of ESF actuation is added in consistent with Revision 1 of US-APWR Design Control Document Chapter 7.
		42 (4.2.5)	Description of safety function performance is modified for clarification.
		67 (6.2.1)	Figure 6.2-1 is clarified to follow the response (UAP-HF-08144) to RAI-15.
		83, 84 (7.0)	Future Licensing submittal related to GDC 15, RG1.204, RG1.206 and ESF function (4.2.2) is added to Table 7-1.
		85 (8.0)	The title of MUAP-07007 Topical Report is corrected.
		116 (C.1)	Description of Malfunction and spurious actuations from Operational VDU is added to follow the response (UAP-HF-08144) to RAI-38.
3	September 2009		The following items are revised based on RAI response (UAP-HF-09261), and erratum correction and clarification are implemented.
		10 (3.3)	Description of conformance to RG 1.204. is revised to follow the response (UAP-HF-09261) to RAI-45.
		11 (3.4)	Description of conformance to BTP HICB-12 is added to follow the response (UAP-HF-09261) to RAI-71.
		16 (4.0)	Description of signal transmission is revised to follow the response (UAP-HF-09261) to RAI-46.
		25 (4.1)	Description of the discrepancies between the list of systems in the PCMS between Section 4.1.c and DCD Section 7.7 is added to follow the response (UAP-HF-09196) to RAI 07.07-18.
		27 (4.1)	Description of CCF of the sensors is added to follow the response (UAP-HF-09261) to RAI-50.

Revision	Date	Page (section)	Description
3 (continued)		33 (4.2.4)	Description of Manual switch configuration is added to follow the response (UAP-HF-09196) to RAI 07.03-15.
		36 (4.2.4)	Description of Manual switch configuration is added to follow the response (UAP-HF-09261) to RAI-47.
		40 (4.2.5)	Description of future modifications of the SPDS is deleted to follow the response (UAP-HF-09261) to RAI-51.
		42 (4.2.5)	Description of criteria for erroneous signal and blocking logic is added to follow the response (UAP-HF-09261) to RAI-54.
		42, 43 (4.2.5)	Description of qualification program is added to follow the response (UAP-HF-09261) to RAI-55.
		44 (4.2.6)	Description of test for DAS is added to follow the response (UAP-HF-09196) to RAI 07.08-2.
		44, 45 (4.2.7)	Section 4.2.7 for Digital Data Communication test is added to follow the response (UAP-HF-09261) to RAI-52.
		48 (4.2)	Figure of Two-Train ESF manual actuation added to follow the response (UAP-HF-09261) to RAI-47.
		49 (4.2)	Figure of Four-Train ESF manual actuation added to follow the response (UAP-HF-09261) to RAI-47.
		50 (4.2)	Figure of Overlap Testability for DAS is added to follow the response (UAP-HF-09196) to RAI 07.08-2.
		51 (4.3)	Reference to MUAP-07005 added to follow the response (UAP-HF-09261) to RAI-04 Supplement.
		52 (4.4.1)	Document number and section number of the Digital Platform Topical Report is added to follow the response (UAP-HF-09261) to RAI-56.
		53 (4.4.2)	Erratum correction "SLS" → "RPS"

Revision	Date	Page (section)	Description
3 (continued)		54 (4.4.3)	Description of response time is revised to follow the response (UAP-HF-09261) to RAI-57.
		55 (4.5)	Description of on-line maintenance of modules is revised to follow the response (UAP-HF-09261) to RAI-58.
		59 (5.1.3)	Description of Operational VDU failure detection is added to follow the response (UAP-HF-09261) to RAI-60.
		59 (5.1.3)	Description of reliability of Operational VDUs is added to follow the response (UAP-HF-09261) to RAI-07 Supplement.
		59 (5.1.4)	Description of functional diversity is revised to follow the response (UAP-HF-09261) to RAI-61 and added for clarification.
		62 (5.1.9)	Description of manual test and self-diagnosis is added to follow the response (UAP-HF-09261) to RAI-63.
		62 (5.1.10)	Description of Unrestricted Bypass of One Safety Instrument Channel with sensors shared by the PSMS and PCMS is added to follow the response (UAP-HF-09261) to RAI-64.
		63, 64 (5.1.13)	Section 5.1.13 for Priority Logic is added to follow the response (UAP-HF-09196) to RAI 07.03-9.
		66 (5.1)	Figure of VDU priority logic is added to follow the response (UAP-HF-09196) to RAI 07.03-9.
		67 (5.1)	Figure of manual and automatic priority logic is added to follow the response (UAP-HF-09196) to RAI 07.03-9.
		68 (5.1)	Figure of priority logic in PIF is added to follow the response (UAP-HF-09196) to RAI 07.03-9.
		69 (5.2.2)	Description of a margin for alarm setpoint is added to follow the response (UAP-HF-09261) to RAI-65.

Revision	Date	Page (section)	Description
3 (continued)		70 (5.2.4)	Reference for Environmental Specification is added to follow the response (UAP-HF-09261) to RAI-66.
		77 (6.3.1)	Description of Software Life Cycle Process Requirement is revised to follow the response (UAP-HF-09261) to RAI-67.
		78 (6.3.1)	Description of verification of Engineering Tools is added to follow the response (UAP-HF-09261) to RAI-77.
		82 (6.4.3)	Description of cyber security management is added to follow the response (UAP-HF-09261) to RAI-70.
		84 (6.5.2)	Description of MTBF is revised to follow the response (UAP-HF-09261) to RAI-78.
		86 (6.5.3)	Erratum correction "Variation of Process Value" on Figure 6.5-2 is deleted.
		86 (6.5.3)	Document number of the Digital Platform Topical Report is added.
		88 (6.5.4)	Description of setpoint methodology is added to follow the response (UAP-HF-09261) to RAI-71.
		102 (A.4.11)	Description of fail state is revised to follow the response (UAP-HF-09261) to RAI-04 Supplement.
		105 (A.5.6.3.2)	Description of separation criteria is revised to follow the response (UAP-HF-09261) to RAI-75.
		110, 111 (A.5.16)	Description of controller diversity is revised to follow the response (UAP-HF-09261) to RAI-76.
		125 (C.1)	Description of Software Quality Program is revised to follow the response (UAP-HF-09261) to RAI-55.
4	March 2010		The following items are revised based on NRC comments at the public meeting in February 2010 or editorial correction.

Revision	Date	Page (section)	Description
4 (continued)		general	Descriptions for Safety I&C Topical Report are modified. “in this Topical Report” → “in this Report”
		general	Descriptions referring Plant Licensing Documentation are deleted or modified to appropriate DCD Chapter or Technical/ Topical Report.
		general	Document numbers and/or document names are added to reference reports.
		xv (Abstract)	Description of the purpose of a revision is added.
		xvi (Abstract)	Description of Credit for leak detection in D3 analysis is deleted.
		1 (1.0)	Description of the purpose of a revision is added.
		5 (3.1(6))	Editorial correction Explanation of the common module is revised.
		10 (3.4(8))	Editorial correction Description of non-safety anticipatory trips is modified to be equivalent to DCD Chapter 7.
		11 (3.4(16))	Description of MRP is added.
		12 (3.5(4))	Description of Conformance to NUREG/CR-6421 is modified.
		17 (4.1)	Figure 4.1-1 is revised.
		22 (4.1 b(15))	Editorial correction Description of TSC computers is revised.
		22 (4.1 b(16))	Editorial correction Description of EOF is revised.
		27 (4.1 d)	Description of DAS components is rvised to follow the action item at the public meeting.
		33 (4.2.2)	Description of latching the ESFAS actuation signals is added to follow the action item at the public meeting.

Revision	Date	Page (section)	Description
4 (continued)		34 (4.2.3)	Editorial correction Description of a fail mode of a PIF module is added to follow the response (UAP-HF-10045) to RAI 516-4027.
		35 (4.2.3)	Editorial correction Description of Functional Assignment Analysis of SLS is added.
		36 (4.2.3)	Editorial correction ▪ "The SLS interlocks" → "The SLS receives interlocks from the RPS" "through the application software" →"through the component level application software"
		36 (4.2.4 b)	Following sentences are added to follow the action item at the public meeting. ▪ However, ...Class 1E criteria. ▪ For all design basis event, ... Class 1E criteria.
		38 (4.2.5 a)	Editorial correction ▪ "IEEE 603" → "IEEE 603-1991"
		41 (4.2.5 c)	Editorial correction ▪ "HSI" → "Class 1E credited HSI"
		41 (4.2.5 c)	Editorial correction Description of the write permission function of PSMS controllers is added.
		42 (4.2.5 c)	Editorial correction ▪ "component level" → "component level Lock function"
		42 (4.2.5 c)	Editorial correction Description of the priority between S-VDU and O-VDU is revised.
		43 (4.2.6)	Editorial correction ▪ "and processors" → ", processing logic and outputs"

Revision	Date	Page (section)	Description
4 (continued)		44 (4.2.6)	Editorial correction ▪ “or train level” → “, train or component level” ▪ “Spurious actuation... in the plant safety analysis. “→ deleted ▪ “disconnect and termination” → “disconnect terminations” ▪ “within the PIF module” → “within the 2-out-of-2 logic of the PIF module”
		51 (4.3)	Following sentence is added to follow the action item at the public meeting. ▪ “This automated cross-channel checking is credited to replace manual cross-channel checking in plant technical specification surveillances.”
		51 (4.4)	Following sentence is added to follow the action item at the public meeting. ▪ “Manual testing overlaps with self-diagnostics to ensure the integrity of the self-diagnostics.”
		51-54 (4.4.1)	Descriptions of equivalent tests in conventional plants are added.
		52 (4.4.1)	Description of Analog process Inputs is added.
		54 (4.4.1)	Description of the configuration of the RTS output interface for each reactor trip breaker is added.
		54 (4.4.2)	Editorial correction ▪ “an Operational VDU or Safety VDU” → “any VDU (eg. Operational VDU or Safety VDU)”
		55 (4.4.3)	Description of the failure impact of MELTAC components on system response time is added.
		55 (4.5)	Editorial correction ▪ “I/O modules” → “controller failures (including I/O modules)”
		59 (5.1)	Description of Credit for leak detection in Defense-in-Depth and Diversity analysis is deleted to follow the action item at the public meeting.

Revision	Date	Page (section)	Description
4 (continued)		60-61 (5.1.5)	Editorial correction ▪ “BTP HICB-19” → “BTP 7-19”
		61 (5.1.6)	Section 5.1.6 Credit for leak detection in Defense-in-Depth and Diversity analysis is deleted to follow the action item at the public meeting.
		62 (5.1.8)	Editorial correction Description of Appendix C and D is added.
		63 (5.1.9)	Editorial correction ▪ “The self-diagnostics discussed above” → “These manual surveillance tests, along with the self-diagnostics and software memory integrity tests discussed above,”
		63 (5.1.10)	Editorial correction ▪ “Technical Specifications” → “plant’s maintenance procedures”
		64-65 (5.1.13)	Descriptions of Priority logic are modified to follow the action item at the public meeting.
		67 (5.1)	Figure 5.1-3 is modified to follow the action item at the public meeting.
		68 (5.1)	Figure 5.1-4 is modified to follow the action item at the public meeting.
		69 (5.1)	Editorial correction Figure 5.1-5 is revised.
		70 (5.2.1)	Editorial correction ▪ “Seismic Category 1” → “Seismic Category I”
		71 (5.2.5)	Editorial correction Description of power sources for the PSMS is revised.
		74 (6.0)	Reference to the application software life cycle is added to follow the action item at the public meeting.
		77 (6.2)	Editorial correction ▪ “...described in this section” → “...summarized in this section”

Revision	Date	Page (section)	Description
4 (continued)		77 (6.2)	Editorial correction Following sentence is added. ▪ The details are described in MUAP-07017.
		78 (6.2.2 (4))	Editorial correction ▪ "...described in this section" → "...summarized in this section"
		78 (6.3)	Editorial correction Description of software life cycle requirements is modified.
		82 (6.4)	Editorial correction ▪ "...described in this section" → "...summarized in this section"
		82 (6.4)	Editorial correction Following sentence is added. ▪ The details are described in the US-APWR DCD Chapter 7 and MUAP-07017.
		83 (6.4.3)	Editorial correction ▪ "the cyber security requirements of NEI 04-04, or equivalent" → "the current NRC cyber security requirements"
		83 (6.4.3)	Editorial correction Followings items are deleted. ▪ It is noted that ... to all projects. ▪ In addition, ... cyber security program. ▪ For example, for the US-APWR ▪ In addition, ... resulting defensive model.
		84 (6.5.1)	Editorial correction Added the reference for Functional Assignment Analysis technical report.
		84 (6.5.1)	Editorial correction ▪ "Table 6.2-1" → "Table 6.5-1"
		87 (6.5.3)	Editorial correction References to the response time of safety I&C system are added.
		88 (6.5.4)	References are revised to follow the action item at the public meeting.

Revision	Date	Page (section)	Description
4 (continued)		90 (6.5.6)	Editorial correction Reference to seismic analysis is added.
		91 (6.5.7)	Editorial correction ▪ "...is based on RG 1.180" → "...complies with RG 1.180"
		92 (6.5.8)	Editorial correction Reference to fire protection and fire protection program is added.
		93 (6.5)	Editorial correction Figure 6.5-4 is revised.
		94 (7.0)	Chapter 7 FUTURE LICENCING SUBMITTALS is deleted due to revision as Technical Report.
		95 (8.0)	Editorial correction References are modified and updated.
		105 (A.5.5)	Editorial correction Description of failure modes of the trip mechanism of the reactor trip breakers and ESF components is added to be equivalent to DCD Chapter 7.
		106 (A.5.6.1)	Description of the justification for the single RCS flow instrument tap is added to follow the action item at the public meeting.
		107 (5.6.3.3)	Editorial correction ▪ "... the PCMS includes Signal Selection Algorism which prevents..." → "... the PCMS Signal Selection Algorithm prevents..." ▪
		108 (A.5.7)	Description of the Software Memory Integrity test is added to follow the action item at the public meeting.
		111 (A.5.11)	Description of identification of safety related documents is added to follow the action item at the public meeting.
		116 (A.6.3)	Editorial correction ▪ "PCMS basic platform software" → "PCMS Signal Selection Algorithm software"

Revision	Date	Page (section)	Description
		116 (A.6.3)	Editorial correction Description of Configuration Management is modified.
		119 (A.6.8.1)	Editorial correction ▪ "Nominal setpoint" → "Nominal trip setpoint"
		119 (A.6.8.1)	Descriptions of the allowable value and nominal trip setpoint are modified to follow the action item at the public meeting.
		120, 121 (A.7.3)	Description of the train level latching is revised to follow the action item at the public meeting.
		128 (C.1)	Description of Malfunction and spurious actuation is modified to follow the action item at the public meeting.
		130-158 (Appendix D)	Appendix D is added to follow the action item at the public meeting.
5	October 2010	12 (3.5)	Subsection 3.5 is added with addition of Appendix E to follow Closure Plan for US-APWR Instrumentation and Control Open Issues (UAP-HF-10237).
		12 (3.6)	Subsection number is renumbered.
		13 (3.7)	Subsection number is renumbered.
		15 (3.8)	Subsection number is renumbered.
		17 (Figure 4.1-1)	Revised the footnote to follow UAP-HF-10237.
		22 (4.1 a. (18))	Description of Engineering Tool is revised to follow UAP-HF-10237.
		30 (Figure 4.1-5)	The followings are revised. ▪ Configuration of communication sub-system is clarified. ▪ Connection from VDU processors to Consoles are corrected ▪ Number of groups of Safety Logic System is corrected.

Revision	Date	Page (section)	Description
5 (continued)		42 (4.2.5 c)	Description of capability to change MELTAC software for the item “No ability to alter safety software” is revised to follow UAP-HF-10237.
		43 (4.2.5 c)	Description of manual permissive is added to the item “Acceptable safety function performance” for further clarification.
		46 (4.2.7)	The bulleted item for Maintenance Network is added to follow UAP-HF-10237.
		53 (4.4.1)	Description of manual permissive is added to the item “Manual ESF Actuation” for further clarification.
		66 (5.1.13 (1))	Description of the priority logic between S-VDU and O-VDU commands is corrected.
		67 (5.1.13 (3))	Misdescription of permissive for the DHP is deleted.
		67 (5.1.13 (3))	Description of capability to change software is added.
		69 (Figure 5.1-3)	The followings are revised. ・ Priority logic between S-VDU and O-VDU commands ・ Manual permissive logic ・ Lock signal
		70 (Figure 5.1-4)	Lock logic is revised.
		82 (6.3.1 (11))	The item “Software Test Plan” is added to be consistent with BTP 7-14.
		84 (6.4.1)	Description of software change is added.
		84 (6.4.1)	Description of Maintenance Network is added.
		99 (A4.3)	Description of manual bypass permissive is added for further clarificatio.
		120 (A6.6)	Description of manual bypass permissive is added for further clarification.
		120 (A6.7)	Description of manual bypass permissive is added for further clarification.

Revision	Date	Page (section)	Description
5 (continued)		123 (A7.3)	Description of manual bypass permissive is added for further clarification.
		127 (B5.6 d)	Description of capability to change MELTAC software for the item "No ability to alter safety software" is revised to follow UAP-HF-10237.
		127 (B5.6 f)	The item is revised for clarification of priority logic.
		134 (D.1 a)	Clarification for the priority of ESFAS actuation signal is added to follow UAP-HF-10237.
		137 (D.3 a)	Description of the priority of ESFAS actuation signal is revised to follow UAP-HF-10237.
		137 (D.3 b)	Editorial Correction. Misdescription is corrected.
		140 (D.4 a)	Clarification for the priority of ESFAS actuation signal is added to follow UAP-HF-10237.
		140 (Table D.4-1)	Editorial Correction. Misdescription is corrected.
		142 (Table D.4-3)	Editorial Correction. Misdescription is corrected.
		143 (Table D.4-4)	Editorial Correction. Misdescription is corrected.
		144 (Table D.4-5)	Editorial Correction. Misdescription is corrected.
		147, 148 (Table D.4-6)	Effective on safety Function is revised to follow UAP-HF-10237.
		149 (Table D.4-7)	Editorial Correction. Misdescription is corrected.
		151 (Table D.4-8)	Editorial Correction. Misdescription is corrected.
		164 (Appendix E)	Appendix E is added to follow UAP-HF-10237.

Revision	Date	Page (section)	Description
6	April 2011	General	Editorial Correction Use of terminology and typical descriptions are revised or removed to make consistency and to clarify specific application for the US-APWR. (The action item at the public meeting)
		8 (3.3)	Description of the cyber security is deleted to follow the response to RAI 710-5495 Question 07-09-23.
		18 (4.1.1)	Figures 4.1-2 and 4.1-3, and related descriptions are deleted to clarify specific application for the US-APWR. (The action item at the public meeting)
		37 (4.2.5)	The title “Important to Safety Indication” is changed to “Information System Important to Safety”.
		41 (4.2.5)	The item “Additional protection against cyber threats” are deleted to follow the response to RAI 710-5493 Question 07.09-23.
		44 (4.2.7)	The sentence “The defensive … in Section 6.4.3” is deleted to follow the response to RAI 710-5493 Question 07.09-23.
		50-55 (4.3-4.4.2)	Descriptions are revised to follow the response to RAI 698-5490 Question 07.01-26.
		60 (Figure 4.4-4)	Figure 4.4-4 is added to follow the response to RAI 698-5490 Question 07.01-26.
		61 (5.1.1)	The item “Additional protection against cyber threats” is deleted to RAI 710-5493 Question 07.09-23.
		62 (5.1.3)	Description of justification for no periodic manual surveillance testing is added. (The action item at the public meeting.)
		65-66 (5.1.10)	Description of unlimited bypass is added. (The action item at the public meeting.)
		68 (5.1.13)	Editorial Correction Reference section is corrected to Section 4.1.

Revision	Date	Page (section)	Description
6 (continued)		70 (Figure 5.1-3)	Editorial Correction Figure 5.1-3 is revised to make consistency among the descriptions of priority logic. (The action item at the conference call.)
		73 (Figure 5.1-6)	Figure 5.1-6 is added to clarification of the description of manual permissive logic for bypass signals. (The action item at the conference call)
		76 (Figure 5.2-1)	Figure 5.2-1 is revised to be consistent with Figure 7.1- 4 of the DCD Chapter 7.
		77 (Figure 5.2-4)	Figure 5.2-4 is revised to be consistent with Figure 7.1- 7 of the DCD Chapter 7.
		78 (6.0-6.4)	Section 6.0 is revised and Sections 6.1 through 6.4 are deleted to specify the contents. These contents have been described in MUAP-07017.
		79-80 (6.5.1)	Section 6.5.1 is revised to follow the action item at the public meeting.
		84 (6.5.6)	“Plant structures … their safety functions.” is deleted.
		89 (8.0)	Reference 6 is deleted to follow the response to RAI 710-5493 Question 07.09-23 and references are updated.
		91 (A.4.4)	Typical descriptions and Tables A.4.4-1 and A.4.4-2 are deleted. (The action item at the public meeting.)
		93 (A.4.6)	Description of spatially dependent variables is revised. (The action item at the public meeting.)
		97-98 (A5.6.1)	Descriptions are revised for the clarification. (The action item at the public meeting.)
		98 (A.5.6.3.1)	Descriptions are revised for the clarification. (The action item at the public meeting.)
		103 (A.5.11)	Typical description is deleted.

Revision	Date	Page (section)	Description
6 (continued)		103 (A.5.12)	Description of SQAP, SVVP and SCMP is deleted. (The action item at the public meeting.)
		104 (A.5.16)	Table A.5.16-1 is deleted and description is revised to refer the DCD Chapter 7.
		104 (A.5.16)	Typical description is deleted.
		107 (A.6.3)	Description of SQAP, SVVP and SCMP is deleted. (The action item at the public meeting.)
		107 (A.6.6)	Typical description is deleted.
		112-113 (B.5.3)	References to Section 6 are changed to Software Program Manual. (The action item at the public meeting.)
		114 (B.5.6)	Item e is deleted to follow the response to RAI 710-5493 Question 07.09-23.
		116 (B.5.11)	Reference to Section 6 is changed to Software Program Manual. (The action item at the public meeting.)
		118 (C.1)	Description of “Malfunction and spurious actuations” is revised to follow the RAI 655-5074 Question 07.07-29.
		Appendix D	Appendix D is revised to follow the action item at the public meeting.
		Appendix E	Appendix E is revised to add the analysis for interdivisional communication from non-safety to safety-related systems. (The action item at the public meeting.)
		168-170 (E1)	Analysis for Staff Position 1.12 is revised to follow the response to RAI 701-5229 Question 07.09-22.
		Appendix F	Appendix F is added to describe safety-related digital I&C design detail conformance to essential safety criteria. (The action item at the public meeting.)

Revision	Date	Page (section)	Description
6 (continued)		Appendix G	Appendix G is added to describe the detailed FMEA for the PSMS. (The action item at the public meeting.)
		Appendix H	Appendix H is added to follow the amended response to RAI 568-4588 Question 07.05-18.
7	May 2011	General	Editorial Correction Use of terminology and typical descriptions are revised or removed to make consistency, to clarify specific application for the US-APWR and to eliminate duplications among DCD Chapter 7 and its supporting documents.
		20 (4.1 a (13))	Descriptions of multidivisional safety VDU are added to follow the action item at the public meeting.
		24 (4.1 b (4))	Descriptions of multidivisional safety VDU are added to follow the action item at the public meeting.
		36 (4.2.4)	Descriptions of multidivisional safety VDU are added to follow the action item at the public meeting.
		77 (6.5.1)	Descriptions of FMEA method are modified to follow the response to RAI 727-5662 Question 07.02-5.
		78 (6.5.1)	Table 6.5-1 and the item of “Fault Classification” in the section 6.5.1 are deleted to follow the response to RAI 727-5662 Question 07.02-7.
		93, 94 (A4.11)	Descriptions for fail safe design are modified to follow the response to RAI 727-5662 Question 07.02-5 and 07.02-6.
		117 (C.1)	Description for supplier control is added to follow the response to RAI 733-5650 Question 07.01-36.
		121, 122 (D.1 (2))	Automatic control commands from PCMS are reviewed and modified to follow the action item at the public meeting.
		133 (Table D.4-5)	Editorial Correction Misdescriptions are corrected.

Revision	Date	Page (section)	Description
7 (continued)		140 (D.4 (a) (ix))	Automatic control commands from PCMS are reviewed and modified to follow the action item at the public meeting.
		Appendix D	Editorial Correction Misdescriptions are corrected.
		Appendix E	Editorial Correction Misdescriptions are corrected.
		192 (Appendix F)	Descriptions of multidivisional safety VDU are added to follow the action item at the public meeting.
		204 (F.2)	Descriptions of multidivisional safety VDU are added to follow the action item at the public meeting.
		205, 208, 209 (F.2.2.3 (4))	Descriptions of multidivisional safety VDU are added to follow the action item at the public meeting.
		211, 212 (F.2.2.4 (3))	Descriptions of multidivisional safety VDU are added to follow the action item at the public meeting.
		220 (Figure F.2-8)	Added the figure to describe the communication independence design of safety VDU trains in order to follow the action item at the public meeting.
		222 (Table F.2-2)	Automatic control commands from PCMS are reviewed and modified to follow the action item at the public meeting.
		223, 224 (Appendix G)	Editorial Correction Misdescriptions are corrected.
		226 to 229 (Table G.2-1)	Editorial Correction Misdescriptions are corrected.
		235 to 238 (Table G.2-2)	Editorial Correction Misdescriptions are corrected.
8	November 2013	General	Editorial Correction
		General	Updated reference document to latest version.

Revision	Date	Page (section)	Description
8 (continued)		xxv-xxviii (List of Acronyms)	Revised to be consistent with the DCD.
		7, 82 (3.3-(4), 6.5.1)	Revised to follow the response to RAI 727-5662 Question 07.02-6.
		29 (Figure 4.1-5)	Revised to follow the response to Chapter 7 ACRS Subcommittee questions on April 25-26, 2013 Item 3.
		32, 71, 82, 95, 105, 110 (4.2.1, 5.1.10, 6.5.2, A.4.9, A.5.15, A.6.7)	Revised to follow the response to Chapter 7 ACRS Subcommittee questions on April 25-26, 2013 Item 14.
		36, 37, 84 (4.2.4 a, 4.2.4 c, 6.5.3, Figure 6.5-2)	Revised to follow the response (UAP-HF-11244) to additional questions from the NRC item No. 1, 4, 6-3 and 6-4.
		39 (4.2.5 b(2))	Revised to follow the response to RAI 771-5827 Question 07.01-42.
		41 (4.2.5 c)	Revised to follow the response to RAI 992-6999 Question 07.09-26 sub-question 1.
		42 (4.2.5 c)	Revised to follow the response to RAI 972-6900 Question 07.09-25.
		44, 51, 52, 77, 88 (4.2.6, 6.5.8, Figure 4.2-5, Figure 4.2-6, Figure 5.1-5, Figure 6.5-4)	Revised to follow the response to RAI 775-5836 Question 07.08-23 and 24.
		45, 46, 53 (4.2.7, Figure 4.2-7)	Revised to follow the response to Chapter 7 ACRS Subcommittee questions on April 25-26, 2013 Item 13.

Revision	Date	Page (section)	Description
8 (continued)		54, 55, 59 (4.3, 4.4, 4.4.1)	Revised to follow the response (UAP-HF-11314) to the additional questions from the NRC item No. 1-3, 1-4 and 1-7.
		54, 58 (4.3, 4.4.1)	Revised the description of memory integrity check (MIC) to be consistent with the DCD Chapter 16.
		58 (4.4.1)	Revised to follow the response to RAI 837-5945 Question 07.01-44.
		58, 59 (4.4.1)	Revised to follow the response (UAP-HF-11204) to Safety I&C RAI-22
		65 (Figure 4.4-4)	Revised the coverage of safety VDU test to be consistent with the description of Section 4.2.4 of MUAP-07005.
		69, 70 (5.1.8)	Revised to follow the response to RAI 996-7040 Question 07.07-33.
		123, 134, 149 (D.1, D.4)	Revised Sec D.1-(1)-a), D.1-(1)-b), D.1-(1)-c), D.4-a)-(iv), and D.4-c)-(ii) to be consistent with the DCD Tier 2 Chapter 7.
		159 to 224, 261 (Appendix E, Appendix F, Table G.2-2)	Revised to follow the response to RAI 778-5866 Question 07.09-24.
		205 (Figure F.1-5)	Revised to be consistent with Figure 4.1-15 of MUAP-07005.
		262 to 316 (Appendix H)	Revised to follow the response to RAI 568-4588 Question 07.05-18.
		317 to 322 (Appendix I)	Added Appendix I to follow the response to RAI 992-6999 Question 07.09-26 sub-question 1.
		323 to 344 (Appendix J)	Added Appendix J to follow the response to RAI 996-7040 Question 07.07-33.

Mitsubishi Heavy Industries, Ltd.
16-5, Konan 2-chome, Minato-ku
Tokyo 108-8215 Japan

Abstract

This Technical Report describes the Design of the MHI digital safety-related systems and the Design Process that will be used for the remaining work needed to apply these systems to specific nuclear power plants. MHI seeks NRC approval of this Design and Design Process for application to the safety-related systems of the US-APWR. The digital safety-related systems were developed by MHI for nuclear power plants in Japan. For applications in the US, this report demonstrates conformance of the Design and Design Process to all applicable US Codes and Standards. These include:

- Code of Federal Regulations
- Regulatory Guides
- Branch Technical Positions
- NUREG-Series Publications
- IEEE-Standards
- Other Industry Standards

MHI’s fully computerized instrumentation and control (I&C) system provides significant benefits to the safety of nuclear power, such as reduction of operations and maintenance work load, which reduces the potential for human error. Based on experience in Japan, MHI’s digital I&C systems improve the reliability and availability for plant operation.

To fully understand MHI’s safety-related systems, this report provides an overview of MHI’s overall I&C system, which includes both safety-related and non-safety systems. Non-safety systems are briefly described with emphasis on their interface to the safety-related systems. MHI’s overall I&C system is categorized into four echelons, these are Human-System Interface System (HSIS), Protection and Safety Monitoring System (PSMS), Plant Control and Monitoring System (PCMS), and Diverse Actuation System (DAS).

The non-safety PCMS provides automatic controls for normal operation. The safety-related PSMS provides automatic reactor trip and engineered safety features actuation. These same safety-related and non-safety functions may be manually initiated and monitored by operators using the HSI System, which includes both safety-related and non-safety sections. The HSI System is also used to manually initiate other safety-related and non-safety functions that do not require time critical actuation, including safety functions credited for safe shutdown of the reactor. After manual initiation from the HSI System, all safety functions are executed by the PSMS, and all non-safety functions are executed by the PCMS. The HSI System also provides all plant information to operators, including critical parameters required for post accident conditions.

The PCMS and PSMS utilize the Mitsubishi Electric Total Advanced Controller (MELTAC) platform which is described in a separate Technical Report. Maximum utilization of a common digital platform throughout a nuclear plant reduces maintenance, training, and changes due to obsolescence, thereby minimizing the potential for human error. The potential for common cause failure (CCF) in these systems is minimized due to the simplicity of their basic design, the maturity of the MELTAC platform and MHI’s design process (based on operation in Japan), the elevated quality programs applied to both systems, and the significant functional diversity within the numerous computers that compose these systems. Regardless of this very low potential for common cause failure, the DAS is provided to accommodate beyond design basis

common cause software failures that could adversely affect the PSMS and PCMS concurrent with operational occurrences and design basis accidents. The DAS provides diverse automation for time critical functions and diverse HSI to allow the operator to monitor critical safety functions and manually actuate safety-related process systems.

This report was originally issued as a Topical Report because MHI was originally seeking approval of this design and design process for the US-APWR and for digital upgrades in operating plants. However, in Revision 4, this report was changed from a Topical Report to a Technical Report applicable only to the US-APWR. The generic descriptions of the Topical Report were eliminated in this Technical Report.

MHI’s I&C systems take advantage of capabilities within digital technology that were not available for analog systems. Some of these design aspects may not be readily familiar to all NRC reviewers and there may be minimum NRC or industry guidance for their review. Therefore, this document puts special emphasis on the explanation of these aspects of the design and their conformance to codes and standards. The following are key examples of these areas:

a. Multi-channel operator stations
b. HSI to accommodate reduced operator staffing
c. Operation under degraded conditions
d. Integrated RPS/ESFAS with functional diversity
e. Common cause failure modes for Defense-in-Depth and Diversity (D3) analysis
f. Common output modules for PSMS/PCMS and DAS
g. Control system failure modes for safety analysis
h. Credit for self-diagnosis for technical specification surveillances
i. Unrestricted bypass of one safety-related instrument channel
j. Minimum inventory of HSI
k. Computer based procedures (CBPs)
l. Priority Logic

MHI specifically seeks NRC approval of the design aspects identified above. However, MHI understands that complete approval of items a, b, c, e, j and k will require additional consideration of Human Factors Engineering (HFE) and CCF which are described in the HSI Topical Report MUAP-07007 and the D3 Topical Report MUAP-07006, respectively. For these items, MHI seeks approval of only the I&C aspects described in this report.

Table of Contents

List of Tables

List of Figures

List of Acronyms

ac	alternating current
ALR	automatic load regulator
ALT	actuation logic test
ANSI	American National Standards Institute
AOO	anticipated operational occurrence
AOP	abnormal operating procedure
ARP	alarm response procedure
ATWS	anticipated transient without scram
AVR	auto voltage regulator
BISI	bypassed and inoperable status indication
BOP	balance of plant
BTP	branch technical position
CBP	computer based procedure
CCF	common cause failure
CCW	component cooling water
CDF	core damage frequency
CFS	condensate feedwater system
COL	Combined License
COM	communication system
COTS	commercial-off-the-shelf
CPU	central processing unit
CRC	Cyclic Redundancy Check
CRDM	control rod drive mechanism
CS	containment spray
C/V	containment vessel
CVCS	chemical and volume control system
D3	defense-in-depth and diversity
DAS	diverse actuation system
DBA	design nasis accident
dc	direct current
DCD	Design Control Document
DHP	diverse HSI panel
DI	digital input
DMC	date management console
DNB	departure from nucleate boiling
DNBR	departure from nucleate boiling ratio
DO	digital output
ECC	error check and correct
ECCS	emergency core cooling system
EFW	emergency feedwater
EHG	electro-hydraulic governor
EMC	electromagnetic compatibility

EMI	electromagnetic interference
EOF	emergency operations facility
EOP	emergency operating procedure
EPG	emergency procedure guideline
EPS	Emergency Power Supply system
ERDS	emergency response data system
ERG	emergency response guideline
ESF	engineered safety features
ESFAS	engineered safety features actuation system
FEM	finite element method
FET	field-effect transistor
FLB	feedwater line break
FMEA	failure modes and effects analyses
FPGA	field programmable gate array
FRG	functional restoration guideline
F-ROM	flash electrically erasable programmable read only memory
FTA	Fault Tree Analysis
GBD	graphical block diagram
GOMS	goals, operators, methods, and section rules
GSS	gland seal system
GTG	gas turbine generator
HDSR	historical data storage and retrieval
HFE	human factors engineering
HFP	hot full power
HSI	human-system interface
HSIS	human-system interface system
HVAC	heating, ventilation, and air conditioning
HZP	hot zero power
I&C	instrumentation and control
I/F	interface
I/O	input/output
ICIS	incore nuclear instrumentation system
IEC	International Electrotechnical Commission
IEEE	Institute of Electric and Electronic Engineers
IPL	interposing logic
ITAAC	inspections, tests, analyses, and acceptance criteria
IV&V	independent verification and validation
LBD	licensing basis documentation
LBLOCA	large break loss-of-coolant accident
LCO	limiting condition for operation
LDP	large display panel
LERF	large early release grequency
LOCA	loss-of-coolant accident
LOOP	loss of offsite power
LSSS	limiting safety system settings

M/G	motor generator
MCR	main control room
MELTAC	Mitsubishi Electric Total Advanced Controller
MFRV	main feedwater regulation valve
MFW	main feedwater
MHI	Mitsubishi Heavy Industries, Ltd.
MIC	memory integrity check
MSDV	main steam depressurization valve
MSIV	main steam isolation valve
MSLB	main steam line break
MSRV	main steam relief valve
MSS	main steam system
MTBF	mean time between failure
NIS	nuclear instrumentation system
NPSH	net positive suction head
NSSS	nuclear steam supply system
OBE	operational-basis earthquake
OC	operator console
OLM	on-line maintenance
O-VDU	operational VDU
PA	postulated accident
PAM	post accident monitoring
PCMS	plant control and monitoring system
PCT	peak cladding temperature
PIF	power interface
PLD	programmable logic device
PORV	power operated relief valve
POSIX	Portable Operating System Interface
PR	power range
PRA	probabilistic risk assessment
PRC	process recording computer
PSMS	protection and safety monitoring system
QA	quality assurance
QAP	quality assurance program
RCCA	rod cluster control assembly
RCS	reactor coolant system
RCPB	reactor coolant pressure boundary
RFI	radio frequency interference
RG	Regulatory Guide
RHR	residual heat removal
RMS	radiation monitoring system
RO	reactor operator
ROM	read only memory
RPI	rod position indication
RPS	reactor protection system

RSC	remote shutdown console
RSR	remote shutdown room
RT	reactor trip
RTA	Reactor Trip Actuation
RTB	reactor trip breaker
RTD	resistance temperature detector
RV	reactor vessel
RWS	refueling water system
RWSP	refueling water storage pit
SAR	Safety Analysis Report
SBO	station blackout
SDCV	spatially dedicated continuously visible
SDV	safety depressurization valve
SFP	spent fuel pit
SFPCS	spent fuel pit cooling and purification system
SG	steam generator
SGTR	steam generator tube rupture
SI	safety injection
SIS	safety injection system
SLB	steam line break
SLS	safety logic system
SPDS	safety parameter display system
SRSS	square root sum of squares
SSA	signal selection algorithm
SSC	structure, system, and component
SSE	safe-shutdown earthquake
S-VDU	safety VDU
SWC	surge withstand capability
TADOT	trip actuation device operational test
T_{avg}	average temperature
TBV	turbine bypass valve
T_{cold}	cold temperature
T_{hot}	hot temperature
TMI	Three Mile Island
TR	Topical Report
TSC	technical support center
UMC	unit management computer
UPS	uninterruptible power supply
UV	undervoltage
UV-ROM	ultra-violet erasable programmable read only memory
V&V	verification and validation
VCT	volume control tank
VDU	visual display unit

1.0 PURPOSE

The purpose of this Technical Report is to describe the Mitsubishi Heavy Industries, Ltd. (MHI) Safety-Related System and the Design Process used by MHI. MHI seeks approval from the US Nuclear Regulatory Commission for the use of the MHI Safety-Related System for the US-APWR.

This report was originally issued as a Topical Report because MHI was originally seeking approval of the safety-related system designs and design process for the US-APWR and for digital upgrades in operating plants. Therefore, this report contains generic design descriptions with the intent that these generic descriptions would be referenced and supplemented, as necessary, by Plant Specific Licensing documentation. However, this report was changed from a Topical Report to a Technical Report, only applicable to the US-APWR, at the fourth revision.

2.0 SCOPE

In this report the complete set of safety-related and non-safety systems is referred to as the Overall I&C System. The safety-related system described in this report is referred to as the Protection and Safety Monitoring System (PSMS).

The PSMS includes the Reactor Protection System, Engineering Safety Feature Actuation System, the Safety Logic system and the Safety-related Human-Systems Interface (HSI) System. MHI seeks approval for the PSMS including its interface to non-safety systems such as the Plant Control and Monitoring System (PCMS) and the Diverse Actuation System (DAS). These non-safety systems are described in this report only to the extent necessary to understand the PSMS interface.

The PSMS is built on the MELTAC platform which is described in a separate MELTAC Platform Technical Report, MUAP-07005. In addition, the MELTAC platform is applied to the Plant Control and Monitoring System. The MELTAC equipment applied for non-safety applications is the same design as the equipment for safety-related applications. However, there are differences in Quality Assurance (QA) methods for design and manufacturing.

3.0 APPLICABLE CODE, STANDARDS AND REGULATORY GUIDANCE

This section identifies compliance to applicable codes and standards and conformance with applicable NRC guidance, as appropriate. Unless specifically noted, the latest version issued on or prior to the date of this document is applicable. The following terminology is used in this section:

Equipment - This refers to the components that are the subject of this report. “Equipment” includes the safety-related digital I&C systems and the safety-related digital I&C platform. “Equipment” does not include the non-safety digital I&C or HSI systems or the non-safety digital I&C or HSI platforms.

3.1 Code of Federal Regulations

(1) 10 CFR 50 Appendix A: General Design Criteria (GDC) for Nuclear Power Plants

GDC 1: Quality Standards and Records
The Quality Assurance program meets the requirements of 10 CFR 50 Appendix B.

GDC 2: Design Bases for Protection against Natural Phenomena
This Equipment is seismically qualified. The Equipment is located within building structures that also provide protection against other natural phenomena. Specific buildings and Equipment locations are described in the US-APWR Design Control Document (DCD).

GDC 4: Environmental and Dynamic Effects Design Bases
This Equipment is located in a mild environment that is not adversely affected by plant accidents.

GDC 5: Sharing of Structures, Systems, and Components
There is no sharing of this Equipment among nuclear power units.

GDC 12: Suppression of Reactor Power Oscillations
Specific reactor trip functions implemented within this Equipment are described in the US-APWR DCD Chapter 7.

GDC 13: Instrumentation and Control
Specific instrumentation and control functions implemented within this Equipment are described in the US-APWR DCD Chapter 7.

GDC 15: Reactor Coolant System Design
Steady state and transient analyses are performed to assure that RCS design conditions are not exceeded during normal operation. Protection and control setpoints implemented within this Equipment are based on these analyses. Specific analysis and setpoints are described in the US-APWR DCD Chapter 15.

GDC 17: Electric Power Systems
The electric power sources for this Equipment and the plant components controlled by this Equipment are discussed in the US-APWR DCD Chapter 7 and Chapter 8. This document describes the interface requirements for these power sources.

GDC 19: Control Room
This Equipment provides the safety-related Human System Interfaces (HSI) for the control room. The non-safety digital I&C systems and the non-safety digital I&C platform provide non-safety HSI for the control room. The Human Factors design aspects of the HSI and the control room design are described in the HSI System Topical Report, MUAP-07007.

GDC 20: Protection System Functions
Specific protection system functions implemented within this Equipment are described in the US-APWR DCD Chapter 7.

GDC 21: Protection System Reliability and Testability
This Equipment includes automated testing with a high degree of coverage, and additional overlapping manual test features for the areas that are not covered by automated tests. Most manual tests may be conducted with the plant on line, and with the Equipment bypassed or out of service. Equipment that cannot be tested with the plant on line can be tested with the plant shutdown. Depending on the system design for a specific plant, the Equipment is configured with N or N+1 redundancy, where N is the number of trains needed for single failure compliance. For systems with N+1 redundancy this GDC is met with one train bypassed or out of service. The redundancy configuration for the US-APWR is N or N+1, depending on the function. The number of required trains for each function is defined in the US-APWR Technical Specifications.

GDC 22: Protection System Independence
Redundant trains are physically and electrically isolated to ensure that failures that originate in one train cannot propagate to other trains. All Equipment is qualified to ensure that the Equipment is unaffected by adverse conditions that may concurrently affect multiple trains. Interlocks between redundant trains and administrative controls ensure maintenance is performed on one train at a time.

GDC 23: Protection System Failure Modes
All detected failures are alarmed. The reactor trip functions are designed to fail to the actuated trip state on loss of power, on failures that are not automatically detected, or on failures that are automatically detected and would prevent proper execution of the trip function. The Engineered Safety Features functions are designed to fail to their safe state.

GDC 24: Separation of Protection and Control Systems
Redundant trains of the protection systems are physically and electrically isolated from the non-safety control systems. Where safety-related sensors are shared between control and protection systems, signal selection logic in the control system prevents erroneous control actions due to single sensor failures. Eliminating these erroneous control actions prevents challenges to the protection system while it is degraded due to the same sensor failure. Where non-safety signals control safety-related systems or components, logic in the safety-related systems ensures prioritization of safety functions.

GDC 25: Protection System Requirements for Reactivity Control Malfunctions
Specific functions implemented within this Equipment to protect against Reactivity

Control Malfunctions are described in the US-APWR DCD Chapter 15. Specific features designed into the MHI non-safety control systems to limit the extent of Reactivity Control Malfunctions are described in the US-APWR DCD Chapter 15.

GDC 29: Protection against Anticipated Operational Occurrences
The Equipment achieves a high probability of accomplishing its safety functions through components with conservative design margins, redundancy to accommodate random failures, and a quality program that minimizes the potential for design or manufacturing errors.

(2) 10 CFR 50.34 (f)(2) Post-TMI Requirements

- (iii) Control room
  The Human Factors design aspects of the HSI and the control room are described in the HSI System Topical Report, MUAP-07007.

- (iv) Safety Parameter Display
  The non-safety HSI systems provide safety parameter displays in the control room. Some data presented on safety parameter displays originates in this Equipment.

- (v) Bypassed and inoperable status indication
  This indication is provided by this Equipment and by the non-safety HSI system. All bypassed or inoperable signals for safety-related systems originate in this Equipment.

- (xi) Relief and safety-related valve position Indication
- (xii) Auxiliary feedwater system initiation and flow indication
- (xiii) Pressurizer heater control
- (xiv) Containment isolation systems
- (xvii) Accident monitoring instrumentation
- (xviii) Inadequate core cooling monitoring
- (xix) Instruments for monitoring plant conditions following core damage
- (xx) Pressurizer level indication and controls for pressurizer relief and block valves
  Specific functions implemented within this Equipment to meet the Post-Three Mile Island (TMI) requirements, items xi thru xx above, are described in the US-APWR DCD Chapter 7.

(3) 10 CFR 50.36 Technical specifications

- (1) Safety limits, limiting safety-related system settings, and limiting control settings.
  This Equipment is used to maintain safety-related limits. The MHI non-safety control systems are used to maintain control limits.

- (2) Limiting conditions for operation.
  This Equipment is configured with N or N+1 redundancy, as discussed above for compliance to GDC 21. For systems with N+1 redundancy there are no limiting conditions for operation (LCO) related to bypassed or out of service conditions for a single instrument channel.

- (3) Surveillance requirements
  This Equipment includes extensive automatic testing, as discussed above for compliance

to GDC 21. Provisions are included for periodic surveillance to confirm the operability of the automatic test features and to manually test features of the system that are not tested automatically. Most manual tests may be conducted with the plant on line. Functions that cannot be tested with the plant on line are tested during plant shutdown. The test interval for all manual tests is based on reliability and risk based analysis.

(4) 10 CFR 50.49 Environmental Qualification of Electric Equipment Important To Safety For Nuclear Power Plants

This Equipment is located in an environment that would at no time be significantly more severe than the environment that would occur during normal plant operation, including anticipated operational occurrences. Therefore, these criteria are not applicable although the criteria are applicable to certain instrumentation that interfaces to this Equipment. The qualification of this instrumentation is described in the US-APWR DCD Chapter 7.

(5) 10 CFR 50.55a

- (a)(1) Quality Standards for Systems Important to Safety

This Equipment was originally developed under a Japanese nuclear quality program that is equivalent to 10 CFR 50 Appendix B. Other licensing documents describe this equivalence. An approved 10 CFR 50 Appendix B quality program is now in effect for all Equipment.

- (h) Invokes IEEE Std 603-1991

See conformance to IEEE Std 603-1991

(6) 10 CFR 50.62 ATWS Rule

The Diverse Actuation System (DAS), which is used to actuate plant systems for anticipated transient without scram (ATWS) mitigation, is described briefly in this report and in more depth in the Topical Report for Defense in Depth and Diversity, MUAP-07006. The DAS is diverse from this Equipment, with the exception of the final module that interfaces to plant ESF components. This common module is part of the PSMS described in this report. The diversity between this Equipment and the DAS is described in the Topical Report for Defense in Depth and Diversity, MUAP-07006.

(7) 10 CFR 52.47

- (a)(1)(iv) Resolution of Unresolved and Generic Safety Issues
- (a)(1)(vi) ITAAC in Design Certification Applications
- (a)(1)(vii) Interface Requirements

Conformance to the requirements in items iv thru vii, above, are described in the US-APWR DCD and its references.

- (a)(2) Level of Detail

The content of this report, together with the additional information described in other digital system Topical Reports and the US-APWR DCD, is sufficient to allow the NRC staff to reach a final conclusion on all safety-related questions associated with the design. The information includes performance requirements and design information sufficiently detailed to permit the preparation of acceptance and inspection requirements by the NRC, and procurement specifications and construction and installation specifications by an applicant.

- (b)(2)(i) Innovative Means of Accomplishing Safety Functions

In the near term, the Equipment is expected to be applied to conventional I&C safety-related and non-safety functions typical of current operating plants and new evolutionary plants. In the longer term, the Equipment is expected to be applied to more innovative safety functions as may be typical of new passive plants. All specific plant safety functions are described in the US-APWR DCD Chapter 7.

(8) 10 CFR 52.79(c) ITAAC in Combined Operating License Applications
The inspections, tests, analyses, and acceptance criteria that demonstrate that this Equipment has been constructed and will operate in conformity with the Commission's final safety conclusion, will be described in the US-APWR DCD Tier 1.

3.2 Staff Requirements Memoranda

(1) SRM to SECY 93-087

・ II.Q Defense against Common Cause Failures in Digital I&C Systems
Compliance is described in the Topical Report on Defense-in-Depth and Diversity, MUAP-07006.

・ II.T Control Room Annunciator (Alarm) Reliability
Alarm signals are generated from this Equipment and from MHI non-safety I&C systems. Alarm annunciators are provided by the MHI non-safety HSI system, which is internally redundant. The overall integrated design conforms to separation and independence criteria between trains and between safety and non-safety trains.

3.3 NRC Regulatory Guides

(1) RG 1.22 Periodic Testing of Protection System Actuation Functions
See GDC 21 compliance. Protection actuation functions are completely testable through a combination overlapping automatic and manual tests. Manual tests can only be conducted when a train is bypassed. Trains are interlocked to prevent concurrent bypassing of redundant functions in more than one redundant train.

(2) RG 1.29 Revision 4 Seismic Design Classification
The Equipment is designated Seismic Category I. Specific portions of the Equipment whose continued function is not required are designated Seismic Category II. Seismic Category II Equipment is designed so that the Safe Shutdown Earthquake (SSE) will not cause a failure which will reduce the functionality of the safety function to an unacceptable level.

(3) RG 1.47 Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems
See compliance to 10 CFR 50.34 (f)(2)(v). Alarms are provided for all bypassed or inoperable safety functions; these alarms are provided on selectable displays. Spatially dedicated continuously visible alarm displays are provided for any bypassed or inoperable condition that prevents actuation of the safety function at the train level. The ability to manually actuate bypassed or inoperable alarms at the train level is provided for conditions that are not automatically detected.

(4) RG 1.53 Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems
-endorses IEEE Std 379-2000
See compliance to GDC 21 and 24. Safety functions are designed with N or N+1 trains.

Each train is independent from the other safety trains and from non-safety trains. Independence ensures that credible single failures cannot propagate between trains within the system and therefore can not prevent proper protective action at the system level. Single failures considered in the trains are described in the Failure Modes and Effects Analyses (FMEA) for each system. The FMEA method for the Equipment is provided in this report. The FMEA for safety-related I&C system of the US-APWR is discussed in Appendix G of this report.

(5) RG 1.62 Manual Initiation of Protective Actions
All RPS and ESFAS safety functions can be manually initiated at the system level by conventional switches located in the main control room. Manual initiation requires a minimum of Equipment and the Equipment common to manual and automatic initiation paths is kept to a minimum, by bypassing automated measurement channel bistable functions. No credible single failure in the manual, automatic or common portions will prevent initiation of a protective action by manual or automatic means.

(6) RG 1.75 Physical Independence of Electric Systems
-endorses IEEE Std 384-1992
Redundant safety trains are physically and electrically independent of each other and physically and electrically independent of any non-safety trains. Physical independence is maintained either by the required distance or by barriers which prevent propagation of fire or electrical faults. Electrical independence is maintained by fiber optic cable communication interfaces or conventional isolation modules, such as opto-couplers, relays or transformers. Conventional isolation modules include fault interrupting devices such as fuses or circuit breakers. Conventional isolation modules prevent propagation of transverse and common cause faults from the maximum credible energy source. Fiber optic cable communication interfaces, and specifications and qualification of conventional isolation modules are discussed in this report.

(7) RG 1.89 Qualification for Class 1E Equipment for Nuclear Power Plants
-endorses IEEE Std 323-1974
The environmental qualification of this Equipment is achieved through an appropriate combination of type testing and analysis. This Equipment is located in a mild environment that is not adversely effected by plant accidents. Therefore qualification for temperature, humidity, and radiation is by analysis of component specifications, room ambient conditions, and heat rise calculations for the installed configuration. Seismic qualification and electromagnetic interference (EMI) qualification are proven through type testing. This Equipment has no known aging mechanisms; random failures will be detected through periodic surveillance and testing.

(8) RG 1.97 Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants
-endorses IEEE Std 497-2002
This Equipment is used to process and display signals from accident monitoring instrumentation of all variable types. It meets all the applicable requirements. Signals from some accident monitoring instrumentation are also transmitted from this Equipment to the non-safety HSI system for displays and alarms. Independence is maintained between all trains. Specific accident monitoring instrumentation for the US-APWR is described in the US-APWR DCD Chapter 7.

(9) RG 1.100 Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants

This Equipment is designated Seismic Category I. It is designed and qualified to withstand the cumulative effects of a minimum of five (5) Operational Basis Earthquakes (OBEs) and one (1) Safe Shutdown Earthquake (SSE) without loss of safety function or physical integrity. The input spectrum is selected to envelope all anticipated applications. Conformance to this envelope for the US-APWR applications is discussed in the US-APWR DCD Chapter 7.

(10) RG 1.105 Setpoints for Safety-Related Instrumentation
-endorses ISA-S67.04-1994 and ANS-10.4-1987
The uncertainties associated with the Equipment are described in the MELTAC Platform Technical Report, MUAP-07005. This includes uncertainties for signal conditioning modules, signal splitters, instrument loop power suppliers and analog to digital converters. The uncertainties associated with specific process instrumentation and the resulting safety-related setpoints are demonstrated in MUAP-09022, US-APWR Instrument Setpoint Methodology. The methodology used to combine all uncertainties to establish safety-related setpoints is described in MUAP-09022 and briefly summarized in this report.

(11) RG 1.118 Periodic Testing of Electric Power and Protection Systems
-endorses IEEE Std 338-1987
See compliance to GDC 21, 10 CFR 50.36 and RG 1.22. All safety functions are tested either automatically or manually. Manual tests do not require any system reconfiguration, such as jumpers or fuse removal.

(12) RG 1.151 Instrument Sensing Lines
-endorses ISA-S67.02
Compliance is described in Section 7.1.3.7 of the US-APWR DCD Chapter 7.

(13) RG 1.152 Criteria for Programmable Digital Computers in Safety Systems of Nuclear Power Plants
-endorses IEEE Std 7-4.3.2-2003
The methods used for specifying, designing, verifying, validating and maintaining software for this Equipment complies with these requirements. The life cycle process for the digital platform software is described in the MELTAC Platform Technical Report, MUAP-07005. The life cycle process for the system application software is described in MUAP-07017.

(14) RG 1.153 1996 Criteria for Safety Systems
-endorses IEEE Std 603-1991
Compliance with the General Design Criterion identified in this Regulatory Guide is discussed above. Compliance with IEEE Std 603-1991 is discussed below.

(15) RG 1.168 Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
-endorses IEEE Std 1012-1998 and IEEE Std 1028-1997
This Equipment uses processes for verification, validation, reviews and audits that comply with this Regulatory Guide. The design processes for the digital platform are described in the MELTAC Platform Technical Report, MUAP-07005. The design processes for the digital safety-related systems are described in this MUAP-07017.

(16) RG 1.169 Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
-endorses IEEE Std 828-1990 and IEEE Std 1042-1987

This Equipment is designed and maintained using a Configuration Management process that complies with this Regulatory Guide. The Configuration Management process for the digital platform is described in the MELTAC Platform Technical Report, MUAP-07005. The Configuration Management process for the digital safety-related systems is described in MUAP-07017.

(17) RG 1.170 Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
-endorses IEEE Std 829-1983
The test documentation for this Equipment complies with this Regulatory Guide. The test documentation for the digital platform is described in the MELTAC Platform Technical Report, MUAP-07005. The test documentation for the digital safety-related systems is described in MUAP-07017.

(18) RG 1.171 Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
-endorses IEEE Std 1008-1987
Unit testing for this Equipment complies with this Regulatory Guide. This unit testing for the digital platform is described in the MELTAC Platform Technical Report, MUAP-07005. Unit testing for the digital safety-related systems is described in MUAP-07017.

(19) RG 1.172 Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
-endorses IEEE Std 830-1993
The Software Requirements Specifications for this Equipment comply with this Regulatory Guide. The Software Requirements Specifications for the digital platform are described in the MELTAC Platform Technical Report, MUAP-07005. The Software Requirements Specifications for the digital safety-related systems are described in MUAP-07017.

(20) RG 1.173 Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
-endorses IEEE Std 1074-1995
The Software Life Cycle Process for this Equipment complies with this Regulatory Guide. The Software Life Cycle Processes for the digital platform is described in the MELTAC Platform Technical Report, MUAP-07005. The Software Life Cycle Processes for the digital safety-related systems is described in MUAP-07017.

(21) RG 1.180 Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems
-endorses MIL-STD-461E, IEC 61000 Parts 3, 4, and 6, IEEE Std C62.41-1991, IEEE Std C62.45-1992, IEEE Std 1050-1996
This Equipment complies with the EMI/Radio Frequency Interference (RFI) requirements of this standard. Qualification testing for the digital platform is described in the MELTAC Platform Technical Report, MUAP-07005. Requirements and features of the digital safety-related systems that ensure compliance to the platform qualification envelope are described in this report.

(22) RG 1.209 Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants
-endorses IEEE Std 323-2003
This Equipment, which consists of safety-related computer-based I&C systems, is located

in a mild environment. There is no change in the environment due to plant accidents. This equipment is tested and analyzed to satisfy the mild environmental qualification requirements.

(23) RG 1.204 Guidelines for Lightning Protection of Nuclear Power Plants
The US-APWR DCD Chapter 8 describes conformance to RG 1.204 for the plant's electrical and grounding systems (e.g., Section 8 of the FSAR). In addition, the MELTAC digital platform complies with the electrical surge requirements defined by RG 1.180. In aggregate, this conformance provides suitable lightening protection.

(24) RG 1.206 Combined License Applications for Nuclear Power Plants
For the US-APWR the level of detail needed for the NRC staff to make a final safety determination is described in the DCD and COLA (Combined License Application). This document is intended to supplement the information provided in the DCD and COLA. This document may be referenced directly by the COLA or indirectly (via reference to the US-APWR DCD, which references this document).

3.4 NRC Branch Technical Positions

(1) BTP 7-1 Guidance on Isolation of Low-Pressure Systems from the High-Pressure Reactor Coolant System
(2) BTP 7-2 Guidance on Requirements of Motor-Operated Valves in the Emergency Core Cooling System Accumulator Lines
(3) BTP 7-3 Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps out of Service
(4) BTP 7-4 Guidance on Design Criteria for Auxiliary Feedwater Systems
(5) BTP 7-5 Guidance on Spurious Withdrawals of Single Control Rods in Pressurized Water Reactors
(6) BTP 7-6 Guidance on Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode
Compliance with BTP 7-1 thru 6, above, is described in the US-APWR DCD Table 7.1-2.

(7) BTP 7-8 Guidance for Application of Regulatory Guide 1.22
All functions of the protection system are testable at power.

(8) BTP 7-9 Guidance on Requirements for Reactor Protection System Anticipatory Trips
Reactor trip on turbine trip function is an anticipatory trip used in the protection system as described in DCD Chapter 7. For this non-safety trip the following requirements are met:

- All non-safety equipment is isolated from the safety-related system to prevent electrical fault propagation and adverse communication interaction.
- Safety functions have priority over all non-safety functions.
- Analysis demonstrates that credible non-safety signal failures do not result in plant conditions that are outside the boundary of the safety analysis.

(9) BTP 7-10 Guidance on Application of Regulatory Guide 1.97
The Equipment complies with this BTP for processing all instrumentation signals. However, RG 1.97 Revision 4 has superseded Revisions 2 and 3, for which this BTP was written. Therefore, where there are conflicts, the Equipment meets the requirements of RG 1.97 Revision 4.

(10) BTP 7-11 Guidance on Application and Qualifications of Isolation Devices
-endorses IEEE Std 472, ANSI Std C62.36, ANSI Std C62.41, ANSI Std C62.45
See compliance to RG 1.75. Isolation devices are qualified in compliance to these standards.

(11) BTP 7-12 Guidance on Establishing and Maintaining Instrument Setpoints
The Equipment complies with this BTP. See compliance to RG 1.105. Section 6.5.4 defines the methodology used to combine all uncertainties to establish limiting safety system settings (LSSS) and Allowable Values defined in the plant technical specifications.

(12) BTP 7-13 Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors
The methods used for periodically verifying the accuracy and response time of resistance temperature detectors (RTDs) complies with this standard. The method is described in the US-APWR DCD Chapter 7.

(13) BTP 7-14 Guidance on SW Reviews for Digital Computer Based I&C Systems
-endorses IEEE Std 730
The Equipment complies with this BTP. See compliance to RG 1.168 thru 1.173.

(14) BTP HICB-16 Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52
This guidance was withdrawn. See compliance to RG 1.206.

(15) BTP 7-17 Guidance on Self-Test and Surveillance Test Provisions
See compliance to GDC 21, 10 CFR 50.36, RG 1.22 and RG 1.118. Surveillance testing taken together with automatic self-testing provides a mechanism for detecting all failures.

(16) BTP 7-18 Guidance on Use of Programmable Logic Controllers in Digital Computer Based I&C Systems
This Equipment is not a commercial-grade computer system; the MELTAC life cycle activities, including production, and all application level life cycle activities are conducted under a 10 CFR 50 Appendix B Quality Assurance Program (QAP).

(17) BTP 7-19 Guidance on Evaluation of Defense in Depth and Diversity in Digital Computer Based I&C Systems
The MHI safety-related digital I&C systems utilize the MELTAC safety-related digital I&C platform. The MHI non-safety digital I&C systems utilize the MELTAC non-safety digital I&C platform. The two MELTAC platforms are essentially the same, however some QA aspects of design and manufacturing are not equivalent between safety-related and non-safety platforms. The Defense-in-Depth and Diversity Topical Report, MUAP-07006 describes the diversity within the safety-related and non-safety I&C systems. The report also describes the methodology for coping with a common cause failure of all of these systems and provides an example of this methodology for one Design Basis Accident (DBA). Coping for all DBAs is described in D3 Coping Analysis report, MUAP-07014.

(18) BTP 7-21 Guidance on Digital Computer Real Time Performance
The real-time performance for this Equipment complies with this BTP. The method for determining response time performance for the digital safety-related systems (including the digital platform) is described in this report. The response time performance for digital platform components is described in the MELTAC Platform Technical Report, MUAP-

07005. Requirements for system response time for conformance with the plant design basis and the response time of actual plant systems is described in the US-APWR DCD Chapter 7 and MUAP-09021.

3.5 NRC Interim Staff Guidance

(1) DI&C-ISG-04, Digital Instrumentation and Control
This Equipment conforms to all requirements of this guidance including key requirements for:

- Interdivisional Communication
- Command Prioritization
- Multidivisional Control and Display Stations

A detailed discussion of compliance to all aspects of ISG-04 is provided in Appendix E.

3.6 NUREG-Series Publications (NRC Reports)

(1) NUREG-0737, Supplement 1 Clarification of TMI Action Plan Requirements
This Equipment is used for compliance with the following TMI Action Plan Requirements:

- Plant Safety Parameter Display – This Equipment provides safety-related data to the MHI non-safety HSI system which provides this display for the control room and for emergency support facilities.
- Indication and Control for Safety Components (e.g., relief valves, pressurizer heaters, containment isolation valves), Inadequate Core Cooling Monitoring and Instrumentation for Accident Monitoring - This Equipment provides safety-related controls and monitors safety-related instruments to generate safety-related displays. Alarms and non-safety displays are generated by the MHI non-safety HSI system.

(2) NUREG-0800 Chapter 7 of the USNRC Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, Rev. 4
This Equipment fulfills all safety-related requirements of this NUREG for monitoring safety-related plant instrumentation and controlling safety-related plant components. Descriptions of specific plant systems are described in the US-APWR DCD Chapter 7.

(3) NUREG/CR-6303 Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems
The design of this Equipment is described in this report. The assessment of diversity within this Equipment and between this Equipment and other I&C systems is described in the Defense-in-Depth and Diversity Topical Report, MUAP-07006. The Defense-in-Depth and Diversity Topical Report also describes the method of coping with common cause failure vulnerabilities.

(4) NUREG/CR-6421 A Proposed Acceptance Process for Commercial-Off-the-Shelf (COTS) Software in Reactor Applications. See compliance to BTP 7-18.

3.7 IEEE Standards

(1) IEEE Std 7-4.3.2 2003 Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations

This Equipment conforms to all requirements of this standard, as augmented by RG 1.152, including key requirements for:

- Software quality and life cycle processes
- Independent Verification and Validation
- Communications independence

A detailed discussion of compliance to all aspects of IEEE Std 7-4.3.2 is provided in Appendix B.

(2) IEEE Std 323 2003 Qualifying Class 1E Equipment for Nuclear Power Generating Systems
This Equipment is qualified in compliance with this standard, as augmented by RG 1.89.

(3) IEEE Std 338 1987 Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems
This Equipment conforms to this standard, as augmented by RG 1.22.

(4) IEEE Std 344 2004 Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations
This Equipment conforms to this standard as augmented by RG 1.100.

(5) IEEE Std 379 2000 Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems
This Equipment conforms to this standard as augmented by RG 1.53.

(6) IEEE Std 383 2003 Type Test of Class 1E Electric Cables, Field Splices, and Connections for Nuclear Power Generating Stations
The cable and electrical connections used within this Equipment and between this Equipment conform to this standard, including requirements for flame retarding qualification requirements. Cables for interfaces to/from this equipment to other I&C systems and components are discussed in the US-APWR DCD Chapter 7.

(7) IEEE Std 384 1992 Criteria for Independence of Class 1E Equipment and Circuits
This Equipment conforms to this standard as augmented by RG 1.75. All safety functions are implemented within multiple trains with physical separation and electrical independence between redundant safety trains and between safety and non-safety trains. Electrical independence is accomplished primarily through the use of fiber optic technology. Independence of electrical circuits is accomplished with isolation modules and physical separation or barriers, such as conduits.

(8) IEEE Std 420 1982 Design and Qualification of Class 1E Control Board, Panels and Racks.
Standard enclosures for this Equipment conform to this standard. These enclosures are described in this report.

(9) IEEE Std 472 IEEE Guide for Surge Withstand Capability (SWC) Tests
As stated in BTP 7-11, this standard is currently intended for electrical protective relaying applications; it is not intended for digital systems. Therefore this Equipment complies with the surge withstand requirements of ANSI C62.41 and ANSI C62.45.

(10) IEEE Std 494 1974 Method for identification of Documents Related to 1E Equipment.
The documentation for this Equipment conforms to this standard by having the term

"Nuclear Safety Related" applied on the face of each document and drawing that is provided to the licensee. Generic documents and drawings used only for internal use by MHI do not contain this designation.

(11) IEEE Std 497 2002 Accident Monitoring Instrumentation for Nuclear Power Generating Stations
See compliance for RG 1.97.

(12) IEEE Std 603 1991 Safety Systems for Nuclear Power Generating Stations
1998 version is currently not endorsed by NRC
This Equipment conforms to this standard, as augmented by RG 1.153, including key requirements for:

- Single failures
- Completion of Protective Action
- Quality
- Qualification
- Independence
- Testability
- Monitoring and Information
- Bypasses

A detailed discussion of compliance to all aspects of IEEE Std 603 is provided in Appendix A.

(13) IEEE Std 730 1989 Software Quality Assurance Plans

(14) IEEE Std 828 1990 IEEE Standard for Software Configuration Management Plans

(15) IEEE Std 829 1983 Software Test Documentation

(16) IEEE Std 830 1993 IEEE Recommended Practice for Software Requirements Specifications

(17) IEEE Std 1008 1987 IEEE Standard for Software Unit Testing

(18) IEEE Std 1012 1998 IEEE Standard for Software Verification and Validation Plans (2004 not yet endorsed by NRC)

(19) IEEE Std 1016 1987 IEEE Recommended Practice for Software Design Descriptions

(20) IEEE Std 1028 1997 IEEE Standard for Software Reviews and Audits

(21) IEEE Std 1042 1987 IEEE Guide To Software Configuration Management

(22) IEEE Std 1074 1995 IEEE Standard for Developing Software Life Cycle Processes
1997 version not yet endorsed by NRC
The software design process and documentation for this Equipment conforms to the requirements of IEEE Std 730 thru 1074, above.

3.8 Other Industry Standards

(1) ANS-10.4 1987 Guidelines for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry
The computer programs used to develop setpoints for this Equipment conform to this standard, as endorsed by RG 1.105.

(2) ANSI C62.41 IEEE Recommended Practice on Surge Voltages in Low-Voltage AC Power Circuits
This Equipment complies with the sections of this standard endorsed by RG 1.180.

(3) ANSI C62.45 IEEE Guide on Surge Testing for Equipment Connected to Low-Voltage AC Power Circuits
This Equipment complies with the sections of this standard endorsed by RG 1.180.

(4) IEC 61000 Electromagnetic compatibility (EMC)
This Equipment complies with the following sections of this standard:

- IEC 61000-4-2: Testing and measurement techniques - Electrostatic discharge immunity tests. Basic EMC publication
- IEC 61000-4-4: Testing and measurement techniques - Electrical fast transient/burst immunity test. Basic EMC publication
- IEC 61000-4-5: Testing and measurement techniques - Surge immunity test
- IEC 61000-4-12: Testing and measurement techniques - Oscillatory waves immunity test.

(5) ISA-S67.04 1994 Setpoints for Nuclear Safety Related Instrumentation Used in Nuclear Power Plants
See compliance to RG 1.105. The methodology used to develop setpoints for this Equipment conforms to this standard, as endorsed by RG 1.105.

(6) MIL-STD-461E Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment
This Equipment complies with this standard as referenced in RG 1.180. This standard replaces MIL-STD-461D and MIL-STD-462D.

4.0 SYSTEM DESCRIPTION

Nuclear power plant instrumentation senses various plant parameters, and continuously transmits appropriate signals to the control systems during normal plant operation, and to the reactor trip and engineered-safety feature systems to detect abnormal and accident conditions.

The instrumentation and control (I&C) systems presented in this report provide protection against unsafe reactor operation during steady-state and transient power operation. The primary purpose of the I&C systems is to provide automatic initiating signals, automatic and manual control signals, and monitoring displays to mitigate the consequences of faulted conditions.

Descriptions are given in Section 4.1 for the Overall I&C System architecture, Section 4.2 for the more detailed system description of safety-related systems, Section 4.3 for the self-diagnostic features, Sections 4.4 and 4.5 for the testability features.

4.1 Overall I&C System Architecture

The MHI Overall I&C System is fully digital. It has been developed and applied in a step-by-step approach in Japanese PWR plants.
General specifications of the Overall I&C System are summarized below:

(1) Main control board

- Fully computerized
- Consists of safety Visual Display Units (VDU) and non-safety VDU panels
- Minimal conventional switch, only for regulatory compliance (e.g., RG 1.62)

(2) Safety I&C

- Fully digital
- Consists of MELTAC platform
- Four train redundant Reactor Protection System
- Four train redundant ESF actuation system
- Four train redundant Safety Logic System for component control
- Four train redundant Safety-Related HSI System

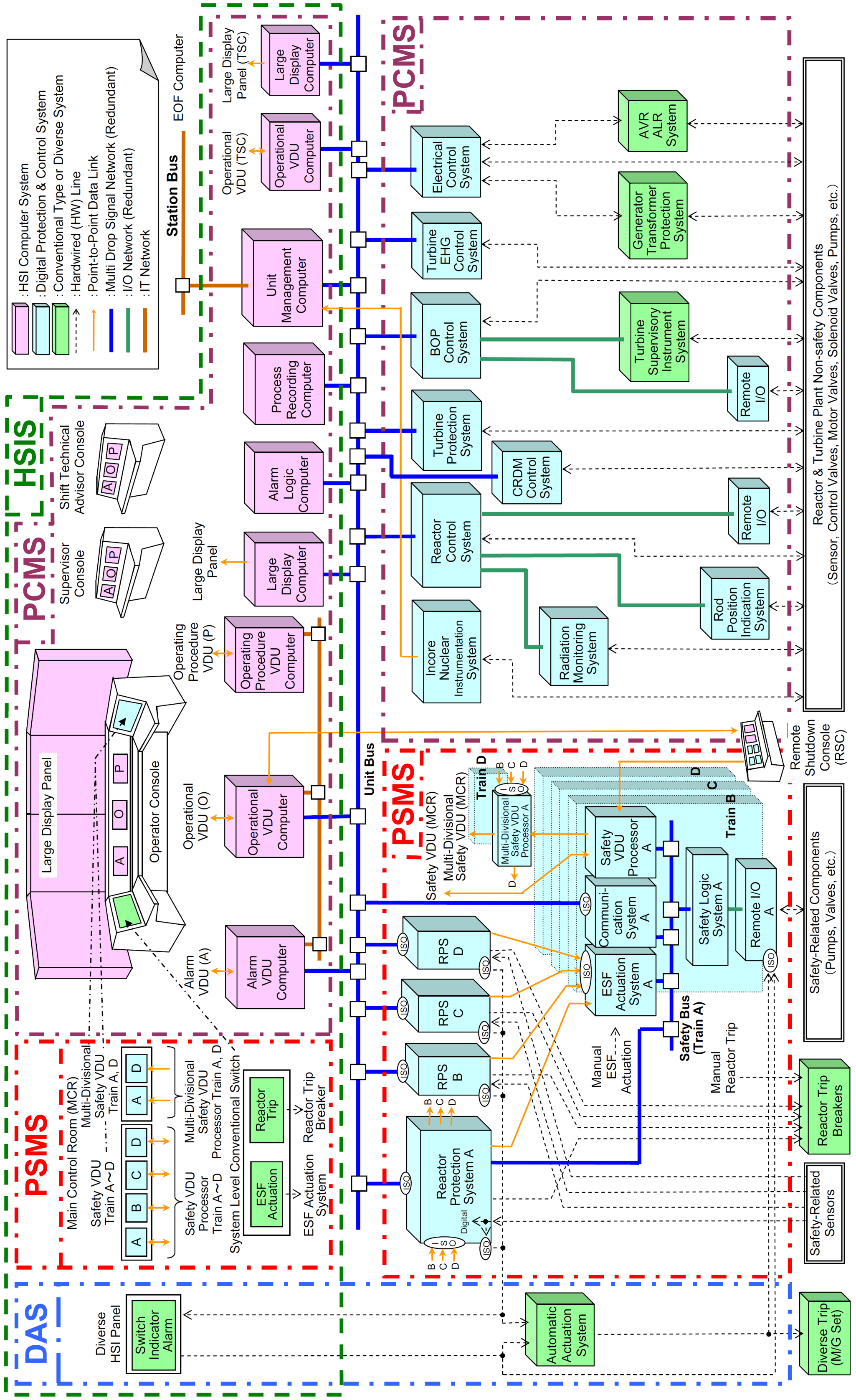
(3) Non-safety I&C

- Fully digital
- Consists of MELTAC platform
- Duplex redundant digital architecture for each control and process monitoring sub-system
- Diverse Actuation System

(4) Data communication

- Fully multiplexed including Class 1E signals
- Consists of multi-drop data bus and serial data link
- Uses fiber optics communication networks for noise immunity and isolation between redundant safety trains and between safety-related and non-safety systems

The architecture of the Overall I&C System is shown in Figure 4.1-1.


: HSI Computer System
: Digital Protection & Control System
: Conventional Type or Diverse System
: Hardwired (HW) Line
: Point-to-Point Data Link
: Multi Drop Signal Network (Redundant)
: I/O Network (Redundant)
: IT Network
EOF Computer
Station Bus
Large Display Panel (TSC)
Large Display Computer
Operational VDU (TSC)
Operational VDU Computer
Unit Management Computer
Process Recording Computer
Alarm Logic Computer
Large Display Panel
Large Display Computer
Operating Procedure VDU (P)
Operating Procedure VDU Computer
Operational VDU (O)
Operational VDU Computer
Alarm VDU (A)
Alarm VDU Computer
HSIS
PCMS
Shift Technical Advisor Console
Supervisor Console
A O P
Large Display Panel
Operator Console
A O P
PSMS
Main Control Room (MCR)
Safety VDU Train A~D
Multi-Divisional Safety VDU Train A, D
A B C D
A D
Safety VDU Processor Train A~D
Multi-Divisional Safety VDU Processor Train A, D
System Level Conventional Switch
ESF Actuation
Reactor Trip
ESF Actuation System
Reactor Trip Breaker
DAS
Diverse HSI Panel
Switch Indicator Alarm
Unit Bus
PCMS
Electrical Control System
Turbine EHG Control System
BOP Control System
Turbine Protection System
CRDM Control System
Reactor Control System
Incore Nuclear Instrumentation System
Radiation Monitoring System
Rod Position Indication System
Remote I/O
Remote I/O
Turbine Supervisory Instrument System
Generator Transformer Protection System
AVR ALR System
Reactor & Turbine Plant Non-safety Components (Sensor, Control Valves, Motor Valves, Solenoid Valves, Pumps, etc.)
Remote Shutdown Console (RSC)
PSMS
Safety VDU (MCR)
Multi-Divisional Safety VDU (MCR)
Train D
Multi-Divisional Safety VDU Processor A
B C D
D
Train B
C
D
Safety VDU Processor A
Communication System A
Safety Logic System A
Remote I/O A
ESF Actuation System A
Safety Bus (Train A)
ISO
RPS D
RPS C
RPS B
Reactor Protection System A
Digital
B C D
I S O
Manual ESF Actuation
Manual Reactor Trip
Safety-Related Components (Pumps, Valves, etc.)
Reactor Trip Breakers
Safety-Related Sensors
Automatic Actuation System
Diverse Trip (M/G Set)

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

Note: Each train of the PSMS has a Maintenance Network per division. The PSMS controllers are normally disconnected from the Maintenance Network.

Figure 4.1-1 The Overall Architecture of the I&C System

The Overall I&C System consists of the following four echelons as illustrated in Figure 4.1-1:

a. Human-System Interface (HSI) System
b. Protection and Safety Monitoring System (PSMS)
c. Plant Control and Monitoring System (PCMS)
d. Diverse Actuation System (DAS)

The following sections summarize the function of each I&C echelon in Figure 4.1-1.

a. Human-System Interface (HSI) System

This section provides an overview of the complete HSI System, which includes the HSI portions of the Protection and Safety Monitoring System, the Plant Control and Monitoring System, and the Diverse Actuation System. The hardware and software aspects of the HSI portion of the Protection and Safety Monitoring System are described in detail in this report. The Human Factors Engineering aspects and the detail functional design of the complete HSI System are also described in the HSI System Topical Report, MUAP-07007.

Figure 4.1-2 Deleted

Figure 4.1-3 Deleted

(1) Operator Console (OC)

Plant information and controls (i.e., for all safety and non-safety trains) are displayed and accessed on the non-safety operational VDU screens of the Operator Console. All operations from the Operator Console are available using touch screens or other pointing devices on the non-safety operational VDUs. Safety VDU panels on the Operator Console provide access to safety-related information and controls using touch screens. There are one or more safety VDU panels for each safety train.

- Conventional switches for system level actuation are also installed on the Operator Console.

In conformance with RG 1.62, the switches for the safety functions identified have hardwired signal paths that bypass as much computer based processing as is practical. This is discussed in more detail in subsequent sections.

For the US-APWR the Operator Console allows one Reactor Operator (RO) to control the plant under all normal and abnormal plant conditions, except conditions where the HSI System itself is degraded. The Operator Console will also accommodate continuous operation by two ROs. Operation by one or two ROs is at the discretion of the utility. Operation with one or two ROs and operation under degraded HSI conditions is discussed in the HSI System Topical Report, MUAP-07007.

(2) Large Display Panel (LDP)

The Large Display Panel includes sufficient Spatially Dedicated Continuously Visible (SDCV) indications and alarms, so that the total status of the plant can be easily accessed without requesting VDU screens on the Operator Console. Important information for normal operation and important information for emergency or accident conditions are displayed on the Large Display Panel. Easy and reliable comprehension for all operating crew members is achieved from the information on this panel by continuously displaying high level plant conditions.

The Large Display Panel also includes a variable display which is selectable by the operation crew members. The operation crew members can share this information to enhance crew interaction and coordination.

(3) Supervisor Console

The Supervisor Console is designed for use by the main control room supervisor (i.e., Senior Reactor Operator). The Supervisor Console has the same non-safety VDU screens with the same operational capability as on the Operator Console. However, normally the Supervisor Console has monitoring capability only. All operational displays are selectable from the VDUs with touch screens or other pointing devices.

(4) Shift Technical Advisor Console

The Shift Technical Advisor Console is for the safety engineer. It is located in the Main Control Room (MCR). The Shift Technical Advisor Console has the same non-safety VDU screens with the same operational capability as the Operator Console. However, normally the Shift Technical Advisor Console has monitoring capability only. All operational displays are selectable from VDUs with touch screens or other pointing devices.

(5) Diverse HSI Panel (DHP)

The Diverse HSI Panel consists of conventional back-up switches and indicators. The Diverse HSI Panel is used in the case of a common cause failure of the safety-related and non-safety digital I&C systems.

(6) Process Recording Computer (PRC)

The Process Recording Computer provides historical data storage and retrieval (HDSR) functions. The system records process trends and all binary transitions such as alarms, equipment state changes etc. Historical data from the Process Recording Computer is accessible in the MCR on the Data Management Console (DMC).

(7) Alarm Logic Processor

The Alarm Logic Processor receives alarm signals from the safety-related and non-safety I&C equipment. This processor classifies these alarms according to their priority and their acknowledgement status, and transmits alarm status information to the Alarm VDU Processor and Large Display Panel Processor.

(8) Unit Management Computer (UMC)

The Unit Management Computer performs plant performance calculations, including core monitoring and fuel management applications. It also compiles data to create daily operations reports. Calculation results and reports are accessible in the MCR on the Data Management Console (DMC).

(9) Operational VDU Processor

The operational VDU Processor manages information and graphic displays for the non-safety operational VDUs located on the Operator Console, Shift Technical Advisor Console Supervisor Console, and Remote Shutdown Console. It also receives operator commands such as screen navigation and software control from the operational VDUs.

(10) Alarm VDU Processor

The Alarm VDU Processor manages the displays for the Alarm VDUs located on the Operator Console, Shift Technical Advisor Console, and Supervisor Console. It also receives operator commands such as screen navigation and alarm acknowledgement from the Alarm VDUs.

(11) Operating Procedure VDU Processor

The Operating Procedure VDU Processor manages the displays for the Operating Procedure VDU located on the Operator Console, Shift Technical Advisor Console, and Supervisor Console. It also receives operator commands such as procedure navigation, from the Operating Procedure VDU and Alarm VDU. The Operating procedure VDU communicates with the operational VDU processors and the Alarm VDU processors.

(12) Large Display Processor

The Large Display Panel Processor manages the displays on the Large Display Panel.

(13) Safety VDU Processors

The safety VDU consists of the safety VDU panel and the safety VDU Processor. The safety VDU Processors manage the displays on the safety VDU panels located on the Operator Console and the Remote Shutdown Console. They also receive operator commands such as screen navigation and software control from the safety VDU panels. There are two types of the safety VDUs as described in Figure 4.1-1.

(a) Safety VDU
The safety VDU can control and monitor all safety functions of each train.

(b) Multidivisional Safety VDU
The multidivisional safety VDU can monitor critical safety functions for the safe shutdown of all four trains.

There are one or two safety VDU Processors for each safety train, each located in a separate fire area.

(14) Remote Shutdown Console (RSC)

The Remote Shutdown Console is used for achieving and maintaining safe shutdown conditions in the event that the MCR is not available for any situation, including fire which results in catastrophic damage to I&C equipment located in the MCR. For the US-APWR safe shutdown is defined as Cold Shutdown.

The Remote Shutdown Console has the same non-safety VDU screens with the same operation and alarm capability as on the Operator Console. The Remote Shutdown Console also provides safety VDU panels for each safety train with the same operational capability as on the Operator Console.

(15) Technical Support Center (TSC) Computers

The TSC includes computers to support operational VDUs and the Large Display Panel. The TSC computers provide plant data displays to assist in the analysis and diagnosis of abnormal plant conditions. The information available at the TSC provides the same information available in the MCR.

(16) Emergency Operations Facility (EOF) Computer

The EOF Computer provides plant data displays to assist in the diagnosis of abnormal plant conditions and to evaluate the potential or actual release of radioactive materials to the environment. The information available at the EOF is a subset of the same information available in the MCR. The station bus provides information to plant and corporate personnel and to the EOF and NRC (via emergency response data system (ERDS)).

(17) Data Management Console (DMC)

The DMC is a common terminal unit of the UMC and PRC. The DMC display shows calculation results and reports which were provided by the UMC and historical information stored from the PRC.

(18) MELTAC Engineering Tool

The MELTAC engineering tool is a personal computer. It is used for diagnosing module failures in the PSMS. It is also used for some periodic testing. PSMS controllers are normally disconnected from the Maintenance Network, which is the interface between the controllers and the MELTAC engineering tool.

The MELTAC engineering tool is also used to change application software in PSMS controllers. Application software contains all logic functions, setpoints, constants, and controller configuration data. To change the application software, a hardwired connection must be made to the central processing unit (CPU) module. To make this connection the controller must be de-energized and its CPU module must be removed from the controller chassis and placed in a dedicated re-programming chassis. The dedicated re-programming chassis can be connected to the Maintenance Network for connection to the MELTAC engineering tool, or the MELTAC engineering tool can be connected directly to the dedicated re-programming chassis.

When a PSMS controller(s) is connected to the Maintenance Network to allow diagnosis or testing from the MELTAC engineering tool, or is de-energized to allow CPU module removal for re-programming by the MELTAC engineering tool, appropriate administrative controls are adopted as follows:

- An alarm(s) is generated in the MCR for the controller(s) that is connected to the Maintenance Network or is de-energized.

- The controller(s) that is connected to the Maintenance Network or is de-energized is declared inoperable and the affected inoperable functions of that controller(s) are managed in accordance with plant Technical Specifications.

The use of the MELTAC engineering tool is described in various sections, below.

b. Protection and Safety Monitoring System (PSMS)

The PSMS is discussed in detail in subsequent sections. This section provides a brief overview.

The PSMS encompasses all safety-related I&C systems in the plant with the exception of some special instrumentation systems (e.g., neutron monitoring) and special purpose controllers (e.g., Class 1E gas turbine generator (GTG) engine controls). The PSMS interfaces with these other safety-related systems and components.

The following sections describe the major systems and components within the PSMS echelon:

(1) Reactor Protection System (RPS)

The Reactor Protection System has a configuration of four redundant trains, with each train located in a separate I&C equipment room. Each train receives process signals, including NIS (nuclear instrumentation system) and safety-related RMS (radiation monitoring system), from safety-related field sensors. These sensors are used for monitoring of critical safety functions, including post accident monitoring, for monitoring and control of plant safety-related systems and for reactor trip and ESF actuation. The logic functions within the RPS are limited to bi-stable calculations and voting for reactor trip and engineered safety features actuation.

Each train performs 2-out-of-4 voting logic for like sensor coincidence to actuate trip signals to the four trains of the Reactor Trip Breakers (RTBs) and actuate ESF signals to the four trains of the ESF actuation system. Each train also includes a hardwired manual switch on the Operator Console to directly actuate the Reactor Trip Breakers. This switch bypasses the RPS digital controller.

This is a microprocessor based digital system that achieves high reliability through segmentation of primary and back-up trip/actuation functions, redundant 4 trains, failed equipment bypass functions, and microprocessor self-diagnosis, including data communications.

The system also includes features to allow manual periodic testing of functions that are not automatically tested by the self-diagnosis, such as actuation of reactor trip breakers. Manual periodic tests can be conducted with the plant on-line and without jeopardy of spurious trips due to single failures during testing.

Figure 4.1-4 shows the configuration of the Reactor Protection System. Figure 4.1-5 shows the configuration of the ESFAS, safety logic system (SLS), and Safety-Related HSI System, which are described below.

(2) ESF Actuation System (ESFAS)

The ESF actuation system has four redundant trains, with each train located in a separate I&C equipment room.
Each ESFAS train receives the output of the ESF actuation signals from the all four trains of the Reactor Protection System. Each train receives manual train level actuation signals from corresponding train level switches on the Operator Console. There is/are one or two conventional switch(es), which contains two contacts interfacing two separate digital inputs for each train level ESF actuation, hardwired from the Operator Console to the ESFAS. Each ESF actuation system train performs 2-out-of-4 voting logic for like system level coincidence to automatically actuate train level ESF actuation signals for its respective train of the Safety Logic System. Each ESF actuation system train performs 2-out-of-2 voting logic for signals from the manual initiation switches on the Operator Console. The ESF actuation systems also provides automatic load sequencing for the Class 1E GTGs to accommodate the Loss of Offsite Power (LOOP) accident. Safety-related plant components are manually loaded on the non-safety Alternative Generator from the Safety Logic System for Station Blackout conditions.

This is a microprocessor based system that achieves high reliability through redundancy within each train and microprocessor self-diagnosis, including data communications. The system also includes features to allow manual periodic testing of functions that are not automatically tested by the self-diagnosis, such as manual system level actuation inputs. Manual periodic tests can be conducted with the plant on-line and without jeopardy of spurious system level actuation due to single failures during testing.

(3) Safety Logic System (SLS)

The Safety Logic System has one train for each plant process train. For the US-APWR there are four trains for some plant systems and two trains for others.

Each train of the Safety Logic System receives ESF train level actuation demand signals and LOOP load sequencing signals from its respective train of the ESFAS. The Safety Logic System also receives manual component level control signals from the Operator Console and Remote Shutdown Console (safety VDUs and operational VDUs), and manual component level control signals from the hardwired back-up switches on the Diverse HSI Panel. The SLS also receives process signals from the RPS for interlocks and controls of plant process systems. This system performs the component-level control logic for safety-related actuators (e.g., motor-operated valves, solenoid operated valves, switchgear etc.)

The SLS controllers for each train are located in separate I&C equipment rooms. The system has conventional input/output (I/O) portions and I/O portions with priority logic to accommodate signals from the Diverse Actuation System (which is discussed below). To minimize field cabling, the I/O for each train in the US-APWR is remotely distributed throughout the plant in close proximity to safety-related actuators.

This is a microprocessor based system that achieves high reliability through redundancy within each train and microprocessor self-diagnosis, including data communications. The system also includes features to allow periodic testing of functions that are not automatically tested by the self-diagnosis, such as final actuation of safety-related components. Manual periodic tests can be conducted with the plant on-line and without jeopardy of spurious component actuation due to single failures during testing.

(4) Safety-Related HSI System

The Safety-Related HSI system consists of conventional hardwired switches for manual initiation of reactor trip and ESF initiation signals, safety VDUs and multidivisional safety VDUs which provide Post Accident Monitoring indications and manual controls and status indications for all components in the safety-related process systems.

Each train of the Safety-Related HSI System except the multidivisional safety VDU interfaces with the corresponding trains of all other systems within the PSMS. The multidivisional safety VDUs interface with all four train safety VDUs. There are Safety-Related HSI components for each train located on the Operator Console and the Remote Shutdown Console. The safety VDU Panels, the multidivisional safety VDU Panels and switches for each train are isolated from each other. The safety VDU Panels, the multidivisional safety VDU Panels and switches at the Operators Console and the Remote Shutdown Console are also isolated from each other and from the controllers in the PSMS to ensure that HSI failures that may result from a fire in one location cannot adversely affect the HSI in the alternate location.

(5) Reactor Trip Breakers (RTBs)

When a measurement exceeds the setpoint, the RPS initiates signals to open the Reactor Trip Breakers. This action removes power to the control rod drive mechanism coils permitting the rods to fall by gravity into the core. This rapid negative reactivity insertion will cause the reactor to shutdown.

Figure 4.1-6 illustrates the configuration of the reactor trip breakers. The breakers are located in 2 separated rooms.

c. Plant Control and Monitoring System (PCMS)

The PCMS encompasses all non-safety I&C systems in the plant with the exception of special purpose controllers (e.g., Alternate Generator engine controls). The PCMS interfaces with these other non-safety systems and components so there is only one fully integrated HSI system in the MCR.

The following sections describe the major systems within the PCMS echelon.

(1) Reactor Control System

The Reactor Control System receives non-safety field sensor signals. This system also receives status signals from plant process components and manual operation signals from the Operator Console to control and monitor the nuclear steam supply system (NSSS) process components. This system controls continuous control components, such as modulating air operated valves, and discrete state components such as motor-operated valves, solenoid-operated valves, pumps, etc.

This is a microprocessor based system that achieves high reliability through segmentation of process system groups (e.g., pressurizer pressure control, feedwater control, rod control etc.), redundancy within each segment, and microprocessor self-diagnosis, including data communications.

(2) Radiation Monitoring System (RMS)

The Radiation Monitoring System is a microprocessor based system that monitors plant process radio-activity and area radiation level.

(3) Rod Position Indication System

The Rod Position Indication System is a microprocessor based system that monitors control rod position. It detects dropped rods and misalignment of control rods. The system consists of processing equipment located in the I&C equipment room. For the US-APWR remote I/O is located inside the containment vessel (C/V).

(4) Control Rod Drive Mechanism (CRDM) Control System

The CRDM Control System is a microprocessor based system that receives control rod direction and speed demand signals from the Reactor Control System and manual operation signals from the Operator Console. This system outputs signals to control the electro-magnetic coil sequencing within the CRDMs.

(5) In-Core Neutron Instrumentation System

The In-core Neutron Instrumentation System is a microprocessor based system that provides remote data acquisition for in-core detector signal monitoring.

The In-core Neutron Instrumentation is top-mounted. In-core detectors are inserted into the core through detector guide thimbles which lead to the fuel assemblies and cover the effective axial fuel length. The In-core detectors are horizontally distributed over the entire core at approximately 40 locations. The In-core detectors provide signals for the measurement of core power distribution.

(6) Turbine Protection System

The Turbine Protection System receives signals regarding the turbine-generator and provides appropriate trip actions when it detects undesirable operating conditions of the turbine-generator.

This is a microprocessor based system that achieves high reliability through redundancy within the system and microprocessor self-diagnosis.

(7) Turbine EHG (Electro-Hydraulic Governor) Control System

The Turbine EHG Control System consists of redundant microprocessors and several hardwired logic parts (servo controller, etc.). The system has a speed control unit, a load control unit, an over-speed protection unit and an automatic turbine control unit. This system is used, either for control or for supervisory purposes.
This is a microprocessor based system that achieves high reliability through redundancy and microprocessor self-diagnosis.

(8) Balance of Plant Control System

The Balance of Plant (BOP) control system controls BOP systems such as service water, circulating water, feedwater, turbine control, HVAC, and non-essential component cooling water. The system receives inputs from field process instrumentation and manual operation signals from the Operator Console to control and monitor modulating control valves, and discrete components such as motor operated valves, solenoid operated valves, and pumps.

This is a microprocessor based system that achieves high reliability through segmentation of process systems groups, redundancy within each segment, and microprocessor self-diagnosis, including data communications.

(9) Turbine Supervisory Instrument System

The Turbine Supervisory Instrument system monitors important parameters of the turbine such as vibration, rotor position, etc.

(10) Electrical Control System

The Electrical Control System controls and monitors the electrical system and components.

This is a microprocessor based system that achieves high reliability through redundancy within the system and microprocessor self-diagnosis.

(11) Generator Transformer Protection System

The Generator Transformer Protection System provides a generator trip in case of receiving a turbine trip signal. This system also controls related components (breaker) in case of undesirable operating conditions of the generator and transformer.

(12) Auto Voltage Regulator (AVR)/Automatic Load Regulator (ALR) System

The AVR/ALR System provides regulation of generator voltage.

d. Diverse Actuation System

For coping with common cause failures (CCFs) in the software of the PSMS and PCMS, the Diverse Actuation System (DAS) provides monitoring of key safety-related parameters and back-up automatic/manual initiation of the safety-related and non-safety components required to mitigate anticipated operational occurrences and accidents.

The DAS consists of hardwired analog and binary components which are diverse from the MELTAC platform which is used in the PSMS and PCMS, so that a postulated CCF in these digital systems will not impair the DAS function.

The DAS is classified as a non-safety system. The DAS shares sensor inputs with the PSMS through analog interfaces that are not subject to the postulated CCF in the PSMS. The shared sensors are analog devices, therefore software CCF of the sensors does not need to be considered. Interfaces to safety process inputs and the Safety Logic System outputs are isolated within the safety-related systems through qualified conventional isolation modules.

The DAS provides manual system level actuation controls for critical safety functions. Where the time is insufficient for manual operator action, the DAS provides automatic actuation of the plant safety functions needed for accident mitigation.

The DAS is fully described in the Defense-in-Depth and Diversity Topical Report, MUAP-07006.

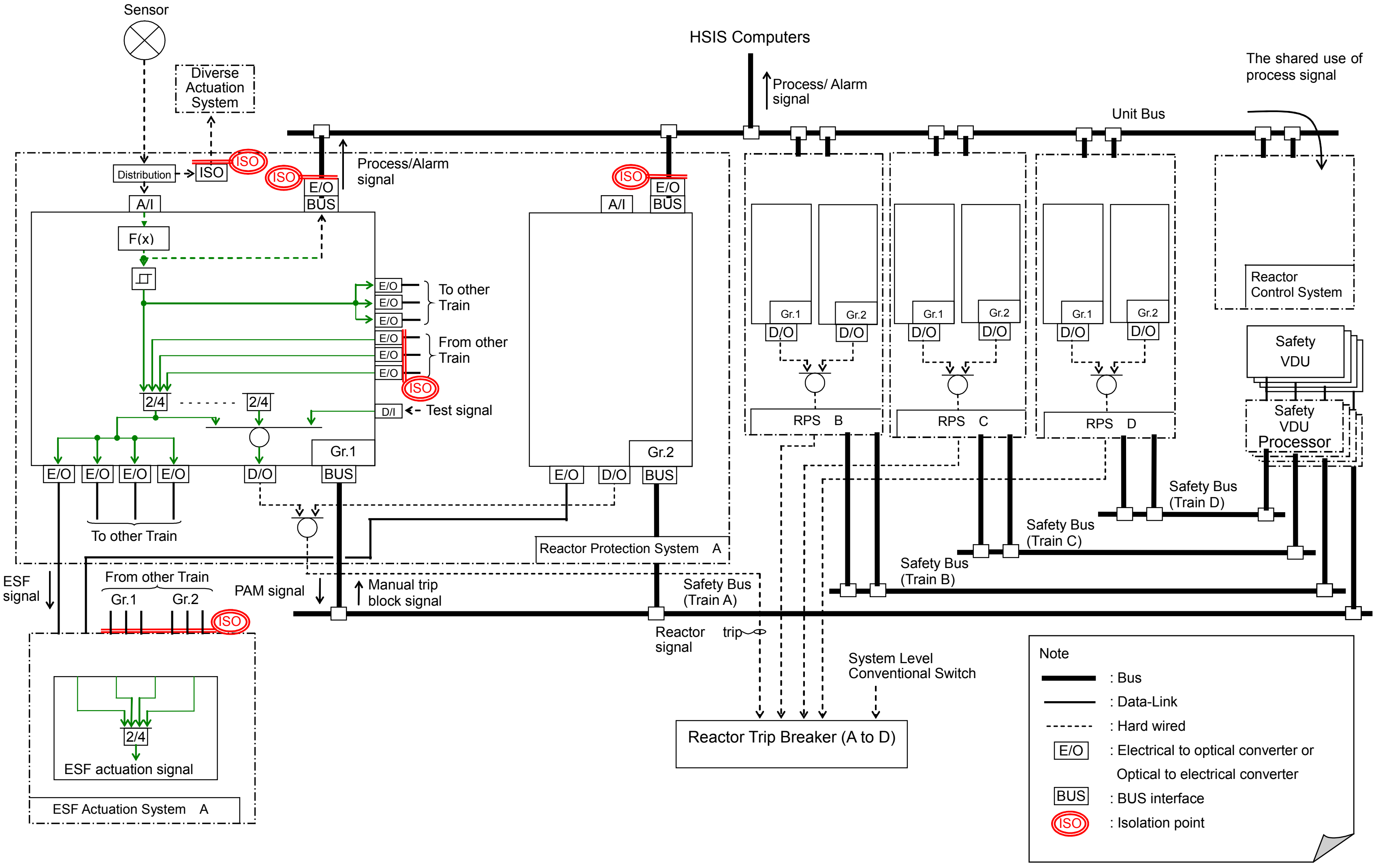


Figure 4.1-4 Configurations of the Reactor Protection System

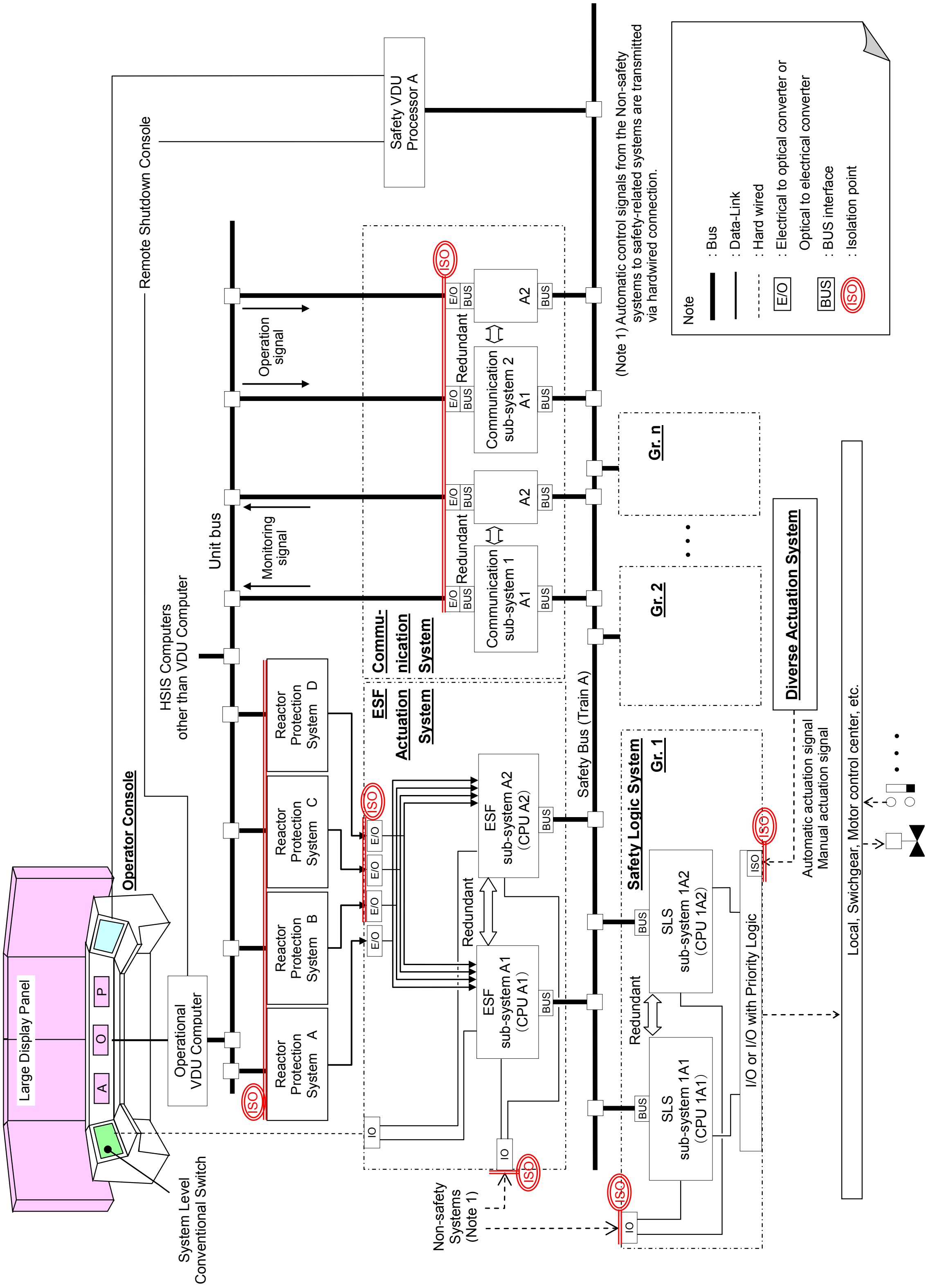


Figure 4.1-5 Configurations of the ESFAS, SLS, and Safety-Related HSI

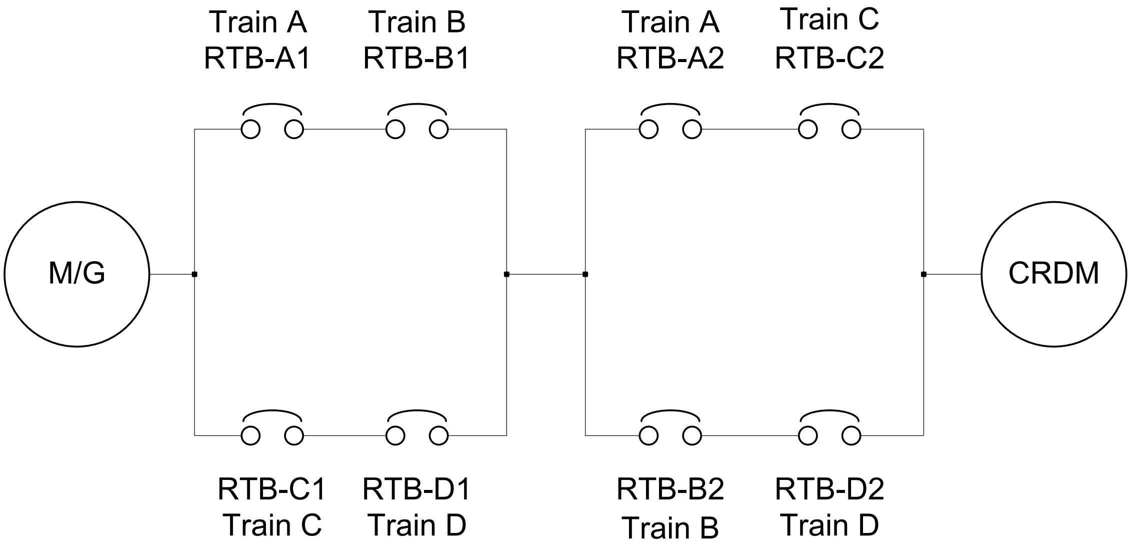


Figure 4.1-6 Configurations of the Reactor Trip Breakers

4.2 Detailed Description of Safety-Related Systems

4.2.1 Reactor Protection System (RPS)

a. Reactor Trip Function in RPS

The RPS automatically prevents operation of the reactor in an unsafe region by shutting down the reactor whenever the predetermined parameter trip setpoints are reached. The safe operating region is defined by several considerations such as mechanical/hydraulic limitations on equipment, and heat transfer phenomena. The RPS maintains surveillance of process variables which are direct measurements of equipment mechanical limitations, such as pressure and also on variables which are direct measurements of the heat transfer capability of the reactor (e.g., reactor coolant flow and reactor coolant temperatures). Other parameters utilized in the RPS are calculated indirectly from a combination of process variables, such as delta T across the reactor core. Whenever a direct process measurement or calculated variable exceeds its setpoint the reactor will be shutdown in order to protect against either gross damage to the fuel cladding or loss of reactor coolant system integrity which could lead to release of radioactive fission products into the containment vessel.

To initiate a reactor trip, the RPS interfaces to the following equipment:

- Sensors and manual inputs
- Reactor trip breakers

The RPS consists of four redundant and independent trains. Normally, four redundant measurements using sensors from the four separate trains are made for each variable used for reactor trip. Selected analog measurements are converted to digital form by analog-to-digital converters within the four trains of the RPS. Signal conditioning may be applied to selected inputs following the conversion to digital form. Following necessary calculations and processing, the measurements are compared against the applicable setpoint for that variable. A partial trip signal for a given parameter is generated if one train’s measurement exceeds its limit. Processing on all variables for a reactor trip is divided into two subsystems in each of the four redundant trains of the RPS. Each train sends its own partial trip signal to each of the other three trains over isolated serial data links. Each train will generate a reactor trip signal if two or more trains of the same variable are in the partial trip state.

Each train of the RPS consists of two separate digital controllers to achieve defense-in-depth through functional diversity. Functional diversity provides two separate methods of detecting the same abnormal plant condition. Each functionally diverse digital controller within a train can initiate a reactor trip. For most events there are at least two diverse sensor measurements for initiation of protection for each plant accident condition. Where two diverse sensor measurements are not available, analog splitters are used to interface the same analog sensor signals to the two functionally diverse controllers.

The reactor trip signal from each of the four RPS trains is sent to a corresponding Reactor Trip Actuation (RTA) train. Each of the 4 RTA trains consists of two Reactor Trip Breakers. The reactor is tripped when two or more RTA trains receive a reactor trip signal. This automatic trip demand initiates the following two actions: 1) it de-energizes the under-voltage trip attachments on the Reactor Trip Breakers, and 2) it energizes the shunt trip devices on the Reactor Trip Breakers. Either action causes the breakers to trip.

The Single Failure Criterion and GDC 24 are met with only three trains in service. Therefore, these requirements are met even when one RPS train and its corresponding RTA train are bypassed. Therefore, bypass of one complete RPS/RTA train is permitted for a limited time period consistent with the reliability of the remaining three trains. Interlocks between RPS trains prevent bypassing two RPS trains or two RTA trains.

It is noted that the PSMS and PCMS share sensors. The method used to ensure this sensor sharing does not compromise conformance to the Single Failure Criterion or GDC 24 while a train is bypassed is discussed below.

b. Engineered Safety Features Actuation Function in RPS

In addition to the requirements for a reactor trip for anticipated abnormal transients, adequate instrumentation and controls are provided to sense accident situations and initiate the operation of necessary Engineered Safety Features (ESF). The occurrence of a limiting fault, such as a loss of coolant accident (LOCA) or a steam line break, requires a reactor trip plus actuation of one or more ESF in order to prevent or mitigate damage to the core and reactor coolant system (RCS) components, and ensure containment vessel integrity.

In order to accomplish these design objectives, the RPS receives signals from various sensors and transmitters for actuation of ESF systems.

The RPS uses selected plant parameters to determine if predetermined safety-related limits are being exceeded. These parameters and safety-related limits are monitored in various combinations which are indicative of primary or secondary system boundary ruptures. Once the required logic combination is completed, the RPS sends the appropriate actuation signals to the ESFAS for event mitigation.

To actuate ESF systems the RPS interfaces with the following equipment:

- Sensors
- Engineered Safety Features Actuation System

Four sensors, each in a separate train, normally monitor each variable which is used for engineered safety features (ESF) actuation. (These sensors may be monitoring the same variable for a reactor trip function as well.) Analog measurements are converted to digital form by analog-to-digital converters within each of the four trains of the RPS. Following the required signal conditioning or processing, the measurements are compared against the setpoints for the ESF to be generated. This signal conditioning, processing, and comparison is done independently within each of the four trains of the RPS. When the measurement exceeds the setpoint, the output of the comparison results in a partial actuation signal for that train. Each RPS train sends its own partial actuation signal to each of the other three RPS trains over isolated serial data links. Each RPS train will generate a system level ESF actuation signal if two or more redundant trains of a single variable are in the partial actuation state.

4.2.2 ESF Actuation System (ESFAS)

The ESFAS consists of one train for each mechanical ESF train in the plant. For the US-APWR some ESF systems have four trains, others have two trains. Since the ESFAS is common to all ESF systems, there are four ESFAS trains for the US-APWR.

The system level ESF actuation signal from each of the four RPS trains is transmitted over isolated data links to an ESFAS controller in each of the ESFAS trains. If there are two ESF trains, the system level ESF actuation signal is transmitted to controllers in two ESFAS trains. If there are four ESF trains, the system level ESF actuation signal is transmitted to controllers in four ESFAS trains.

Manual initiation bypasses the automatic initiation section in the RPS. All trains are separately initiated from train level manual initiation switches. In addition, for four train systems each train is actuated by 2-out-of-3 train level manual initiation signals received from the other 3 trains. Therefore, for all safety functions (two train or four train) all trains are manually initiated by actuating two train level manual initiation switches.

Each ESFAS controller consists of a duplex architecture using dual CPUs, to enhance reliability. In the MELTAC Platform Technical Report, MUAP-07005, this is referred to as a redundant parallel controller configuration. 2-out-of-4 voting logic is performed within each train through the redundant subsystems within each ESFAS controller. Each subsystem generates a train level ESF actuation signal, if the required coincidence of system level ESFAS actuation signals exists at its input, and the correct combination of system level actuation signals exist to satisfy logic sensitive to specific accident situations.

Train level ESF manual initiation signals generated from the Operator Console are also processed by the logic in each redundant subsystem of each ESFAS train to generate the same train level ESF actuation signals. Train level manual initiation signals are generated for each ESFAS signal from conventional switch(es) for each ESFAS train. To avoid spurious actuation from a single contact or signal path failure, each switch contains two contacts that are interfaced to two separate digital inputs. Each ESFAS subsystem processes these signals through 2-out-of-2 voting logic for redundant train level actuation.

Whether automatically or manually initiated, train level ESF actuation signals are transmitted from both subsystems of the ESFAS controller to the corresponding train of the Safety Logic System. The number of ESFAS trains which generate train level ESF actuation signals corresponds to the number of mechanical ESF trains being actuated.

ESF manual actuation function by conventional switch(es) can be manually bypassed for manual testing or maintenance at train level. In addition, some functions may be manually overridden at the train level by deliberate manual operator action to accommodate pre-defined plant conditions after safety function actuation. These override logics are processed in ESFAS controller. Specific bypass or override logic are described in the US-APWR DCD Chapter 7.

The ESF actuation system also provides automatic load sequencing for the Class 1E GTGs to accommodate the Loss of Offsite Power (LOOP) accident. Each ESFAS train monitors the loss of power condition for its respective train. Upon detecting a loss of power, the ESFAS starts the Class 1E GTG for its train and disconnects the loads for its train from the electrical bus. Once the Class 1E GTG is capable of accepting loads, the ESFAS sequences the loads for its train back onto the electrical bus in an order appropriate for the current train level ESF actuation signal(s). The ESFAS sequencing logic accommodates ESF actuation signals occurring prior to or during a loading sequence. The ESFAS load sequencing function is independent for each train.

4.2.3 Safety Logic System

The Safety Logic System (SLS) controls safety-related plant components in all trains based on ESF actuation signals, process instrumentation and component level manual actions from the non-safety operational VDUs and safety VDUs.

The SLS consists of one train for each safety-related mechanical train in the plant. For the US-APWR some safety-related process systems have four trains, others have two trains. Since the SLS is common to all safety-related process systems, there are four SLS trains for the US-APWR.

The SLS consists of multiple controllers in each train. Plant process systems are assigned to controllers based on consideration of maintenance, potential SLS equipment failures and optimization of controller performance. For consideration on functional assignment of SLS controllers, refer to MUAP-09020.

To enhance reliability, each SLS controller consists of a duplex architecture using dual redundant CPUs operating in a redundant parallel configuration. In the MELTAC Platform Technical Report, MUAP-07005, this is referred to as a redundant parallel controller configuration. Each controller of the duplex architecture receives ESF actuation signals and Load Sequencing signals from the corresponding duplex controller of the ESFAS.

The SLS also includes I/O modules mounted in I/O chassis. These I/O chassis can be located either within the same cabinet as the controllers or remotely in separate cabinets that are distributed throughout the plant to reduce the length of cable from the process component or instrument to the I/O chassis. Signals from each SLS controller in the duplex architecture are combined in the output modules using 1-out-of-2 voting logic for control of plant components to the desired safety state.

The SLS I/O modules include contact input conversion devices and Power Interface (PIF) modules. The PIF module transforms the low level signals to voltage and currents commensurate with the actuation devices (such as, motor starters, switchgear, etc.) which they must operate. The actuation devices, in turn, control motive power to the final ESF component. Each train of the Safety Logic System thus interfaces the PSMS to each train of the plant process ESF equipment.

All PIF modules use outputs that must be energized to actuate their respective plant component. When the output is energized, circuit continuity is established (i.e., normally open output contacts). For switchgear and motor operated valves, loss of power or disconnections will have no effect on the plant component and the component will maintain its current position (i.e., If a motor operated valve is in mid-travel, it will fail in the mid-travel position). For motor contactors and solenoids, loss of power or disconnections will result in de-energizing the plant component. De-energized solenoid valves will transit to their mechanically designed failure position (e.g., fail-open or fail-closed).

Each controller has multiple I/O chassis, each chassis has multiple I/O modules and each I/O module accommodates one or more process interfaces. The plant process interfaces are assigned to I/O modules/chassis with consideration of maintenance needs and potential SLS equipment failures. The plant specific Functional Assignment Analysis demonstrates acceptable plant level effects for failure or maintenance of any Controller, including any I/O module or any I/O chassis. Controllers (including I/O modules) are duplicated within a single SLS train if a single failure of the Controller or I/O module will cause a spurious reactor trip. The Controller (including I/O) configuration is described in the US-APWR DCD Chapter 7 and MUAP-09020. PIF modules include logic and interfaces to combine signals from the SLS controllers with signals from the DAS. This interface and logic are also used in a few other cases where fast hardwired response is required, such as turbine trip from turbine protection system.

The primary functions performed by the SLS are described below:

a. Control of ESF Components

The ESFAS provides all system level ESF actuation logics including the automatic load sequence for the Class 1E GTGs. Whether automatically or manually generated, train level ESF actuation signals are transmitted from each ESFAS train to the corresponding train of the Safety Logic System (SLS).

Within the Safety Logic System, the train level ESF actuation signals are then broken down to component actuation signals to actuate each component associated with an ESF. For example, the Emergency Core Cooling System (ECCS) actuation signal must start pumps, align valves, start the Class 1E GTG, and so on. The logic within each train of the Safety Logic System accomplishes this function and also performs necessary interlock to ensure that components are properly aligned for safety. The SLS also controls ESF components based on manual component level controls from operational VDUs and safety VDUs.

b. Control of Safe Shutdown Components

The systems necessary for safe shutdown perform two basic functions. First, they provide the necessary reactivity control to maintain the core in a sub-critical condition. Boration capability is provided to compensate for xenon decay and to maintain the required core shutdown margin. Second, these systems must provide residual heat removal capability to maintain adequate core cooling.

The Reactor Protection System and the Engineered Safety Features Actuation Systems are designed to mitigate accident conditions and achieve immediate stable hot shutdown conditions for the plant.

Manual controls through the safety VDUs or operational VDUs on the Operator Console in the Main Control Room or the Remote Shutdown Console allow operators to maintain longer term hot shutdown conditions and transition to and maintain cold shutdown conditions for the plant. All manual and automatic operation of plant safety-related systems is via the Safety Logic System. Non-safety systems are not required for safe shutdown of the plant.

c. Control of Interlocks Important to Safety

The SLS receives interlock signals from the RPS which operate to reduce the probability of occurrence of specific events or to ensure availability of safety functions.

The Safety Logic System controls these Interlocks Important to Safety through the component level application software in the SLS controllers. Non-safety systems do not control Interlocks Important to Safety.

4.2.4 Safety-Related HSI System

All automated safety functions may be manually initiated and monitored by operators using the safety-related HSI System. The safety-related HSI System is also used to manually initiate other safety functions that are not automated, including safety functions credited for safe shutdown. The safety-related HSI System also provides all safety-related plant information to operators, including critical parameters required for post accident conditions. The safety-related HSIS includes two types of VDUs. Safety VDUs provide the information and operation for components and system level functions of the own train. Multidivisional safety VDUs provide the information for critical safety functions for safe shutdown of all four trains.

a. Control of Reactor Trip Breaker

Operators can trip the Reactor Trip Breakers using conventional switches on the Operator Console. There is one switch for each Reactor Trip Actuation train.

b. Control of ESF Components

The ESF components are controlled from the Safety-Related HSI System on the Operator Console. There are two types of control.

- Touch operations on the safety VDUs
  Touch operations include component and system level functions. Touch operations of component control on the safety VDU are duplicated on the non-safety operational VDUs. Due to better graphics and better screen navigation features, the operational VDUs are the preferred HSI for all normal and abnormal plant conditions. Therefore, the touch operations on the safety VDU are considered backup controls. However, for all design basis events, the safety VDUs are the component level HSI devices credited for compliance to applicable Class 1E criteria.
- Conventional switches on the Operator Console
  Conventional switches are provided to initiate each train level ESF actuation signal. The switches are hardwired to the ESFAS. For all design basis events, the hard controls are the system level HSI devices credited for compliance to applicable Class 1E criteria.

c. Post Accident Monitoring (PAM)

The Safety-Related HSI system displays PAM parameters that are designated Type A, B or C in RG 1.97. The purpose of displaying these post accident monitoring (PAM) parameters is to assist main control room personnel in evaluating the safety-related status of the plant. PAM parameters are direct measurements or derived variables representative of the safety-related status of the plant. The primary function of the PAM parameters is to aid the operator in the rapid detection of abnormal operating conditions. As an operator aid, the PAM variables represent a minimum set of plant parameters from which the plant safety-related status can be assessed.

The Type A and B PAM parameters are normally displayed continuously on the multidivisional safety VDUs on the Operator Console in the Main Control Room. There are two multidivisional safety VDUs; one for Train A and the other for Train D. The parameters are selected based on R.G. 1.97 and at least two channels of each parameter are available. The bases for the selection of the US-APWR PAM variables are described in Appendix H.

d. Safe Shutdown from Outside the Main Control Room

The Remote Shutdown Console, located outside the Main Control Room fire zone, is installed so that safe shutdown can be achieved in the case that the operators can, for any reason, no longer man the MCR.

In order to achieve and maintain the reactor in the cold shutdown condition (safe shutdown state), it is necessary to remove excess heat to control the temperature, pressure and volume of the reactor coolant, and to supply boric acid, etc. Therefore the operating controls of those plant systems necessary for the above mentioned operations, are provided on the Remote Shutdown Console. The Remote Shutdown Console provides the same functions of the operational VDUs and the safety VDUs in the Main Control Room.

These controls are transferred from the Main Control Room to the Remote Shutdown Room (RSR) by MCR/RSR Transfer Switches. The configuration of MCR/RSR transfer system is illustrated in Figure 4.2-1.

Separate Transfer Switch Panels to control each of the four PSMS trains and the PCMS are located just outside of the Main Control Room fire zone (switches dedicated for each of four PSMS trains and dedicated for PCMS in the panel) and in the Remote Shutdown Room (same switch configuration as that of in the Main Control Room fire zone). When the transfer actions from the Main Control Room to Remote Shutdown Console are initiated from both sets of switches for any one train, HSI signals from the MCR are blocked and HSI signals at the RSR are enabled. Transfer is controlled separately for each of the four PSMS trains and separately for the PCMS. Any subsequent damage to MCR HSI devises, caused by the fire in the Main Control Room, does not affect the functions of the Remote Shutdown Console. Transfer from the RSC back to the MCR is activated separately for each of the four PSMS trains and the PCMS using the same transfer switches. Access to the Remote Shutdown Console and the Transfer Switches near the MCR is administratively controlled through closed areas with key access.

This design ensures that no single failure will prevent transfer of more than one train. In addition a single failure will not result in spurious transfer of any train. The design also limits unauthorized transfer by controlling physical access to the transfer switches and ensuring that switches in two separate locations must be actuated before a transfer will occur.

4.2.5 Plant Control and Monitoring System

The non-safety Plant Control and Monitoring System (PCMS) provides direct monitoring and control of non-safety plant systems. It also provides the preferred HSI for all plant systems, including safety-related systems. This section describes the interfaces of the PCMS to the safety-related Protection and Safety Monitoring System (PSMS) and the HSI functions of the PCMS that support plant safety.

a. Instrumentation Shared with the Protection and Safety Monitoring System

In some cases, it is advantageous to employ control signals derived from instrumentation that is also used in the protection trains. This reduces the need for separate non-safety instrumentation which would require additional penetrations into reactor pressure boundaries and additional maintenance in hazardous areas. For each parameter where instrumentation is shared, the PCMS receives four redundant instrument signals from each train of the RPS. The signals are interfaced through fiber optic data networks. As such, an electrical fault in the PCMS cannot propagate to the protection channel.

The SSA ensures the PCMS does not take erroneous control actions based on a single instrument channel failure or single RPS train failure. As such, a single failure will not cause the PCMS to take erroneous control actions that challenge the PSMS, while the PSMS is in a degraded operability state due to the failed instrument channel or failed RPS train. This signal selection algorithm within the PCMS is one design feature that contributes to allowing the RPS to have one instrument channel inoperable or bypassed at all times while still complying with GDC 24 and IEEE Std 603-1991.

b. Information Systems Important to Safety

This section describes information provided to the plant operators from the PCMS for: (1) assessing plant conditions and safety-related system performance, and making decisions related to plant responses to abnormal events; and (2) preplanned manual operator actions related to accident mitigation. The PCMS also provides the necessary information from which appropriate actions can be taken to mitigate the consequences of anticipated operational occurrences.

(1) Post Accident Monitoring (PAM)

A summary of plant safety-related status is continuously displayed on the Large Display Panel and detail information for all PAM parameters can be displayed on the operational VDUs.

(2) Bypassed and Inoperable Status Indication (BISI)

If a safety function of the PSMS is bypassed or inoperable at the train level, this status is continuously indicated on the Large Display Panel and operational VDU. Other bypassed or inoperable conditions that do not result in inoperability of safety functions at the train level are indicated on operational VDUs but not on the Large Display Panel. For example, if a CPU Module of one redundant controller configuration system fails or is turned off within the ESFAS, SLS and communication system (COM), the safety function of the system is still maintained for that train, so this condition is only alarmed at the MCR. For these redundant controller configuration systems, when both of the CPU Modules are turned off, bypassed condition for that system is indicated on LDP and operational VDU by manual BISI operation. Compared with this, before turning off a CPU Module within the RPS or safety VDU of single controller configuration, the system is placed in a bypassed condition, and this bypassed status is continuously indicated on the LDP and operational VDU by manual BISI operation. In addition, if an instrument input to a train of the RPS is bypassed or inoperable, this is continuously indicated on the LDP because that RPS train can no longer perform its safety function for that parameter.

BISI information is displayed on the LDP in the main control room as alarm information. The alarm information on the LDP is spatially-dedicated and continuously visible. The redundant processing of alarm information is described below. Although the LDP itself is not redundant, the LDP screen can be displayed on any operational VDU.

The LDP system and the alarm processors are not Class 1E. Isolation for inputs from the PSMS via fiber optic data-network interfaces ensures independence and separation from safety-related systems.

(3) Plant Alarms

The primary purpose of plant alarms is "to alert operators that the plant is in an abnormal status." Alarms are used not only to draw operator's attention, but also to identify the extent (such as where and what degree) of the abnormal status. The main purposes of alarms can then be summarized as following:

- Alert operators that the plant is in abnormal status.
- Provide operators with information relating to the abnormal status (where and what degree).
- Help operators in making judgments and taking countermeasures.

The computers and data links used to process alarms are redundant. The data links from the safety-related cabinets (RPS, ESFAS, etc.) are physically and functionally isolated to not influence the safety-related system in case of failure of the alarm processing.

The plant alarms are also designed taking into consideration functional and ergonomic aspects, thereby ensuring appropriate fulfillment of operator roles at the time of an alarm.

The main features of the alarm system are as follows:

- Adequate display to acknowledge and recognize alarm information
- Application of alarm prioritization to avoid alarm avalanche
- Request functions from alarm display to relevant operation display and alarm response procedures

These functions help operators to identify and diagnose transients.

(4) Safety Parameter Display System (SPDS)

The safety parameter display system (SPDS) provides a display of plant parameters from which the safety-related status of operation may be assessed in the main control room, TSC, and EOF. The primary function of the SPDS is to help operating personnel in the main control room make quick assessments of plant safety-related status. Duplication of the SPDS displays in the TSC and EOF improves the exchange of information between these facilities and the control room and assists corporate and plant management in the decision-making process. The SPDS is operated during normal operations and during all classes of emergencies.

The functions and design of the SPDS in the main control room are realized as a part of the overall HSI design.

c. Safety-Related Systems and Components Controlled from Operational VDUs

Operational VDUs provide controls for safety-related and non-safety systems and components in all trains. These controls are available by touch operation or other pointing device from the same screen. The common HSI of the operational VDU provides the following operability benefits:

- A single operator can execute procedures that involve multiple safety-related and non-safety systems, simplifying task coordination.
- All software control and monitoring, for safety-related system and non-safety functions, are executed on the same display. This reduces operator transitions between workstation and between display screens, thereby deducing operator work load.
- Computer based procedures allow operators to access relevant display formats which are hyper linked from the procedure and shown on the operational VDU.

The reduction of response time and operator's workload by utilizing integrated operational VDU is described in Appendix I of this Technical Report.

Therefore, even though the safety VDUs and train level conventional switches provide Class 1E credited HSI for all safety-related control and monitoring functions, the operational VDU is the preferred HSI for all normal and abnormal plant conditions. Operation during degraded HSI conditions, such as failure of the operational VDUs, is described in the HSI Topical Report, MUAP-07007.

To ensure there is no potential for the non-safety system to adversely affect any safety functions, the interface between the non-safety operational VDUs in the PCMS and the PSMS is isolated as described below.

- Electrical independence
  Fiber optic interfaces between the PSMS and PCMS prevent propagation of electrical faults between trains. The electrical independence features are shown in Figure 4.2-2.

- Data processing independence
  The PSMS employs communication processors for the PCMS that are separate from the processors that perform safety-related logic functions. The safety-related processors and communication processors communicate via 2-port memory. This ensures there is no potential for communications functions, such as handshaking, to disrupt deterministic safety function processing. The data processing independence features are shown in Figure 4.2-2.

- No ability to transfer unpredicted data
  There is no file transfer capability in the PSMS. Only predefined communication data sets are used between the PSMS and PCMS. Therefore any unknown data is rejected by the PSMS.

- No ability to alter safety-related software
  The software in the PSMS cannot be changed through the non-safety communication network, which is called the unit bus, or from any communication interface that is connected or can be connected to the PSMS. The PSMS software is changeable only when the CPU module that contains the memory devices is removed from the MELTAC

controller. The PSMS basic software is changeable only by removing and replacing the memory device that contains the software. The PSMS application software is changeable only by removing the controller’s CPU module from its chassis and placing it in a dedicated re-programming chassis.

- Acceptable safety function performance
  Normally, manual controls from the safety VDU and manual controls from the non-safety operational VDUs of the PCMS have equal priority (last-in/last-out). However, manual controls from the safety VDU can have priority over any non-safety controls from the PCMS, as follows.

- Failures of non-safety systems are bounded by the safety analysis
  Any plant condition created by the worst case erroneous/spurious non-safety data set (e.g., non-safety failure commanding spurious opening of a safety relief valve) is bounded by the plant safety analysis.

The operational VDU and associated processors are not Class 1E. However, they are tested to the same seismic levels as the PSMS. During this testing the operational VDU and associated processors have demonstrated their ability to maintain physical integrity and all functionality during and after an Operating Basis Earthquake and a Safe Shutdown Earthquake.

4.2.6 Diverse Actuation System

The non-safety Diverse Actuation System (DAS) provides monitoring and control of safety-related and non-safety plant systems to cope with abnormal plant conditions concurrent with a common cause failure (CCF) that disables all functions of the PSMS and PCMS. This section describes the interfaces of the DAS to the PSMS and PCMS and the HSI functions of the DAS that support plant safety. A more detailed description of the DAS is provided in the Defense-in-Depth and Diversity Topical Report, MUAP-07006.

Safety-related or non-safety sensors selected by the plant design are interfaced from within the PSMS or PCMS input modules. These input modules utilize analog splitters and isolation modules that connected the input signals to the DAS prior to any digital processing. Therefore, a software CCF within the PSMS or PCMS will not affect the DAS function. The input module design is described in the MELTAC Platform Technical Report, MUAP-07005.

Within the DAS manual initiation is provided for all critical functions at the train level (e.g., reactivity level, core heat removal, reactor coolant inventory and containment isolation).

Automatic actuation is also provided for functions where time for manual operator action is inadequate.

The DAS has four diverse automatic cabinets (DAACs) and the diverse HSI panel (DHP). The DAS system architecture is shown in Figure 4.2-6. The four DAACs are located in separate Class 1E electrical rooms which are in separate fire and flood zones to cope with internal fire or flood. Failure of one DAAC from internal fire or flood will not affect the DAS automatic functions. In addition, DAS is designed as Seismic Category II to cope with the seismic event concurrent with the software CCF. The seismic qualification method for DAS is equivalent to that for seismic category I qualification of safety-related electrical cabinet.

The DAS interfaces to non-safety process systems and to redundant trains of safety-related process systems. Since the DAS is a non-safety system it does not need to meet the single failure criteria for actuation. However, the design includes redundant inputs, processing logic and outputs arranged in a 2-out-of-2 configuration after taking 1-out-of-2 voting logic twice to ensure the DAS can sustain one random component failure without spurious actuation of either manual or automatic functions at the system, train or component level.

The Diverse HSI Panel is located within the MCR fire zone. The DAS interface to the PSMS output modules is disabled when the MCR is evacuated using the MCR/RSR Transfer Switches, describe above. This ensures that DAS failures that may result due to MCR fire damage will not result in spurious actuation of DAS functions and plant components that could interfere with safe shutdown from the RSC. The DAS is not needed when the MCR is evacuated since a plant accident is not postulated concurrent with a MCR evacuation.

The DAS is a non-safety system; therefore, it does not need to be tested during plant operation. During plant shutdown, the system can be tested by manually injecting input signals to confirm setpoints, and logic functions and system outputs.

In addition, test functions and indications are built into the system so there is no need to disconnect terminations or use external equipment for test monitoring.

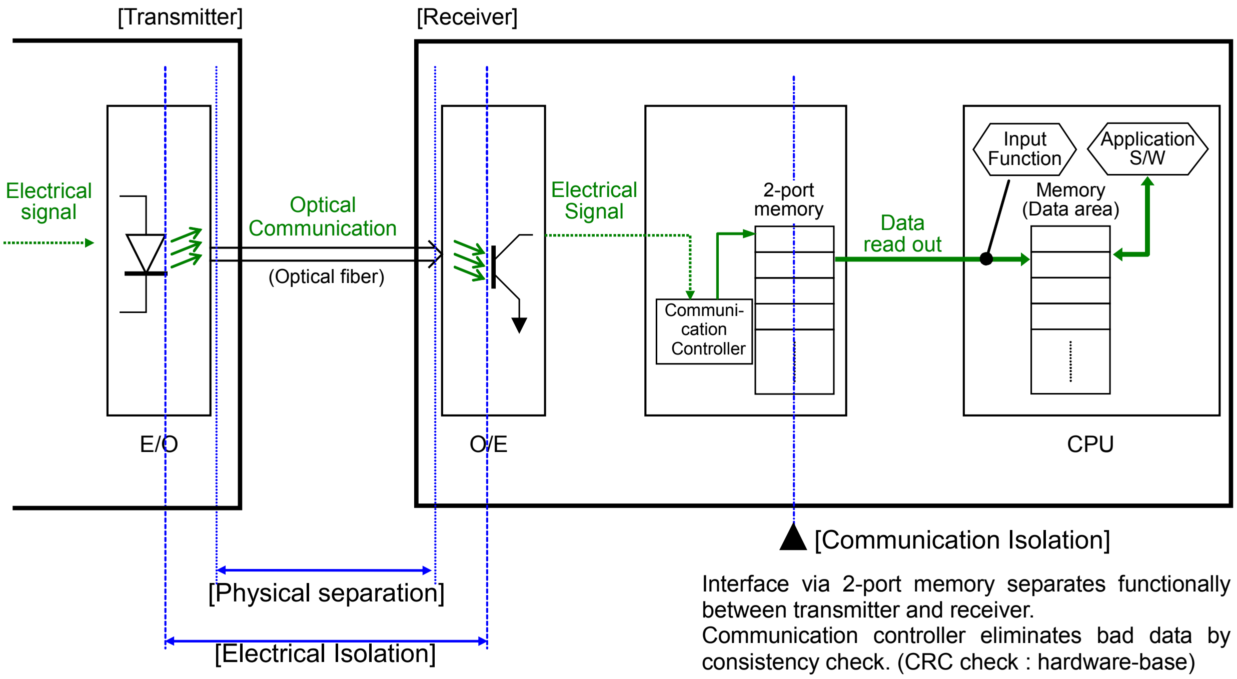
4.2.7 Digital Data Communication

The following digital data communication interfaces are provided in the I&C system;

- The Unit bus provides bi-directional communication between safety-related and non-safety systems for only non-safety functions. The safety-related system and non-safety system are functionally isolated by dedicated communication processors in each safety-related system controller, and priority logic within the safety train that ensure safety functions have priority over all non-safety functions. The Unit bus uses optical fiber to achieve electrical independence of each train. Physical separation between safety-related and non-safety system is accomplished by locating the safety and non-safety trains in different areas. The Unit bus uses the Control Network digital communication technology described in the MELTAC Platform Technical Report, MUAP-07005 Section 4.3.2.
- Communications between different trains are one way data link communication between RPS trains, from RPS to ESFAS and safety VDU trains. Functional separation is achieved by communication controllers that are separate from functional processors and voting logic that processes the data from the different trains. Each data link uses optical fiber to achieve electrical independence of each train. Physical separation between safety trains is achieved by locating it in different areas. These interfaces are the data link digital data communication technology described in the MELTAC Platform Technical Report, MUAP-07005 Section 4.3.3.
- Bi-directional communications between controllers in one (1) safety train are performed by the Safety Bus. The Safety Bus provides deterministic cyclical data communication. Functional independence is provided by separate communication processors within each controller. Fiber optic cable is provided to enhance EMI susceptibility. The Safety Bus uses the Control Network digital communication technology described in the MELTAC Platform Technical Report, MUAP-07005 Section 4.3.2.
- Bidirectional communication between controllers and their respective I/O modules is provided by the I/O Bus described in the MELTAC Platform Technical Report, MUAP-07005 Section 4.1.
- Bidirectional communication between the PSMS controllers and the MELTAC engineering tool is provided by the Maintenance Network described in the MELTAC Platform Technical Report, MUAP-07005 Section 4.3.4. The PSMS controllers are normally disconnected from the Maintenance Network. Temporary connections are made for equipment trouble shooting and periodic surveillance. Temporary connections are managed by administrative controls and plant technical specifications.
- The station bus provides information to plant and corporate personnel and to the EOF and ERDS. The station bus receives information from the PCMS and PSMS via the unit management computer. The isolation device, which is located between the unit management computer and the station bus, provides a hardware-based unidirectional interface which allows only outbound communication. There are no other connections from external sources to the PCMS and PSMS. In addition, the only interface from the PCMS and PSMS to external networks is via the hardware-based unidirectional interface provided

by the isolation device. The hardware-based unidirectional interface provides an outbound only interface to the plant station bus to allow communication to EOF computers, the NRC (via ERDS), corporate information systems and plant personnel computers. The interface with station bus and external networks is shown in Figure 4.2-7.

Figure 4.2-1 Configuration of RSC/MCR Transfer System



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

Figure 4.2-2 Electrical Independence Features between PCMS and PSMS

Figure 4.2-3 Manual Actuation Configuration for Two-Train ESFAS

Figure 4.2-4 Manual Actuation Configuration for Four-Train ESFAS

Figure 4.2-5 Overlap Testability for DAS

Figure 4.2-6 Configuration of DAS

Figure 4.2-7 Interfaces with Station Bus and External Networks

4.3 PSMS Self-Diagnostic Features

The integrity of PSMS components is continuously checked by the platform self-diagnostic features, which are described in detail in Section 4.1.5 in the MELTAC Platform Technical Report, MUAP-07005. The platform self-diagnostic features continuously check the integrity of processing and communication components as well as the range of process inputs. These self-diagnostic features allow early detection of failures, and allow easy and quick repair that improves system availability. Information about detected failures is gathered through system communication networks and provided to maintenance staff in a comprehensive manner. Alarms are generated in the MCR for any failures that affect system functionality. The platform self-diagnostic features control the redundant configuration to maintain all system functions for most single failures.

In addition to platform diagnostic features, the redundant system inputs from different trains are continuously compared to detect failed/drifting instrumentation or input modules. This comparison is performed continuously in the Reactor Control System of the PCMS; deviations are alarmed in the MCR. This automatic CHANNEL CHECK is credited to replace manual CHANNEL CHECK in plant technical specification surveillances.

The integrity of the safety function of the PSMS is continuously checked by their self-diagnostic features. The verification of the self-diagnostic features in the PSMS is confirmed through two diverse test methods:

1. The verification of the self-diagnostic features in all MELTAC controllers in the PSMS is performed during technical specification periodic surveillance testing through the combination of the manually initiated MEMORY INTEGRITY CHECK (MIC), and the manually conducted CHANNEL CALIBRATION, TRIP ACTUATION DEVICE OPERATIONAL TEST (TADOT) or Safety VDU (S-VDU) TEST. For each MELTAC controller in the PSMS, the COT-Digital or ALT- Digital checks each bit of the MELTAC Basic Software, which controls the execution of all PSMS functions, including the self-diagnostic features. In addition, for each MELTAC controller in the PSMS, the CHANNEL CALIBRATION, TADOT and/or S-VDU TEST verifies that the controller can correctly execute program memory instructions.

   Since the TS periodic surveillance test manually confirms that each controller can correctly execute program memory instructions, and the TS periodic surveillance test manually confirms that all memory instructions are correct, including the memory that controls self-diagnosis, the combination of these TS surveillance tests confirms that the PSMS self-diagnostic features are fully operable.

2. The TS periodic manual surveillance tests described above (MIC, CHANNEL CALIBRATION, TADOT and S-VDU TEST) confirms the operability of each MELTAC controller in the PSMS through manual testing methods that are diverse from the self-diagnostic features. If a failure is detected that should have been detected by the PSMS self-diagnostic features, a failure of the PSMS self-diagnostic features is also identified.

   The continuous automatic CHANNEL CHECK, which is also a technical specification surveillance, is conducted by the PCMS, based on signals that are processed by the RPS controllers. This test confirms the operability of the RPS controllers through automated testing that is diverse from the MELTAC self-diagnostic features. If a failure is detected that should have been detected by the MELTAC self-diagnostic features, a failure of the MELTAC self-diagnostic features is also identified. The operability of the automatic CHANNEL CHECK is confirmed through continuous self-testing within the PCMS, and through periodic manual CHANNEL CALIBRATION.

4.4 PSMS Manual Testing and Calibration Features

The integrity of most safety function of the PSMS is continuously checked by the PSMS self-diagnostic features and CHANNEL CHECK performed by the PCMS. The continuous self-diagnostic features enhance the reliability of the PSMS and allow extending the surveillance frequency of most manual surveillances required for Technical Specification compliance In addition, the self-diagnostic features simplify the manual surveillance tests.

The verification of the self-diagnostic features is performed by the combination of (1) manual periodic surveillance tests, that confirm the integrity of all program memory within each MELTAC controller in the PSMS, including the software memory that controls the self-diagnostic functions, and (2) manual periodic surveillance tests that confirm that each controller can correctly execute that program memory. The overlap of these periodic surveillance tests confirms that the PSMS self-diagnostic features are fully operable.

The self-diagnostic features are also confirmed by manual periodic tests and continuous on-line tests that are diverse from the self-diagnostic features. These tests confirm the operability of each MELTAC controller in the PSMS, thereby ensuring that failures have not been missed by the self-diagnostic features.

The coverage of self-diagnosis and manual testing is shown in Figure 4.4-4, and the description of each testing in Figure 4.4-4 is described in Sections 4.4.1 and 4.4.2.

4.4.1 Manual Testing

Manual test features are provided for system level manual initiation of reactor trip and ESF actuation signals, the safety VDU touch screens, binary process inputs and final actuation of plant process components. An additional manual test is conducted to confirm the integrity of the PSMS software memory. Most manual tests may be conducted on-line without full system actuation and without plant disturbance. Each of these manual tests is described in the sections below.

- Manual Reactor Trip (TRIP ACTUATION DEVICE OPERATIONAL TEST)
  The manual reactor trip actuation signals are tested by actuating the conventional switches on the Operator Console, one train at a time. Also, TADOTs are conducted from the O-VDU or S-VDU for the separate undervoltage and shunt trip functions of the reactor trip breakers, as shown in Figure 4.4-1. Correct functionality is confirmed by status signals sent from the RTBs to the O-VDU or S-VDU via the RPS controllers. When the reactor trip function is tested one train of reactor trip breakers will open, but the plant will not trip, since breakers in two trains must open to de-energize the CRDMs.

  The Reliability Analysis method, which demonstrates the need to conduct this test no more frequently than once per 24 months, is described in Section 6.5. However, this test may be conducted more frequently, if required by the reliability of the reactor trip breakers. The test frequency for the reactor trip breakers is described in the US-APWR DCD Chapter 16.

This test corresponds to tests of the reactor trip breakers and manual initiation switches in conventional plants. For the PSMS, This test confirms input and output interfaces, and the program memory processing capability of the RPS. This test overlaps with self-diagnostic tests as shown in Figure 4.4-4.

- Manual ESF Actuation (TRIP ACTUATION DEVICE OPERATIONAL TEST)
  The manual ESF actuation signals are tested on-line by actuating the conventional switches on the Operator Console. Correct functionality is confirmed by status signals sent from the PSMS to the O-VUD or S-VDU. These status signals are generated by the PSMS controllers, so there is overlap between the manual test and the platform self-diagnosis. To prevent train level actuation during this test, a Bypass for Manual Test is activated prior to the test. This blocks all manual initiation signals for one train within the ESFAS logic. In accordance with RG 1.47, the block is alarmed with SDCV display to indicate the ESFAS train is bypassed. Removal of the bypass is verified when the alarm has cleared.

  The Reliability Analysis method, which demonstrates the need to conduct this test no more frequently than once per 24 months, is described in Section 6.5.

  This test corresponds to test of the train level manual initiation switches in conventional plants. For some conventional plants, this test is credited to confirm input and output interfaces, program memory processing, communication and display capability of the ESFAS. This test overlaps with platform self-diagnostic tests as shown in Figure 4.4-4.

- Safety VDU TEST
  Safety VDU touch screens are tested by manually touching screen targets and confirming correct safety VDU response.

  The Reliability Analysis method, which demonstrates the need to conduct this test no more frequently than once per 24 months, is described in Section 6.5.

  There is no test corresponding the safety VDU TEST in conventional plants. For the PSMS, this test is credited to confirm the touch response and display operability of the S-VDUs, the interface between the S-VDU and the S-VDU controllers, program memory processing, communication and display capability of the S-VDU and the S-VDU controllers. This test overlaps with platform self-diagnostic tests as shown in Figure 4.4-4.

- Analog and Binary Process Inputs (CHANNEL CALIBRATION)
  Analog and binary process inputs are tested in conjunction with manual calibration of the process measurement device, as described in Section 4.4.2, below. CHANNEL CALIBRATION is applicable only to binary process devices that have drift potential, such

as undervoltage relays and turbine trip oil pressure switches. Correct functionality is confirmed by reading analog or binary values on any VDU driven by the signal processed by the PSMS.

This test corresponds to tests of process measurement devices in conventional plants. For the PSMS, this test is also credited to confirm the process measurement devices, the interface from those devices to the PSMS, input signal processing, program memory processing, communications and display capability of the RPS or ESFAS. This test overlaps with platform self-diagnostic tests and automated CHANNEL CHECK as shown in Figure 4.4-4.

- Binary Process Inputs (TRIP ACTUATION DEVICE OPERATIONAL TEST)
  Binary process inputs to the PSMS are tested periodically by manipulating the process to stimulate a state change in the process monitoring device. This test applies to binary devices with no drift potential, such as the main feedwater pump trip status signals. This test is also applicable to binary devices with drift potential, as described above, to grossly check their operability on a more frequent basis than CHANNEL CALIBRATION. Correct functionality is confirmed by status signals sent from the PSMS to any VDU driven by the binary status signal generated from the PSMS.

  To avoid spurious actuations during this test, the test is conducted with the train that receives the signal in a bypass mode or with the input channel in a bypass mode. This prevents spurious actuation of this train and it prevents propagation of the input signal state change to other trains.

  The Reliability Analysis method, which demonstrates the need to conduct this test no more frequently than once per 24 months, is described in Section 6.5. However, these tests may be conducted more frequently, if required by the reliability of the process monitoring device. The test frequency for binary process monitoring devices is described in DCD Chapter 16.

  This test corresponds to tests of binary inputs in conventional plants. For some conventional plants, this test is credited to confirm operability of internal system logic functions. For the PSMS, this test is credited to confirm process measurement devices, the interface from those devices to the PSMS, input signal processing, program memory processing, communication and display capability of the RPS or ESFAS (depending on which controller processes the input). This test overlaps with platform self-diagnostic tests as shown in Figure 4.4-4.

- Final Actuation Outputs (TRIP ACTUATION DEVICE OPERATIONAL TEST)

Either test, individual or group, also confirms the functionality of the SLS output module and the interface to the plant component. Since the control signals are generated by the SLS controllers, there is overlap between the manual test and the platform self-diagnosis.

The Reliability Analysis method, which demonstrates the need to conduct manual tests of the SLS outputs no more frequently than once per 24 months, is described in Section 6.5. However, this test may be conducted more frequently, if required by the reliability of the plant process components. The test frequency for the plant process components is described in the US-APWR DCD Chapter 16.

This test corresponds to tests of system outputs in conventional plants. For the PSMS, this test is also credited to confirm the program memory processing capability of the SLS and the COM controllers, the PSMS output device (including the priority logic in the Power Interface Module), the interface from the PSMS to the plant components and the plant components themselves. This test overlaps with platform self-diagnostic tests as shown in Figure 4.4-4.

- Memory Integrity Check (MIC)

This function is used during periodic surveillance tests to confirm that the software in the controller is the same as the off-line version, and therefore has not changed. This test confirms the functional integrity of PSMS software applications without the need to perform functional logic tests. The Memory Integrity Check (MIC) is conducted with the train for the controller to be tested in a bypass condition. Administrative controls assure the remaining three trains are still in service. This ensures that performance of the MIC will not result in a loss of safety function of PSMS.

As described in the MELTAC Technical Report, MUAP-07005, Section 4.1.7.2, software design of the MIC function will be performed under an approved Appendix B program. This assures that the software quality of the MIC function is equivalent to that of a safety system. Therefore, the design for surveillance testing complies with the guidance of BTP 7-17.

The following features minimize the potential for unexpected software change errors that could result in total PSMS failure between test intervals: (1) Access Control: the PSMS software is physically secured, as described in Section 7.9.2.5 of the DCD, and (2) Software Configuration Management: the PSMS software is maintained in accordance with Section 3.11 of “US-APWR Software Program Manual” (MUAP-07017).

The Reliability Analysis method, which demonstrates the need to conduct Memory Integrity Checks no more frequently than once per 24 months, is described in Section 6.5.

This test ensures the integrity of the software credited to execute system safety functions, including correct setpoints, constants and logic functions. This test also ensures the integrity of the software credited to execute self-diagnostic functions. The function of the Memory Integrity Check is designed with augmented quality and maintained in accordance with Appendix D of the US-APWR Software Program Manual (MUAP-07017). The Memory Integrity Check overlaps with platform self-diagnostic tests, automated cross-channel tests and manual tests described above and as shown in Figure 4.4-4.

Figure 4.4-1 shows the overlap testability for reactor trip. Figure 4.4-2 shows the overlap testability for ESF Actuation. Figure 4.4-3 shows the overlap testability for the safety VDU.

4.4.2 Manual Calibration (CHANNEL CALIBRATION)

PSMS analog input modules and power supplies are continuously checked for failure by the platform self-diagnosis. In addition, redundant analog input channels are continuously compared between trains to detect failures and unexpected drift, as discussed in Section 4.3 above.

However, to correct for expected time dependent drift that can commonly affect all redundant analog instruments and analog processing components, these components are periodically checked for accuracy and calibrated as needed. The calibration check for PSMS components is most easily conducted in conjunction with the calibration check for plant process instrument.

Plant process instruments are calibrated using various techniques that stimulate the instrument’s sensing mechanism. During the calibration of the instrument, the analog or binary signal generated by the instrument is monitored on any VDU (e.g., operational VDU or safety VDU). This monitoring ensures the functionality of the signal path from the sensor to the PSMS, and the accuracy of the signal processing within the PSMS, including the analog or binary input module and power supplies. Since the VDU signals are generated by the RPS or

ESFAS controllers, there is overlap between the manual calibration and the platform self-diagnosis.

Process instruments are calibrated one train at a time. During the calibration the instrument channel is bypassed in the RPS. This prevents erroneous RPS or ESFAS actuation due to a single failure of another channel during the calibration.

The Accuracy Analysis method, described in Section 6.5, demonstrates the need to check the calibration of PSMS power supplies and analog input modules no more frequently than once per 24 months. However, this test may be conducted more frequently, if required by the reliability of the plant process instrumentation. The test frequency for the plant process instrumentation is described in the US-APWR DCD Chapter 16.

This manual calibration corresponds to the tests of process measurement devices in conventional plants. For the PSMS, this manual calibration is credited to confirm the process measurement devices, the interface from those devices to the PSMS, input signal processing, program memory processing, communication and display capability of the RPS or ESFAS (depending on which controller processes the input). This test overlaps with platform self-diagnostic tests and automated CHANNEL CHECK as shown in Figure 4.4-4.

4.4.3 Response Time Test

The MELTAC components of the PSMS and most PSMS instrumentation include no components that have known aging or wear-out mechanisms that can impact response time. Therefore response time can only be affected by random failures or calibration discrepancies. All random failures and calibration discrepancies are detected by the testing and calibration methods described above. The MELTAC Technical Report, MUAP-07005, demonstrates that failures that would impact system response time are detectable through self-diagnosis or manual surveillance tests.

Specific components of the PSMS that require periodic response time tests are identified in the US-APWR DCD Chapter 16 Technical Specifications.

4.5 PSMS On-line Maintenance

Components in the PSMS that require periodic age related replacement, such as power supplies, are described in the MELTAC Technical Report, MUAP-07005. Other components are replaced only when they are detected as failed either by self-diagnosis or manual surveillances.

Failures detected by platform self-diagnosis are automatically diagnosed to the replaceable module level. Alarms are provided on operational VDUs and failed module identification is provided on the engineering tool. Alarms are provided for failures detected by self-diagnosis in all processor configurations, single or redundant. Failed processor modules in a Redundant Parallel Controller configuration and failed I/O modules may cause actuation or failure of components in a single train, depending on the application logic.
I/O modules can be replaced while the PSMS controllers are powered. Processor modules (e.g., CPU and digital communication modules), require power to be removed from the chassis, prior to module replacement. For failed processor modules in controllers configured for parallel or standby redundancy, the controllers will recover to their normal redundant configuration with

no plant impact beyond the initial failure, as discussed above. For failed processor modules in single controller configurations, the plant level effects of the failure must be considered, including recognition that the controller must be powered down for module replacement. Replacement of I/O modules must consider that some modules have more than one input or output. Therefore, if the initial failure was limited to a single channel on the module, removal of the failed module may impact more channels and therefore more plant interfaces. Failures and module replacement are considered in the assignment of plant process I/O to I/O modules during the system design, to minimize plant impact during module failure or maintenance.

The plant level of effects of controller failures (including I/O modules) are described in Appendix G of this report and MUAP-09020.

Figure 4.4-1 Overlap Testability for Reactor Trip

Figure 4.4-2 Overlap Testability for ESF Actuation

Figure 4.4-3 Overlap Testability for Safety VDU

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

5.0 DESIGN BASIS

This section puts special emphasis on the explanation of key technical issues and describes the general design features for compliance with seismic and fire protection requirements.

5.1 Key Technical Issue

This section summarizes the I&C system features that specifically address the following key technical issues.

- Multi-channel operator stations
- HSI to accommodate reduced operator staffing
- Operation under degraded conditions
- Integrated RPS/ESFAS with functional diversity
- Common cause failure modes for Defense-in-Depth and Diversity analysis
- Output modules for PSMS and DAS
- Control system failure modes for safety analysis
- Credit for self-diagnosis for technical specification surveillances
- Unrestricted bypassed of one safety-related instrument channel
- Minimum inventory of HSI
- Computer based procedures
- Priority logic

5.1.1 Multi-Channel Operator Station

There is two-way communication between non-safety operational VDUs and the PCMS and between the non-safety operational VDUs and all trains of the PSMS. To ensure there is no potential for the non-safety system to adversely affect any safety functions, the interface between the non-safety operational VDUs in the PCMS and the PSMS is isolated as described in Section 4.2.5, above, are applied.

- Electrical independence
- Data processing independence
- No ability to transfer unpredicted data
- No ability to alter safety-related software
- Acceptable safety function performance
- Failures of non-safety systems are bounded by the safety analysis

5.1.2 HSI to Accommodate Reduced Operator Staffing

There are several features of the I&C systems that support reduced operator staffing:

- The multi-channel operational VDUs provide the primary operator interface for both the MCR and the RSR. The multi-channel operational VDUs allow a single operator to execute Computerized Procedures and control all safety-related and non-safety systems and components from a single HSI device.
- Self-diagnosis and continuous automated calibration features reduce the need for operator support of maintenance and testing activities.
- Most manual surveillance tests requiring operator support can be conducted from the MCR.

5.1.3 Operation under Degraded Conditions

In the event of complete failure of all operational VDUs, the plant can be safely shut down using only the safety VDUs. Also, the plant can be safely shut down using only the safety VDUs in the event of a complete PCMS failure. Based on the high reliability of these non-safety components, complete failure of the PCMS or complete failure of the operational VDUs, are considered to be very infrequent events. Failure of an individual operational VDU is easily detected by operators, because the operational VDU is continuously used for plant operation. The ability to detect individual operational VDU failures and complete failure of all PCMS VDUs is confirmed during HSI validation testing.

The high reliability of the operational VDUs is based on redundancy of components, independence of redundant components and self-diagnostic functions within the computers that support the operational VDUs. Specific reliability data for individual VDU components is not credited.

There is no periodic manual surveillance testing for the operational VDU for the following reasons:

1) The operational VDU has no safety functions, and the safety VDU is only credited.
2) The operational VDU is continuously used; therefore, a failure is immediately detected.
3) The operational VDU communication interfaces are continuously monitored by the self-diagnostic features of the PSMS. These self-diagnostic features are periodically tested as described in Section 4.4.

In addition, in practice, the monitoring and manual control functions of the operational VDU and their communication capabilities are expected to be verified by the following PSMS periodic surveillance tests as described in Section 4.4:

- CHANNEL CALIBRATION
- TRIP ACTUATION DEVICE OPERATIONAL TEST (Actuation Logic and Actuation Output)

5.1.4 Integrated RPS & ESFAS with Functional Diversity

Within the same subsystem of the RPS, RPS bistable and coincidence voting functions are also used for ESFAS, where both functions are actuated on the same parameters and the same setpoint. Where the parameter or setpoints are different, there are separate bistable and voting functions. The functions are combined because integration of RPS and ESFAS requires less hardware than if the functions were separated. Less hardware results in fewer failures and less testing. Fewer maintenance interactions with the system reduce the potential for human errors that can reduce system reliability or cause spurious actuations that threaten plant safety.

Instead of separating RPS and ESFAS, functional diversity is provided within the integrated RPS/ ESFAS through two separate subsystems in each train. For each DBA each subsystem processes diverse sensor inputs that can each detect the DBA and initiate protective actions. PRAs done for the MHI digital I&C design are expected to show significant benefit for this functional diversity; this is confirmed on a plant specific basis.

5.1.5 Common Cause Failure Modes for Defense-in-Depth and Diversity Analysis

BTP 7-19 requires consideration of CCFs that “disable” the protection system. Based on this, the coping analysis described in the Defense-in-Depth and Diversity Topical Report, MUAP-07006 considers CCFs that result in a fail as-is condition in the PSMS and PCMS. The coping analysis does not consider CCFs that result in output state changes (i.e., spurious actuation to de-energized or energized state).

5.1.6 This section intentionally left blank

5.1.7 Output Module for PSMS and DAS

Output Modules in the PSMS interface control signals to the plant components. These same output modules are used to interface control signals from the DAS. A common Output Module provides one power interface conversion device for control of one plant component. This reduces the maintenance that would be required for two separate devices and it reduces the complexity of combining the PSMS and DAS signals via relay logic. Reduced complexity results in improved reliability.

Control signals are interfaced from the PSMS controllers to the software part of the Output Module via the controller’s I/O bus. Control signals from the DAS are interfaced via conventional hardwired connections and conventional isolation modules (for the PSMS only) to the hardware part of the Output Module. The isolation modules are part of the PSMS (i.e., they are Class 1E devices). Therefore DAS output signals interface to plant components via only the hardware part of the Output Module, so CCF within the PSMS or PCMS digital platform will not affect DAS signals.
Figure 5.1-1 shows the signal interface between output module and PSMS and DAS.

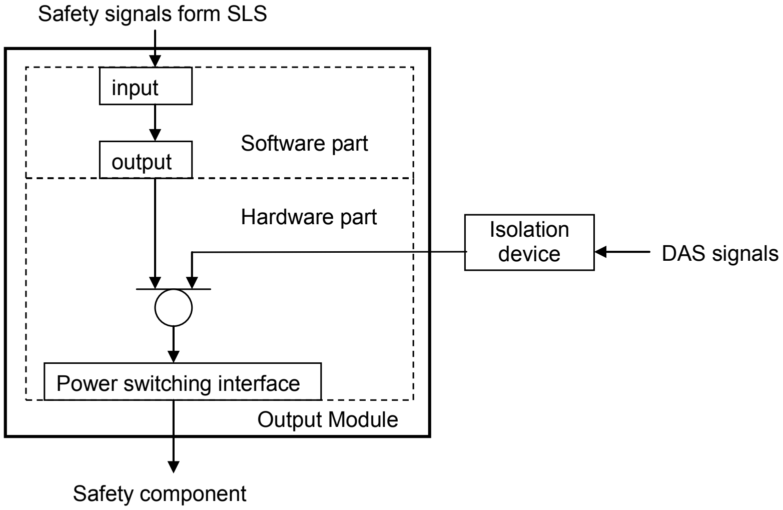


Figure 5.1-1 Signal Interface of Output Module

5.1.8 Control System Failure Mode

The non-safety PCMS has high reliability based on the following design features:

- The MELTAC platform that is applied to the PCMS is essentially the same as the MELTAC platform applied to the PSMS.
- The PCMS includes redundant controllers operating in a redundant standby controller configuration, as explained in the MELTAC Platform Technical Report. In this configuration a back-up standby controller changes into the active control mode if there is a failure of the primary controller.
- Non-safety control functions are partitioned in multiple redundant PCMS controllers to limit the effects of single failures.

Figure 5.1-2 shows the configuration example of the Reactor Control System.

Even assuming any type of failure including software CCFs of the PCMS, including operational VDUs, the US-APWR is adequately protected by demonstrating the following;

1. Consequences of multiple spurious actuation signals from a single PCMS control group caused by multiple random hardware failures or a software design defect meet the DCD Chapter 15 anticipated operational occurrence (AOO) acceptance criteria.

2. Consequences of multiple spurious actuation signals of multiple non-safety components, caused by a software design defect in multiple PCMS control groups, meet the DCD Chapter 15 postulated accident (PA) acceptance criteria.

3. Consequences of multiple spurious actuation signals of multiple safety-related and non-safety components, caused by a software design defect in one or more operational VDUs, meet the DCD Chapter 15 PA acceptance criteria.

The effects of potential PCMS failures are analyzed and described in Appendix J.

5.1.9 Credit for Self-Diagnosis for Technical Specification Surveillance

Testing from the sensor inputs of the PSMS through to the actuated equipment is accomplished through a series of overlapping sequential tests. The majority of the tests are conducted automatically through self-diagnosis.

Figure 4.4-1 shows the overlap testability for reactor trip. Figure 4.4-2 shows the overlap testability for ESF Actuation. Figure 4.4-3 shows the overlap testability for the safety VDU.

Plant specific technical specifications identify manual surveillance tests that confirm input signal calibration and propagation through the digital system. Manual surveillance tests are also provided to confirm command propagation through the digital system and correct control of plant components. These manual surveillance tests, along with the self-diagnosis and Memory Integrity Checks discussed above, are credited to eliminate manual surveillance tests of functional logic and algorithms, setpoints and constants.

5.1.10 Unrestricted Bypass of One Safety-Related Instrument Channel

The PSMS includes multiple trains from sensors to actuated device with complete electrical isolation and independence.

For system functions with four redundant (non-spatially dependent) instrument channels, one instrument channel may be bypassed continuously without violating any design criteria. The system adheres to all criteria with only three instrument channels in operation, as follows:

5.1.11 Minimum Inventory of HSI

Class 1E HSI is provided by the safety VDUs for all safety-related indications and controls. Spatially Dedicated Continuously Visible (SDCV) displays are provided for all critical safety function parameters and for bypassed and inoperable conditions. This data is obtained from the PSMS and PCMS. SDCV HSIs are provided for manual initiation of reactor trip and ESFAS. Additional SDCV HSIs may be provided to ensure timely operator actions for specific plant events. The complete minimum inventory of SDCV HSI is described in the HSI system Topical Report, MUAP-07007. The complete minimum inventory of SDCV HSI is also described in DCD Chapter 18.

5.1.12 Computer Based Procedures

Computer based procedure allows operators to access relevant display formats which are hyper linked from the procedure and shown on the operational VDU. The operator is able to access and operate the required control switch quickly from the linked display formats on the operational VDU, if necessary.

5.1.13 Priority Logic

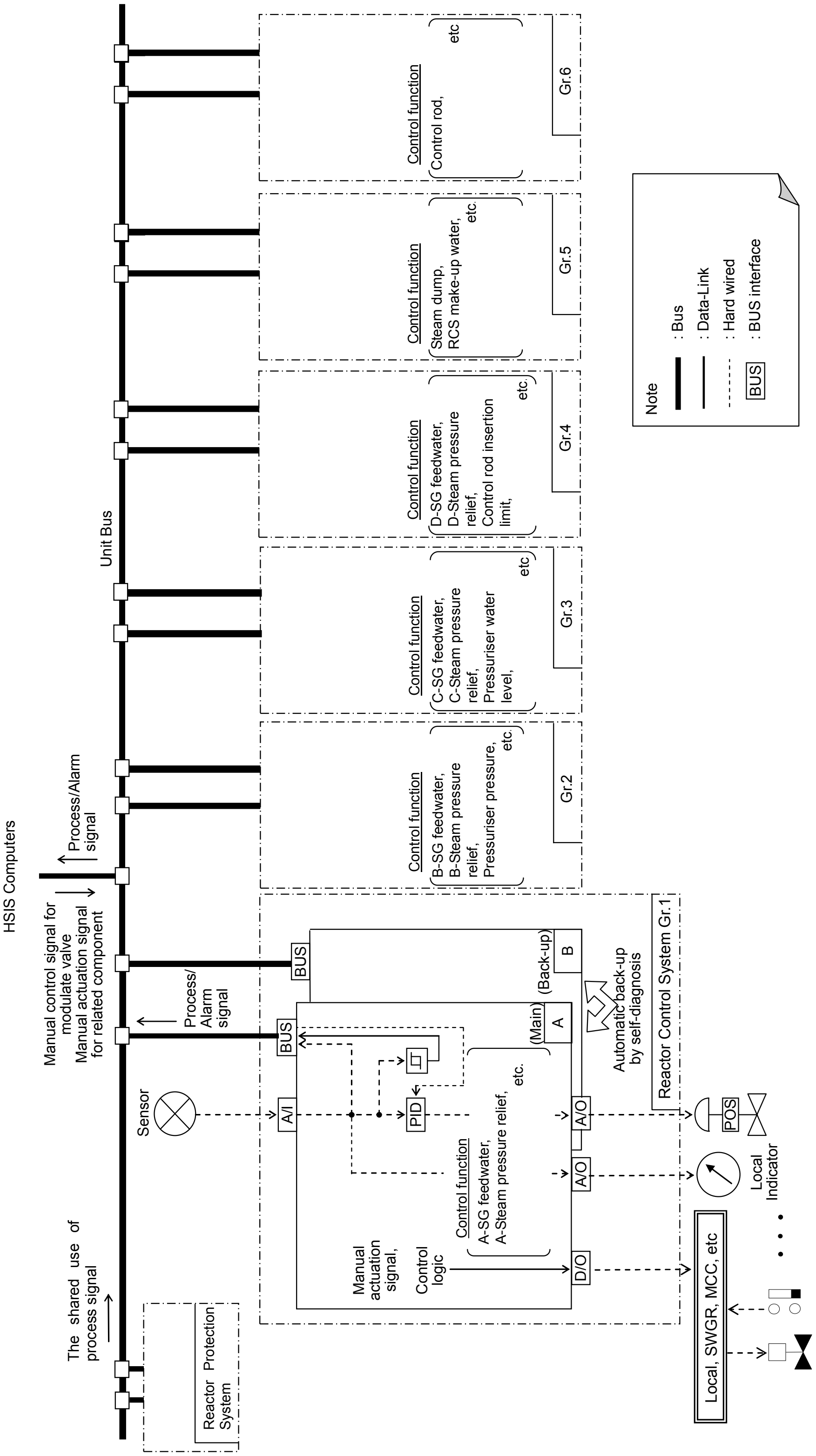


Figure 5.1-2 Configuration Example of Reactor Control System

Figure 5.1-3 Priority Between Commands from Safety VDU and Operational VDU

Figure 5.1-4 Priority for Manual and Automatic Signals of Safety and Non-Safety Demand

Figure 5.1-5 State-Based Priority in PIF

Figure 5.1-6 Manual Permissive Logic for Bypass Signals from Operational VDU

5.2 This section intentionally left blank

Figure 5.2-1 Deleted

Figure 5.2-2 Deleted

Figure 5.2-3 Deleted

Figure 5.2-4 Deleted

6.0 DESIGN PROCESS

The design process for the MELTAC digital platform applied to the PSMS is described in the MELTAC Platform Technical Report, MUAP-07005.

The software life cycle for the PSMS is described in MUAP-07017, Software Program Manual (SPM).

Section 6.5 describes the key analysis conducted during the design process which ensures the final system conforms to critical design basis requirements.

6.1 This section intentionally left blank

Figure 6.1-1 Deleted

6.2 This section intentionally left blank

Figure 6.2-1 Deleted

6.3 This section intentionally left blank

6.4 This section intentionally left blank

6.5 Analysis Method

6.5.1 FMEA Method

The Failure Modes and Effects Analyses (FMEA) demonstrate that:

- All PSMS failures are detectable (through self-diagnosis or manual surveillance tests).
- No single failure will prevent PSMS actuation of RT or ESFAS.
- No single failure will result in spurious PSMS actuation of RT or ESFAS.
- The PSMS will fail to the safe state for all credible failures. The safe state for the RPS is trip. The safe state for ESFAS/SLS is as-is for failures that impair control but do not result in complete loss of component control. The safe state for the ESFAS/SLS is de-energized for failures that result in complete loss of component control.

In addition, the Functional Assignment Analysis demonstrates that credible PSMS failures do not cause plant conditions more severe than those described in the analysis of anticipated operational occurrences in Chapter 15 of the Safety Analysis Report (SAR). The Functional Assignment Analysis for the SLS is documented in MUAP-09020.

This section describes the FMEA method.

Safety functions are designed with multiple trains. Each train is independent from the other trains and from the non-safety trains. Independence ensures that credible single failures cannot propagate between trains within the safety-related system or between safety-related and non-safety trains. Therefore credible single failures can not prevent proper protective action at the system level. The credible single failures considered in the safety-related and non-safety trains are described in the FMEA for each system. The FMEA follows the guidance of IEEE Std 379, which is endorsed by RG 1.53.

Component
The component being analyzed is identified by functional description (e.g., analog input module). Where there are multiple similar components additional descriptive information is added to ensure an unambiguous identification (e.g., chassis/slot location, specific module type, etc.)

Failure Mode
The failure modes of the component are defined in the terms of the component’s output interface to other downstream components. Typical failure modes include High, Low, As-is. One row is included in the table for each credible failure mode.

Method of Failure Detection
The means by which the failure will come to the attention of the plant operation/maintenance staff are identified. This could be by automatic detection or manual testing.

Local Failure Effect
The consequent effect(s) of the failure on the component or on its adjunct components are described. Symptoms and local effects including dependent failure are also provided.

Effect on Protective Function or Plant
For safety-related systems the effect of the failure on the ability to complete the protective function or spurious actuation of the protective function is described, including identification of any degradation in performance or degree of redundancy. For non-safety functions the effect of the failure on the plant is described. Any plant challenges that are outside the boundary conditions of the Plant Safety Analysis are discussed. For safety-related and non-safety functions mitigating design features that prevent or limit the failure effects are discussed.

Failures that are undetectable or result in effects that violate the system design basis are specifically highlighted. These failures are specifically justified or the system design is modified.

Table 6.5-1 Deleted

The FMEA for safety-related I&C system is provided in Appendix G of this report.

6.5.2 Reliability Analysis Method

The reliability of the safety-related I&C system to perform its safety functions is analyzed in the Probabilistic Risk Assessment (PRA).

This analysis starts with the simplified block diagram discussed above for the FMEA. This block diagram shows the major components that must operate correctly for actuation of the safety function. The mean time between failure (MTBF) is identified for each component. The MTBF for components of the MELTAC platform are provided in the MELTAC Platform Technical Report. The MTBF for other components is obtained from industry handbooks or manufacturers publications. The actual reliability data and the source of the data for these components are identified in plant licensing documentation. The system reliability is calculated based on this system model and the MTBF of each component.

The reliability analysis credits internal redundancy within each train, and it credits all four available trains for each system.

However, the reliability analysis credits only three of four instrument channels for each measured parameter. This conservative approach ensures that the system meets the required PRA goals while operating in a degraded condition. Based on this there are no Limiting Conditions of operation expected for extended operation with an instrument channel out of service. Refer to MUAP-07030 Attachments 6A.12 and 6A.13.

The reliability analysis credits the immediate detection of module failures that are tested by self-diagnosis. For failures in components that are manually tested and calibrated, the reliability analysis is based on a 24 months surveillance interval.

The reliability analysis for specific plant applications are discussed in the US-APWR DCD Chapter 19.

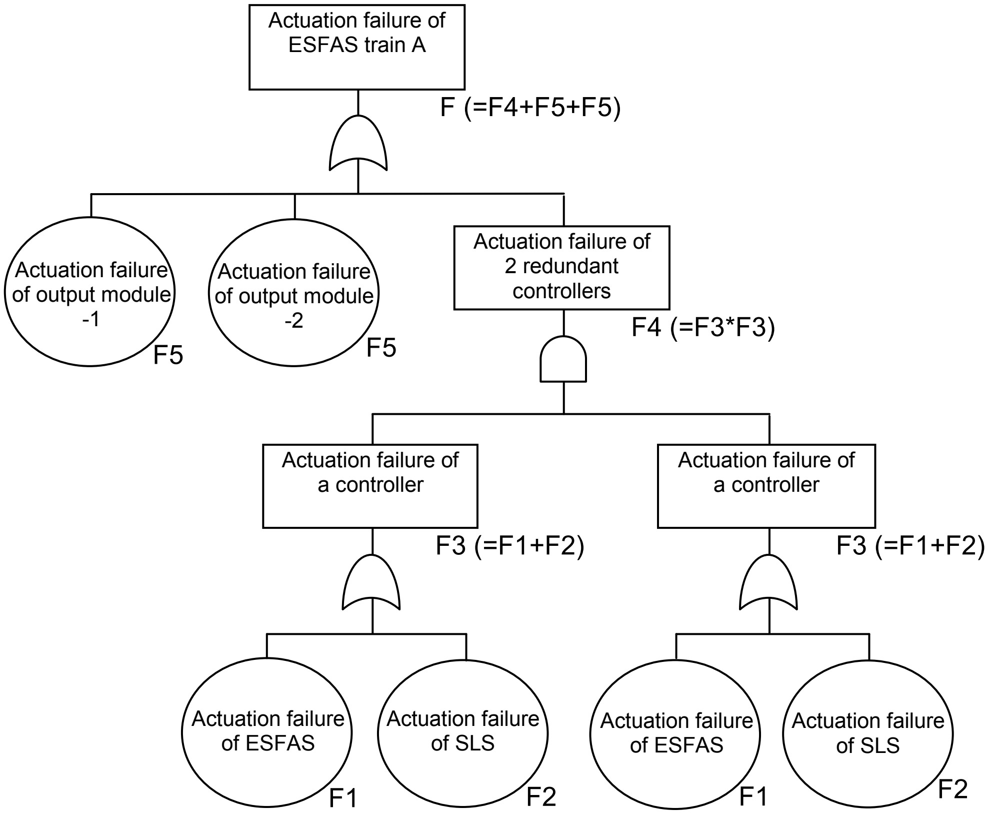

Actuation failure of ESFAS train A
F (=F4+F5+F5)
Actuation failure of output module -1
F5
Actuation failure of output module -2
F5
Actuation failure of 2 redundant controllers
F4 (=F3*F3)
Actuation failure of a controller
F3 (=F1+F2)
Actuation failure of a controller
F3 (=F1+F2)
Actuation failure of ESFAS
F1
Actuation failure of SLS
F2
Actuation failure of ESFAS
F1
Actuation failure of SLS
F2

Figure 6.5-1 Typical FTA for Failure of ESFAS Actuation

6.5.3 Response Time Analysis Method

The response time of the safety functions is used in the plant safety analysis. The response time of each safety function is calculated by adding the response time of each component that makes up the system, from the process measurement to the actuation of the final component.

To illustrate the response time analysis method, the following configuration is the response time model for reactor trip.

Figure 6.5-2 Breakdown Response Time for Reactor Trip

6.5.4 Accuracy Analysis Method

The accuracy of each instrumentation loop for safety function is analyzed to determine the instrument channel set points. A typical loop consists of the following components:

- Sensor
- Analog input module

Loops that include an interface to the DAS would have an additional analog splitter/isolation module.

The accuracy of the complete channel is calculated by combining the accuracy of each component in the loop using statistical methods. A square root of the sum of the squares

(SRSS) method is applied. The accuracy of each component consists of the nominal accuracy plus uncertainty due to temperature effects and time dependent drift.

The typical formula for SRSS uncertainty calculation for one component in the loop takes the form:

$$A = \pm (B^2 + C^2 + D^2)^{1/2}$$

where

A = resultant uncertainty for one component
B, C, D = random and independent terms for each uncertainty element (e.g., temperature, time, etc.).

The method is based on the guidance, ISA-S67.04.01-2000 that is equivalent to ANSI/ISA-S67.04, Part I -1994 endorsed by RG 1.105. The guidance provides the recommended practice for ISA-RP67.04.02 -2000, “Methodologies for the Determination of Setpoints for Nuclear Safety-Related Instrumentation.”

To illustrate the accuracy analysis method, the uncertainty of the loop shown in the following figure is calculated below. The typical calculation model and calculation formula for the channel uncertainty of the instrumentation loop is described.

Figure 6.5-3 Typical Calculation Model for Channel Uncertainty of the Instrumentation Loop

$$CU = \pm (SRA^2 + SPE^2 + STE^2 + SD^2 + SMTE^2 + DCU^2)^{1/2}$$

This section defines key components of the US-APWR setpoint methodology. US-APWR Technical Report MUAP-09022 Instrument Setpoint Methodology describes the details of the uncertainty calculation methods for safety-related system setpoints. Many uncertainties considered in the setpoint methodology for safety-related systems are also applicable to non-safety setpoints, including the Diverse Actuation System. Non-applicable uncertainties are specifically noted in the non-safety setpoint calculations. Non-safety setpoints also exclude limits specifically related to Technical Specifications, such as Allowable Values. The details of the setpoint methodology demonstrate compliance to BTP 7-12.

6.5.5 Heat Load Analysis Method

The heat load of the components within each PSMS enclosure (i.e., cabinet or console in which PSMS equipment is mounted) is calculated to establish room Heating Ventilating and Air Conditioning (HVAC) sizing requirements. Proper HVAC sizing ensures the room ambient temperature stays within expected boundaries. The heat load for each PSMS enclosure is determined by the total consumption of electricity of the PSMS modules within the cabinet. The power consumption for each module is based on the MELTAC platform specifications for each module. Total electric power consumption is converted to total heat load.

The maximum temperature of the components within a PSMS enclosure is also calculated to ensure components operate below their maximum normal temperature (97°F [36°C]), and below their maximum qualified temperature (140°F [60°C]). To establish the internal cabinet operating temperature the temperature rise within the cabinet is calculated. The forced ventilation airflow within the cabinet is increased as necessary to ensure the normal and qualification limits are maintained. The heat rise calculations for each PSMS enclosure are confirmed by actual measurements during integration testing.

6.5.6 Seismic Analysis Method

The seismic analysis method for the PSMS is based on Regulatory Guide 1.100, which endorses IEEE Std 344-2004.

The MELTAC platform (i.e., digital components and cabinet) is qualified by generic seismic type testing. The type testing method for the MELTAC platform is described in the MELTAC Platform Technical Report. This section explains the analysis methods used to confirm that the type tests bound the in plant conditions to which the MELTAC components will actually be exposed.

Seismic analyses, using the equivalent static acceleration method, and the mode superposition time-history method, are performed for the Safe Shutdown Earthquake (SSE). The analyses are performed to determine the seismic force distribution for use in the design of the nuclear island structures, and to develop in-structure seismic responses (accelerations, displacements, and floor response spectra) for use in the analysis and design of seismic subsystems.

The seismic qualification methods for different configurations of MELTAC equipment within the PSMS are described as follow.

(1) Seismic Qualification for MELTAC components mounted within MELTAC cabinets

The seismic analysis confirms that the floor acceleration for each PSMS cabinet location in the plant is lower than the seismic acceleration value during type testing. The seismic analysis also confirms the total mass and distribution of equipment mounted within each cabinet is equivalent or less than the mass and distribution of the equipment mounted in the cabinet during type testing.

(2) Qualification of non-MELTAC enclosures

Special non-MELTAC enclosures, such as the Operator Console and Remote Shutdown Console are computer modeled using techniques such as the Finite Element Method (FEM). The computer model includes the mass and distribution of the equipment mounted within the enclosure. The model is computer stimulated with the floor response spectra for its specific location within the plant. The computer analysis confirms the structural integrity of the enclosure, including the maximum enclosure deflection, and the specific seismic accelerations at the mounting locations for MELTAC components (for use in item c., below).

(3) Qualification of MELTAC components mounted within non-MELTAC enclosures

The seismic accelerations at the equipment mounting locations (from item b. above) are compared to the seismic accelerations recorded at the equipment mounting locations during the MELTAC platform type tests. The analysis confirms that the type testing bounds the accelerations that will be seen by the MELTAC components in these special non-MELTAC enclosures.
Seismic analysis is described in the US-APWR DCD Chapter 3.

6.5.7 EMI Analysis Method

The EMI qualification of the MELTAC platform complies with RG 1.180. The test is performed with a cabinet fully equipped with a typical configuration of components required for a safety-related system. The details of the EMI qualification testing are described in the MELTAC Platform Technical Report, MUAP-07005.

The EMI qualification analysis confirms that the type tested conditions bound the in plant conditions to which the MELTAC components will actually be exposed. This includes the configuration of the MELTAC components and the wire routing, shielding and grounding. The EMI qualification analysis also confirms that the characteristics of the EMI environment for the type test bounds the EMI environment of the plant.

6.5.8 Fire Protection Analysis

Most components within the PSMS are manufactured from fire retardant materials to minimize the combustible load. The combustible load from the PSMS considered in the fire analysis is estimated based on the total content of flammable materials.

The fire protection analysis demonstrates the ability to achieve safe shutdown with a fire in one fire zone of the plant and the following failures of I&C equipment within that fire zone:

- The failures considered in the fire analysis include short circuits, open circuits and application of worst case credible faults in both common mode and transverse mode.
- The four trains of the PSMS and the PCMS are in five separate fire zones. The fire analysis considers the worst case spurious actuations that can result from the failures identified above for the equipment in the one zone with the fire.
- The MCR and RSC contain only HSI for multiple trains of the PSMS and the PCMS (DAS HSI is discussed below). The HSI is enabled in only one location at a time. A fire occurring in the RSC will have no impact on the plant because the HSI in this location is normally disabled. A fire occurring in the MCR will result in failures (as described above) initially in only one train (safety-related or non-safety), due to physical and electrical separation between trains. The fire will ultimately cause these failures in all trains. However, prior to this the MCR/RSC Transfer Switches will be activated to disable all MCR HSI. Therefore there will be no adverse effects on other trains.
- The DAS HSI is also located in the MCR. This HSI interfaces to all four PSMS trains. The DAS HSI is disabled if the MCR/RSC Transfer Switch is in the RSC position. The DAS HSI contains two circuits (1) permissive circuits and (2) system / component switch circuits. Permissive and switch circuits must both actuate to generate control actions in the PSMS. These two circuits are physically and electrically separated, including a fire barrier. In addition, most components within the DAS are manufactured from fire retardant materials to minimize the combustible load. If a fire starts in one DAS circuit, it will be detected by MCR operators, since the DAS is in a continuously manned location. Therefore, there is sufficient time for activation of the MCR/RSC Transfer Switch so that the DAS interfaces are disabled in the PSMS before spurious DAS signals, which may be generated due to propagation of the fire, can cause adverse PSMS control actions.
- The automated section of the DAS contains four subsystems (i.e., DAACs). The DAS is configured with 2-out-of-2 voting logic after taking 1-out-of-2 voting logic twice to generate control signals to the PSMS. These four subsystems are in separate fire zone so that a fire in one area may spuriously actuate only one PSMS train.

Figure 4.2-6 shows this fire protection configuration of DAS.
Fire protection and fire protection program are described in DCD Chapter 9.

Figure 6.5-4 Deleted

7.0 This section intentionally left blank

8.0 REFERENCES

In this section, references referred to in this report except for applicable codes and standards and regulatory guidance in Section 3.0 are enumerated.

1. Safety System Digital Platform -MELTAC-, MUAP-07005-P Rev.9 (Proprietary) and MUAP-07005-NP Rev.9 (Non-Proprietary).

2. Defense-in-Depth and Diversity, MUAP-07006-P-A Rev.2 (Proprietary) and MUAP-07006-NP-A Rev.2 (Non-Proprietary), September 2009.

3. HSI System Description and HFE Process, MUAP-07007-P Rev.5 (Proprietary) and MUAP-07007-NP Rev.5 (Non-Proprietary), November 2011.

4. Quality Assurance Program (QAP) Description for Design Certification of the US-APWR, PQD-HD-19005 Rev.5, May 2013.

5. Methodologies for the Determination of Setpoints for Nuclear Safety-Related Instrumentation, ISA-RP67.04.02-2000.

6. Deleted

7. System 80+ Design Certification Document (DCD).

8. Design Control Document for the US-APWR, Rev.4, August 2013.

9. US-APWR Instrument Set point Methodology, MUAP-09022-P Rev.3 (Proprietary) and MUAP-09022-NP Rev.3 (Non-Proprietary), July 2013.

10. US-APWR Software Program Manual, MUAP-07017-P Rev.5 (Proprietary) and MUAP-07017-NP Rev.5 (Non-Proprietary), November 2013.

11. Defense in Depth and Diversity Coping Analysis, MUAP-07014-P Rev.6 (Proprietary) and MUAP-07014-NP Rev.6 (Non-Proprietary), September 2013.

12. Response Time of Safety I&C System, MUAP-09021-P Rev.3 (Proprietary) and MUAP-09021-NP Rev.3 (Non-Proprietary), August 2013.

13. US-APWR Functional Assignment Analysis for Safety Logic System, MUAP-09020-P Rev.2 (Proprietary) and MUAP-09020-NP Rev.2 (Non-Proprietary), May 2011.

14. MELTAC Platform ISG-04 Conformance Analysis, MUAP-13018-P Rev.0 (Proprietary) and MUAP-13018-NP Rev.0 (Non-Proprietary).

15. Small Break LOCA Sensitivity Analyses for the US-APWR, MUAP-07025-P Rev.3 (Proprietary) and MUAP-07025-NP Rev.3 (Non-Proprietary), March 2011.

Appendix A Conformance to IEEE 603-1991

This appendix describes conformance of the PSMS to the requirements of IEEE Std 603. The section numbers follow the sections in IEEE Std 603. All sections pertain to the 1991 version of this standard unless specifically noted.

A.1. Scope

This conformance section addresses the PSMS, which is the instrumentation and control portion of the safety system.

A.2. Definitions

The definitions are applicable to the PSMS.

A.3. References

The PSMS conforms to all referenced standards, as explained below.

A.4. Safety System Designation

A.4.1 Design Basis Events

The PSMS is designed to protect the health and safety of the public by limiting the release of radioactive material during accident conditions to acceptable limits. The safety analyses described in the US-APWR DCD Chapter 15 demonstrate that even under conservative critical conditions for design basis accidents, the safety systems provide confidence that the plant is put into and maintained in a safe state following accident conditions. The events considered in the safety analysis and limits of plant conditions are described in the US-APWR DCD Chapter 15.

A.4.2 Safety Functions and Corresponding Protective Actions

The functions of the PSMS credited in the plant safety analysis are described in the US-APWR DCD Chapter 15 and Sections 7.2 and 7.3.

A.4.3 Permissive Conditions for Each Operating Bypass Capability

In the PSMS protective functions are initiated and accomplished during various reactor operating modes. Automatic or manual block of a protective function is provided during specific plant modes if that protective action would spuriously actuate due to normally expected plant conditions. Permissive interlocks are provided for manual blocks and both manual and automatic blocks are automatically removed whenever the appropriate plant conditions are not met. Hardware and software used to initiate an automatic block, provide a permissive for a manual block, and achieve automatic removal of the automatic or manual blocks are part of the PSMS and, as such, are designed in accordance with the criteria in this report. Initiation of manual blocks may be by either the operational VDUs or safety VDUs. In either case the PSMS provides the necessary safety permissive and automatic removal.

A.4.4 Variables Required to be Monitored for Protective Action

- The specific variables monitored for reactor trips are described in the US-APWR DCD Section 7.2.

The specific variables monitored for engineered safety features (ESF) actuation are described in the US-APWR DCD Section 7.3.

The Plant Technical Specifications specify the allowable values for the limiting conditions for operation (LCOs) and the trip setpoints for the reactor trip and ESF actuation.

Table A.4.4-1 Deleted.

Table A.4.4-2 Deleted.

A.4.5 The Minimum Criteria for Each Action Controlled by Manual Means

Means are provided in the MCR for manual initiation of protective functions at the system level. Manual control of safety systems at the component level is provided from the MCR and the Remote Shutdown Room.

A.4.5.1 Emergency actuation of reactor trip and/or ESFAS is automatically provided by the PSMS, immediately after an accident is automatically detected. The automated systems allow the plant to achieve a safe stable state with no credited manual operator actions. Operators can detect abnormal conditions by monitoring plant instrumentation and can manually initiate the same protective actuations at any time. Manual initiation of reactor trip or ESFAS is not required or credited in the plant safety analysis. Whether or not these manual actions are credited, there are no interlocks that prevent manual initiation.

To maintain the safe stable state, some manual operator actions are needed. The PSMS is designed so the earliest operator actions are not required for a certain time period defined in the safety analysis from the onset of the accident. Earlier manual operator actions for specific events (e.g., Boron Dilution) are described in the US-APWR DCD Subsection 7.5.1.5, including appropriate HFE justification.

Interlocks ensure that operator actions cannot defeat an automatic safety function during any plant condition where that safety function may be required. In addition, when safety functions are automatically initiated, interlocks ensure that opposing manual actions cannot be taken until acceptable plant conditions are achieved.

A.4.5.2 Manual initiation of one protective action does not interfere with subsequent automatic actuation of other protective actions. There is no capability to completely block or bypass the initiation of any automatic actuation, except when plant condition interlocks permit this blocking as discussed in Section A.4.3, above.

A.4.5.3 The safety-related ventilation system provides cooling, heating, filtration, pressurization and ventilation to the MCR. This ventilation system and its support systems consist of four redundant trains, while the emergency systems consist of two trains, and provide these functions in a reliable and failure tolerant fashion. If offsite power is not available, each Class 1E GTG provides backup power. In case of an accident, the MCR is isolated to protect operators from invading radioactivity, and the emergency ventilation system which consists of two redundant trains is activated.

A.4.5.4 The manual operator actions credited in the safety analysis for accident mitigation, and the variables displayed in the MCR specifically for this purpose are described in the US-APWR DCD Subsection 7.5.1.5. The variables used by operators to monitor the plant and take discretionary manual actions are also discussed in the US-APWR DCD Section 7.5. The HSI for all of these manual functions is available on safety VDUs and operational VDUs.

A.4.6 Spatially Dependent Variables

The minimum number, locations and processing method for spatially dependent variables is described in the US-APWR DCD Section 7.2. Thermowell-mounted resistance temperature detectors (RTDs) installed in each reactor coolant loop provide the hot and cold leg temperature signals required for input to the protection and control functions. The hot leg temperature measurement in each loop is accomplished using three fast-response, multi-element, narrow-range RTDs. The three thermowells in each hot leg are mounted approximately 120 degrees apart in the cross-sectional plane of the piping, to obtain a representative temperature sample. The temperatures measured by the three RTDs are different due to hot leg temperature streaming and vary as a function of thermal power. The PSMS averages these signals to generate a hot leg average temperature.

Radially varying cold leg temperature is not a concern because the RTDs are located downstream of the reactor coolant pumps. The pumps provide mixing of the coolant so that radial temperature variations do not exist.

The power range neutron flux is a spatially dependent variable. Calculations involving overtemperature and overpower delta T use axial variation in neutron flux. Excore detectors furnish this axially-dependent information to the overtemperature and overpower calculations in the RPS. The average nuclear power signals for the reactor protection functions are dependent on the axial power distributions, but the uncertainty of this effect is only for a conservative direction (increase the average power output from the neutron detector). Also, the average nuclear power signals are dependent on the radial neutron flux distributions for anomalies occurring in one core quadrant. These anomalies can be detected by the neutron flux detector in that quadrant and by the detectors in the two adjacent quadrants, but may not be detected by the detector in the opposite quadrant. Therefore, to ensure event detection and accommodate, the neutron flux detectors must be operable in all four quadrants.

A.4.7 Range of Conditions for Safety System Performance

The PSMS is located in a mild environment. The equipment is seismically qualified to meet safe shutdown earthquake (SSE) levels. The equipment is also qualified for electromagnetic and radio frequency interference.

The Emergency Power Supply system (EPS), from emergency busses and generators, and the Uninterruptible Power Supply system (UPS), from plant batteries and inverters, supplies electrical power to the PSMS. The PSMS performs its safety functions within the range of voltage and frequency provided by EPS and UPS.

A.4.8 Functional Degradation of Safety Functions

The PSMS is located in plant areas that provide protection from accident related hazards such as missiles, pipe breaks and flooding. The redundant trains of the PSMS are isolated from each other and isolated from non-safety systems. Isolation ensures functional and communications independence and independence for fires and electrical faults. The design life of PSMS components is maximized when operated continuously in a controlled ventilation environment. The PSMS will operate reliably for extended periods with loss of ventilation.

A.4.9 Reliability

The reliability analysis methods for the PSMS are described in Section 6.5.2. This analysis ensures that the PSMS meets the reliability requirements assumed in the Probabilistic Risk Assessment (PRA). The PSMS includes either N trains or N+1 trains, depending on the application. N is the number of trains needed to meet the single failure criterion and the number of trains needed to meet the single failure criterion.

A.4.10 The Critical Points in Time or the Plant Conditions

The PSMS automatically initiates appropriate protective actions when a plant condition monitored by the system reaches a preset level. The critical points in time are determined by the PSMS response time modeled in the accident analysis. The PSMS is designed and tested to meet the response times assumed in the accident analysis.

The operator can reset the PSMS system level actuation signal using a minimum of two distinct and deliberate actions. There are no automatic resets of the system level actuation signals.

A.4.11 Equipment Protective Provisions

No credible single failure of an equipment protective device prevents the initiation or accomplishment of a safety function at the system level.

The PSMS continuously checks internal conditions such as power supply and digital component operability. Components are automatically shut down under component failure conditions that may lead to unpredictable system performance. These checks are conducted independently within each train of the PSMS; therefore, a spurious shutdown of PSMS equipment will only affect one train.

The equipment protective features are designed to place the safety systems in a safety state, or into a state that has been demonstrated to be acceptable, if the safety-related equipment fails or the equipment protective device operates. Each protection function has different characteristics and therefore different techniques are used to achieve a fail-safe design. Examples of protective features for selected functions include:

- Reactor trip circuits are designed to fail in the tripped state.

- Engineered safety features actuated components are designed to fail into a de-energized state or fail as-is. The de-energized state applies to failures that result in complete loss of component control. The as-is state is selected for failures that impair control but do not result in complete loss of component control. This state has been demonstrated to be acceptable if conditions such as disconnection, loss of power source, or postulated adverse environments are experienced.

- Analog sensor circuits are designed, so that a loss of power will produce an off-scale signal that can be identified by the protection system as bad. Loss of power can occur in the sensor, the analog distribution module or the analog portion of the analog input module. Digital protective equipment input circuits are designed to recognize off-scale values based on the expected range of the input signal (e.g., 4-20 mA). When an off-scale signal is detected, the digital equipment will take appropriate action (partial actuation or generation of alarms).

- Failures in binary sensor circuits cannot be distinguished from normal binary state changes. Therefore, for the RPS loss of power to binary inputs will result in alarms and partial trip signals, since the RPS is designed to fail to a trip condition. For binary sensor inputs to the ESFAS controllers, the application will generate alarms only, since the ESFAS is designed to fail as-is.

- A safe signal means the signal results in a trip or a partial trip actuation by failure of sensor circuits described as above. A safe signal is a part of signal generated by a loss of power, therefore, it can be recognized as a result of alarms and a partial trip actuation.

- The failure modes and effects analysis in Appendix G identifies the module level effects of off-scale sensor failures (“Fail high” and “Fail low”), the method of failure detection, and the resulting effect for the system level RT and ESF functions.

- Actuation signals from multiple PSMS trains are provided for selected actuated equipment to improve the reliability of the protection system and minimize the impact of equipment protective provisions.

Equipment protective provisions may also be included in the instrumentation monitored by the PSMS and the plant components controlled by the PSMS. Provisions such as electrical fault and thermal overload protection are common in safety-related plant components. Any provisions of this type are described in the US-APWR DCD Subsection 8.3.1. Since all equipment protective provisions are independent within each train of the safety systems, a spurious shutdown of plant equipment will only affect one train.

A.4.12 Other Special Design Basis

The PSMS complies with all applicable regulatory and industry criteria as described in Section 3. A non-safety DAS is included to provide the functions necessary to reduce the risk associated with postulated common cause failures of PSMS functions. The DAS is separate, independent and isolated from the PSMS. The DAS is diverse from the PSMS in all design aspects, including software, hardware, function and HSI.

A.5. Safety System Criteria

A.5.1 Single Failure Criterion

A single failure within the PSMS does not prevent the initiation or accomplishment of a protective function at the system level, even when a channel is intentionally bypassed for test or maintenance.

The safety system includes sufficient redundancy to meet system performance requirements even if the system is degraded by a single failure. Redundancy begins with the sensors monitoring the variables and continues through the signal processing and actuation electronics. Redundant actuations are also provided.

Connections between redundant trains or connections that carry signals to or from non-safety systems are designed to ensure that faults or erroneous data originating in one train cannot propagate and cause failure of another train. The design ensures that any erroneous operation that may be caused by signals from other safety trains, including the non-safety trains, is within the boundaries of the safety analysis and is mitigated by other protective actions.

One design goal of the PSMS is to minimize inadvertent reactor trips and ESF actuations. Redundancy is provided for critical circuits which could malfunction and give an erroneous trip or ESF actuation signal. The reactor trip breaker arrangement prevents a single failure from causing a reactor trip. The 2-out-of-4 actuation logic for reactor trip requires trip signals from 2-out-of-4 trains.

The design to reduce the likelihood of inadvertent trips or engineered safety features actuations does not negate the ability of the safety system to meet the single failure criterion, even when channels are bypassed for test or maintenance.

A.5.2 Completion of Protective Action

Once initiated, either automatically or manually, protective functions proceed to completion. In addition, system level signals cannot be manually reset until the plant condition is restored to a pre-determined setpoint. The operator can override ESF actuation, after the protective function proceeds to completion. The override can be initiated only on a component-by-component basis by deliberate intervention using a minimum of two distinct manual actions.

A.5.3 Quality

The quality of PSMS components and modules and the quality of the PSMS design process is controlled by a program that meets the requirements of ASME NQA-1-1994.

Conformance to ASME NQA-1-1994 is described in the Topical Report, Quality Assurance Program (QAP) Description For Design Certification of the US-APWR (Reference 4).

A.5.4 Equipment Qualification

DCD Subsection 7.1.3.7 describes the environmental and seismic qualification of the PSMS.

A.5.5 System Integrity

PSMS is located in plant areas that provide protection from natural phenomena related hazards such as tornadoes, and accident related hazards such as missiles, pipe breaks and flooding. The equipment is environmentally and seismically qualified and qualified for input power variations.

For the RTS, the undervoltage and shunt trip mechanisms of the reactor trip breaker will trip under the conditions of loss of power or disconnection, except failures or disconnections prior to the 2-out-of-4 voting logic. The ESF components will maintain their current position or transition to their mechanically designed failure position under the above conditions.

A.5.6 Independence

A.5.6.1 Between Redundant Portions of a Safety System

Train independence is carried throughout the PSMS as well as the sensors and the devices actuating the protective function. Physical separation is used to achieve separation of all redundant train components. Wiring for redundant trains uses physical separation or barriers to provide independence of the circuits. Separation of wiring is achieved using separate wireways, cable trays, and containment penetrations for each train. Separation distances and barriers conform to regulatory guides or industry standards. Where this is not possible due to physical constraints, such as for HSI devices on control panels, analysis and testing are used to demonstrate the adequacy of the isolation method. Separate power feeds energize each redundant protection train.

Where redundant equipment communicates, such as between the trains of the RPS, fiber optic cables are employed to preserve electrical independence of the trains. Communications independence is achieved by communication modules that are separate from the safety function processing modules. Functional independence is achieved by coincidence voting logic.

There are no electrical components, including sensors that are common to redundant portions of the PSMS.

The only shared component that is common to redundant portions of the safety system is the instrument tap on the high pressure side of reactor coolant flow measurement used for the low reactor coolant flow reactor trip signal. This common instrument tap is used for all four redundant flow instruments (i.e., there is a separate flow instrument for each PSMS train). The common instrument tap is separated to four redundant sensing lines connected to the four redundant flow transmitters. Also the common instrument tap design has been applied to most conventional PWR plants in U.S.

ANSI/ISA S67.02-1980 endorsed by RG 1.151 describes that a single process pipe tap to connect process signals to redundant instruments shall not be used. However, the latest version of the ANSI, ANSI/ISA S67.02.01-1999 describes that if a single process connection cannot be avoided, justification shall be provided to permit its use. The common instrument tap on reactor coolant flow measurement of the US-APWR is justified as follows.

A.5.6.2 Between Safety Systems and Effects of a Design Basis Event

The PSMS is qualified to maintain its functional capability during and after a design basis earthquake. The PSMS is protected against other design basis events by other plant structures.

A.5.6.3 Between Safety Systems and Other Systems

A.5.6.3.1 Interconnected Equipment

There are no components that are common to the PSMS and PCMS/DAS, with the exception of shared sensors, and specific signals interfaced from the PCMS to the PSMS. The SSA described in Section 4.2.5a ensures the shared sensors cannot result in adverse control protection interaction. The use of shared sensors between the PSMS and DAS is justified in Section 7.2.5 and Appendix B of MUAP-07006. The PCMS signals that are interfaced to all redundant divisions of the safety systems are justified in Appendix D.

For other safety and non-safety sensors there are no shared instrument sensing lines or taps.

Fiber optic cables provide inherent isolation for electrical faults. No special testing is required to demonstrate this isolation capability.

A.5.6.3.2 Equipment in Proximity

Non-safety wiring is separated from safety-related wiring or separated with barriers, in accordance with RG 1.75 and IEEE Std 384. Where separation distances are less than those suggested by RG 1.75 and IEEE Std 384, plant licensing documentation references analysis or tests that justify the adequacy of the wiring routing.

A.5.6.3.3 The Effects of a Single Random Failure

There are no single failures that can result in a design basis event concurrent with preventing proper action of any portion of the PSMS. Although sensors are shared between the PCMS and PSMS, the PCMS Signal Selection Algorithm prevents erroneous control system actions due to single sensor failures. So if a shared sensor were to fail, one train of the PSMS is degraded, but there would be no resulting design basis event that would require protective action.

A.5.6.4 Detailed Independence Criteria

IEEE Std 384-1981, Regulatory Guide 1.75

Cables of one train are run in a separate raceway and physically separated from cables of other trains. Group N raceways are separated from safety groups A, B, C and D. Raceways from Group N are routed in the same areas as the safety groups according to spatial separation stipulated in Regulatory Guide 1.75-2005 and IEEE Std 384-1992

The exceptions to the guidance in Regulatory Guide 1.75 are based on test results used to support exceptions to the separation guidance for operating nuclear power plants.

Non-Class 1E circuits are electrically isolated from Class 1E circuits, and Class 1E circuits from different separation groups are electrically isolated. Isolation is by qualified isolation devices, shielding and wiring techniques, physical separation (in accordance with Regulatory Guide 1.75 for circuits in raceways), or an appropriate combination thereof.

When isolation devices are used to isolate Class 1E circuits from non-Class 1E circuits, the isolation devices are identified as Class 1E and are treated as such. Beyond the isolation device(s) these circuits are identified as non-Class 1E and are separated from Class 1E circuits in accordance with the above separation criteria.

A.5.7 Capability for Test and Calibration

Testing from the sensor inputs of the PSMS through to the actuated equipment is accomplished through a series of overlapping sequential tests. The majority of the tests are conducted automatically through self-diagnosis. Most remaining manual tests may be performed with the plant at full power. Manual and automatic tests are described in Section 4.4.

The functional integrity including OR/AND logic, bistable function, etc. of the PSMS software is confirmed by the Memory Integrity Check, and confirmed diversely by the self-diagnostic function. These tests preclude the need to perform manual functional tests for each logic, bistable, etc. The integrity of the software within each PSMS controller, and the integrity of the software in the MELTAC engineering tool (to which the controller software is compared), is maintained by the software configuration management program.

The test frequency for manual tests is based on a reliability analysis. This analysis demonstrates the need to conduct manual tests for PSMS equipment no more frequently than once per 24 months, which is no more than once per fuel cycle. Therefore conducting manual tests for PSMS equipment on-line or off-line, during refueling shutdown, is at the discretion of the plant owner.

A.5.8 Information Displays

A.5.8.1 Displays for Manually Controlled Actions

There are no manually controlled actions credited in the plant safety analysis. All actions credited for accident mitigation are automated. Any exception to this is described in the US-APWR DCD Subsection 7.5.1.5.

Should manual actions be required by the safety analysis the safety VDUs provide the following HSI functions:

- Plant process indications that would lead operators to take those actions
- Required manual controls
- Indications to confirm the manual controls have been executed (i.e., component status feedback)

The operational VDUs provide the following HSI functions:

- Plant process indications that would lead operators to take those actions
- Prompting alarms
- Indications to confirm the effectiveness of the manual control actions

The HSI Topical Report, MUAP-07007 provides a description of all PCMS HSI functions.

A.5.8.2 System Status Indication

The actuation of a protective action is indicated at the train level and component level by the PCMS using data received from the PSMS.

The following information is generated by the PSMS for display by the PCMS:

- Parameter values that lead to trip/actuations
- Pre-trip and trip alarms signals indicating status of partial trip signal paths
- Status indication for system level actuation signal paths and train level actuation signal paths
- Actuated equipment status – This status is displayed at the component level and also at the train level. Train level displays use logic to show the successful or unsuccessful actuation of all required components.

In addition, the safety VDU provides actuated equipment status at the component level.

A.5.8.3 Indication of Bypasses

The PSMS provides the operator with indications of bypassed status, as described in Section 4.2.5 b. The display of the status information for RPS and ESFAS allows the operator to identify the specific bypassed functions, and to determine if the trip/actuation logic has reverted to a condition that accommodates the inoperable equipment (i.e., 2-out-of-3, 2-out-of-2, and 1-out-of-2). In addition to the status indication, an alarm is sounded in the MCR if more than one bypass is attempted for a given protection function.

SDCV indications for each train are automatically provided for inoperable or bypassed conditions that adversely affect the function of the train. SDCV indications can also be manually actuated for conditions that are not automatically monitored. For example, for unmonitored components, such as hand-wheel valves, the component’s status is manually entered in the PCMS data base. The component status is displayed on operational VDU displays. In addition, if that status adversely affects the operability of the train, the train level SDCV indication is automatically activated. The train level SDCV indication can also be manually actuated directly for other unexpected conditions that may have no manual data entry capability in the PCMS data base.

A.5.8.4 Location of Displays

All PSMS controls and indications are located on the Operator Console or the Remote Shutdown Console. These consoles are ergonomically designed for easy operator access to information and controls. Displays for normally used operational VDUs include controls and associated information and alarms. Safety VDUs, which provide backup HSI, normally provide information displays. Screen navigation is required to switch to control displays. The indications and alarms on the MCR Large Display Panel are easily viewable from the operational VDUs, safety VDUs, or conventional system level PSMS controls.

Detailed descriptions of the HSI are provided in the HSI Topical Report.

A.5.9 Control of Access

The PSMS controllers and I/O are located within cabinets with key locks. Cabinet doors are expected to be normally locked. Each train of PSMS cabinets is expected to be located in physically separate equipment rooms that are also accessible only with the appropriate security access (e.g., key or security card). The US-APWR DCD Section 13.6 describes the security system and physical arrangement.

Access to controls within the PSMS cabinets is required to access any controls that can disable or change the functional configuration of the system. This includes access to setpoint adjustments, channel calibration adjustments, test points, and software change points.

A.5.10 Repair

The PSMS facilitates the recognition, location, replacement, repair and adjustment of malfunctioning components or modules. The built-in diagnostics, along with the operational VDU alarms and MELTAC engineering tool provide a mechanism for rapidly identifying and locating malfunctioning assemblies.
Channel bypass permits replacement of malfunctioning sensors or PSMS components, without jeopardizing plant availability, and while still meeting the single failure criterion.

A.5.11 Identification

Equipment within each redundant train of the PSMS has distinct color coded labels. Cabinets are marked on their exterior with labels clearly visible from cabinet entry doors. Equipment, within a cabinet, that is the same train as the cabinet marking, is not marked. However, any equipment that is not the same train as the cabinet marking, is marked to show its different train assignment. For cabinets or control panels that contain multiple trains of equipment, such as the Operator Console, all PSMS equipment is distinctly marked by train. Non-cabinet mounted PSMS equipment, such as the RSC and Transfer Switch Panel are also marked.

The US-APWR DCD Subsections 7.1.3.19 describes distinct train color coding for labels and name tags.

In accordance with IEEE Std 494, PSMS end-user documentation is identified “Nuclear Safety Related”. End-user documentation includes:

(1) Drawings such as instrument diagrams, functional control diagrams, one line diagrams, schematic diagrams, equipment arrangements, cable and tray lists, wiring diagrams
(2) Instrument data sheets
(3) Design specifications
(4) Instruction manuals
(5) Test specifications, procedures, and reports
(6) Device lists

A.5.12 Auxiliary Features

The PSMS is built on the digital platform described in the MELTAC Platform Technical Report. All components of this platform, with the exception of the MELTAC engineering tool personal computer, are safety-related and conform to the requirements for safety systems. Other auxiliary features such as electrical power sources and building HVAC are described in the US-APWR DCD Subsection 7.1.1.10, Chapters 8 and 9.

The PSMS includes safety functions such as reactor trip and ESF actuation. It also includes the following associated non-safety functions:

- Alarm signal generation
- Indications for RG 1.97 Rev.4 Type D variables
- Indications for system actuation status
- Cabinet temperature monitoring
- Door open monitoring
- Input power monitoring

These associated non-safety functions are not isolated from the PSMS. Therefore they are considered part of the safety-related system.

A.5.13 Multi-Unit Stations

There is no sharing of PSMS components between units.

A.5.14 Human Factors

The Human Factors Engineering program applied to the PSMS functions is described in the HSI Topical Report.

A.5.15 Reliability

The PSMS reliability is used in the Probabilistic Risk Assessment (PRA). That analysis is described in the US-APWR DCD Chapter 19, and MUAP-07030 Attachments 6A.12 and 6A.13. The component level reliability which is the basis for the PRA analysis is described in the MELTAC Platform Technical Report, MUAP-07005. The system level reliability method which is the basis for the PRA analysis is described in Section 6.5.2.

A.5.16 Common Cause Failure (IEEE 603-1998)

The following features of the PSMS minimize the potential for Common Cause Failure:

- Isolation of redundant trains
- Conformance to the single failure criterion
- Equipment qualification to preclude external influence
- A digital platform with many years of operation in nuclear power applications
- Simple deterministic software processing
- Graphic based software design tools
- Graphic based maintenance tools for calibration, test and repair
- Segmentation of diverse reactor trip functions into separate RPS controllers (discussed in more detail below)
- A rigorous design process for systems, software and hardware that meets the requirements for safety-related systems
- A rigorous independent Verification and Validation process that meets the requirements for safety-related systems

For each design basis accident addressed in the plant safety analysis, two diverse parameters are used to detect the event and initiate protective actions. These diverse parameters are processed in two separate Controller Groups within each train of the RPS. Table 7.2-5 described in DCD Chapter 7 shows examples of this diversity.

Table A.5.16-1 Deleted.

The plant safety analysis describes the two parameters and how they are credited in the safety analysis.

The two diverse parameters are monitored by two separate sensors which interface to two separate digital controllers within the RPS. The two controllers each process these inputs through diverse application programs to generate reactor trip and/or ESF actuation signals. This two fold diversity is duplicated in each redundant RPS train. The processing of diverse parameters results in functional redundancy within each RPS train. This functional redundancy helps to minimize the potential for CCF.

A.6. Sense and Command Features - Functional and Design Requirements

The Sense and Command Features of the safety system are encompassed by the PSMS, including the RPS, ESFAS, SLS and Safety-Related HSI System.

A.6.1 Automatic Control

The PSMS is designed to automatically initiate reactor trip and actuate the engineered safety features necessary to mitigate the effects of anticipated operational occurrences and design basis accidents. The PSMS automatically initiates appropriate safety functions whenever a variable measured by the PSMS reaches a trip or actuation setpoint. The earliest operator actions are not required for certain time period defined in the safety analysis. Any exception to this is described in the US-APWR DCD Subsections 7.5.1.5.

A.6.2 Manual Control

Manual initiation of reactor trip is provided at the train level. Manual initiation of ESF is also provided at the train level. Conventional switches are provided for use as a manual backup to the automatic protection signals provided by the PSMS. Manual initiation of a protective function performs all actions performed by automatic initiation, such as providing the required action sequencing functions and interlocks.

Manual initiation of reactor trip bypasses all PSMS controllers, as shown in Figure A.6.2-1. Manual initiation of ESF bypasses the RPS controllers as shown in Figure A.6.2-1. Manual initiation depends on the operation of the minimum of equipment and, once initiated, proceeds to completion unless deliberate operator intervention is taken. No single failure in either the automatic portion, manual portion, or shared portion prevents manual or automatic initiation of a protective function at the train level. This capability is achieved through the redundant structure of the PSMS.

Redundant manual controls and indications are also provided by redundant PSMS trains to maintain safe stable plant conditions after the protective actions are completed. In addition, the PSMS provides redundant manual controls and indications to achieve and maintain safe shutdown.

All manual controls and indication discussed above are located in the MCR and are easily accessible to the operator. Manual controls and indications to achieve safe shutdown are also located on the Remote Shutdown Console.

Figure A.6.2-1 Manual Control

A.6.3 Interaction between the Sense and Command Features and Other Systems

Certain information derived from PSMS channels is used by the PCMS to control the plant. This reduces the number of penetrations into critical pressure boundaries, such as into the reactor coolant loops, pressurizer and steam generators (SGs). It also helps reduce congestion and enhance separation.

A control system Signal Selection Algorithm within the PCMS is used so that a malfunctioning PSMS channel does not cause the control system to take erroneous control actions that would result in a challenge to the PSMS. Therefore, where protection signals are used for control, functional isolation is provided between the control and protection systems.

A.6.4 Derivation of System Inputs

To the extent feasible and practical, protection system inputs are derived from signals that are direct measures of the desired variables. The PSMS calculates some variables where direct measurement is not feasible. These are the thermal over temperature delta-T reactor trip and the overpower delta-T reactor trip. Direct process measurements for protective actions and algorithms for calculated functions are described in the US-APWR DCD Subsection 7.2.1.

A.6.5 Capability for Testing and Calibration

Input sensors from each PSMS are compared continuously in the PCMS to detect abnormal deviations. This comparison occurs after the analog to digital conversion in the PSMS so it also checks the accuracy of PSMS components. PSMS sensors are periodically stimulated to calibrate the sensor for expected time dependent drift. The readout for this calibration also occurs after the analog to digital conversion in the PSMS, so it also checks the accuracy of PSMS components.

The PSMS facilitates the diagnosis, location, and repair or adjustment of malfunctioning components.

A.6.6 Operating Bypasses

Test and maintenance bypasses are described in Section A.6.7. Several Operating Bypasses are described in this section.

- Some Operating Bypasses automatically block certain protective actions that would otherwise prevent modes of operations such as start-up. These Operating Bypasses are automatically initiated separately within each PSMS train when the plant process permissive condition is sensed by the PSMS input channel(s). Automatically initiated Operating Bypasses are described in the US-APWR DCD Subsections 7.2.1.6 and 7.3.1.6.

Other Operating Bypasses must be manually initiated. These Operating Bypasses can be manually initiated separately within each PSMS train when the plant process permissive condition is sensed by the PSMS input channel(s). Manually initiated Operating Bypasses are described in the US-APWR DCD Subsection 7.1.3.11. These bypasses may be manually initiated from the S-VDU or O-VDU. To manually initiate an Operating Bypass from the O-VDU the Bypass Permissive for the train must be enabled.

All Operating Bypasses, either manually or automatically initiated, are automatically removed when the plant moves to an operating regime where the protective action is required if an accident occurred. Status indication is provided in the control room for all Operating Bypasses.

A.6.7 Maintenance Bypass

These bypasses may be manually initiated from the S-VDU or O-VDU. To manually initiate a Maintenance Bypass from the O-VDU the Bypass Permissive for the train must be enabled.

a. Input Channel Bypass

The safety system is designed to permit the unrestricted bypass for maintenance, test, or repair of any one protection input channel in the group of channels monitoring a selected variable. This bypass is accomplished during power operation without causing initiation of a protective function. The system also meets the single failure criterion while permitting power operation for an indefinite period of time with one channel of the selected variable bypassed. Indication is provided in the control room if some part of the system has been administratively bypassed or taken out of service.

With one channel bypassed, the RPS does not permit the bypass of a second channel in the group monitoring the same variable. An attempt to apply multiple bypasses is blocked, and trip/actuation is not triggered by the attempt.

Except for two channel function, there are four protection channels for each actuation function. Accident and reliability analyses assume that one of these channels is in the bypass mode at the time of the accident. This assumption precludes potential limitations that might have otherwise been placed on the use of the bypass feature.

For each input, the technical specifications limit the period allowed for two channels to be out of service (i.e., either two failed in a non-trip state or one in bypass and one failed in a non-trip state). The time specified in the technical specifications is supported in the probabilistic and risk insights considering the probability of the event and the significance of the input to event mitigation.

b. Train Level RPS Bypass

Each RPS train takes inputs from one or more input process sensors, performs compensation or other calculation which terminates in one or more bistable functions where the process variable is compared against setpoints. The coincidence logic portion of the RPS receives the partial trip outputs from these comparisons and combines them with the partial trip status of the other channels to initiate a reactor trip or ESF actuation.

Each RPS train has the ability to bypass all partial trip input signals from the other trains. This function is useful if an entire RPS train is taken out of service. When an entire RPS train is bypassed each individual channel for that train is bypassed and therefore subject to the alarms and interlocks described above for individual input channels. Therefore, if input channels are previously bypassed the RPS train level bypass may be blocked or alarmed. In the same manner, if an RPS bypass is already active, any attempt to put additional input channels in bypass is alarmed / blocked.

There are four RPS channels for each ESF actuation function. Accident and reliability analyses assume that one of these channels is in the bypass mode at the time of the accident. This assumption precludes potential limitations that might have otherwise been placed on the use of the bypass feature.

For each ESF actuation function, the technical specifications limit the period allowed for an RPS train to be bypassed or out of service. The time specified in the technical specifications is determined by considering the degree of redundancy provided for the function and the importance of the function.

A.6.8 Setpoint

A.6.8.1 Setpoint Uncertainties

Three values applicable to reactor trip and ESF actuations are specified:

- Safety limit
- Allowable value
- Nominal trip setpoint

The safety limit is the value assumed in the accident analysis and is the least conservative value.

The allowable value is the Technical Specification value and is obtained by subtracting the unmeasurable channel uncertainties from the safety limit. The method used for combining all process measurement effects to determine the unmeasurable process measurement uncertainty is described in Section 6.5.4.
The nominal trip setpoint is the value set into the equipment and is obtained by adding or subtracting the total channel uncertainties (unmeasurable and measurable) plus a safety margin, from the safety limit. The minimum safety margin allows for the normal expected measurable instrument loop drift between calibration intervals, such that the Technical Specification allowable value is not exceeded for normally operating equipment. The method used for combining all uncertainties in a process loop to determine the resulting total channel uncertainty and the method for determining the normally expected instrument loop drift between calibration intervals is described in Section 6.5.4.

As described above, allowance is made for process uncertainties, instrument error, instrument drift, and calibration uncertainty to obtain the nominal trip setpoint value that is actually set into the equipment. The only requirement on the instrument's accuracy is that, over the instrument span, the error must always by less than or equal to the error value allowed in the accident analysis. The instrument does not need to be the most accurate at the setpoint value as long as it meets the minimum accuracy requirement. The accident analysis accounts for the expected errors at the actual setpoint.

A.6.8.2 Multiple Setpoints

Multiple trip setpoints are used for some reactor trip parameters. Some of these trip setpoints are automatically enabled or disabled based on setpoints for other plant parameters which are indicative of different modes of plant operation. These plant mode monitoring parameters provide positive means to ensure that the more restrictive trip setpoint is used.

Other trip setpoints are manually enabled or disabled based on administrative controls. To manually disable a setpoint a permissive interlock must be reached. This interlock can be based on the same process parameter or an alternate process parameter. If the interlock permissive condition is no longer satisfied the manually disabled setpoint is re-enabled.

The hardware and software used to prevent improper use of less restrictive trip settings are considered part of the PSMS.

Parameters with multiple setpoints that are automatically or manually disabled are described in the US-APWR DCD Subsections 7.2.1.6.1, 7.2.1.6.2, 7.3.1.6.2, and 7.3.1.6.3.

A.7. Executive Features - Functional and Design Requirements

The Execute Features of the safety system include the Reactor Trip Breakers, the breakers and motor starters for ESF components and all ESF components (e.g., pumps, valves etc.). The Sense and Command Features of the Safety System, which are encompassed by the PSMS, actuate these Execute Features. The Reactor Trip Breakers are actuated directly by the PSMS. Some plant components are also actuated directly by the PSMS, such as solenoid operated valves. Other plant components, such as pumps and motor operated valves, are actuated by the PSMS via breakers and/or motor starters.

A.7.1 Automatic Control

The Execute Features respond to control signals from the PSMS. The PSMS output signals may be the result of automatic or manual control signals. The priority between automatic and manual controls, and between manual controls at different operating locations is based on logic that resides within the PSMS.

A.7.2 Manual Control

Manual controls that are an integral part of the Execute Features include conventional control switches located on breakers or motor starters, or in proximity to plant process components. These are referred to as Execute Feature Manual Controls. These manual controls are provided for maintenance of the plant process component. The Execute Feature Manual Controls are not part of the PSMS (i.e., the Sense and Command Features). These manual controls are not required for any design basis event, including safe shutdown from outside the MCR.

During normal operation, the Execute Feature Manual Controls are in a passive state which allows automatic/manual controls from the PSMS to control the plant component. If an Execute Feature Manual Control is activated it will block or override control from the PSMS. Should this occur, the component is considered inoperable and appropriate train level inoperable indications are provided in the MCR, as described in Section A.4.11, above. The Execute Feature Manual Controls are located in security controlled access areas, or behind key locked cabinet doors.

A.7.3 Completion of Protective Action

Once actuated circuit breakers inherently remain in their actuated position. A deliberate opposite control signal is needed to reposition the breaker. This applies to the reactor trip breakers and breaker controlled plant components. Therefore when a breaker is actuated (open or close) from the PSMS, the protective action inherently goes to completion and the component remains in its position when the protective action signal is removed.

Motor-starters, motor-operated valves and solenoid valves also inherently remain in their actuated position, if the actuated position is the de-energized position. If the PSMS requires the component to energize for the protective action, the component will respond to the PSMS, but will reposition to its deenergized state, when the PSMS actuation signal is removed. Therefore, the SLS component level logic latches the train level protective action signal from the ESFAS to ensure the component remains in its protective action position when the train level ESFAS signal is removed. A deliberate automatic or manual control action is required to unlatch the SLS control logic.

It is noted that once travel for a motor-operated valve is completed, the valve will remain in its position even after the PSMS control signal is removed. A deliberate automatic or manual control action is required to reposition a motor-operated valve.

A.7.4 Operating Bypass

There are no Operating Bypasses in the Execute Features.

A.7.5 Maintenance Bypass

The Execute Feature Manual Controls, discussed above, may be considered Maintenance Bypasses. These controls have access controls. In addition, if Execute Feature Manual Controls disable a safety system, plant administrative controls ensure this occurs in only one train at a time. Plant Technical Specifications limit the amount of time plant systems may be in an inoperable condition.

A.8. Power Source Requirements

Power sources for PSMS are described in the US-APWR DCD Subsection 7.1.1.10 and Chapter 8.

Appendix B Conformance to IEEE 7-4.3.2 -2003

This appendix describes conformance of the digital PSMS to the requirements of IEEE Std 7-4.3.2. The section numbers follow the sections in IEEE Std 7-4.3.2. All sections pertain to the 2003 version of this standard unless specifically noted.

B.1. Scope

This conformance section addresses the computer portions of the PSMS.

B.2. References

The PSMS conforms to all referenced standards, as explained below.

B.3. Definitions and Abbreviations

The definitions are applicable to the PSMS.

B.4. Safety System Design Basis

No requirements beyond IEEE Std 603-1998 are necessary.

B.5. Safety System Criteria

B.5.1 Single Failure Criterion

No requirements beyond IEEE Std 603-1998 are necessary.

B.5.2 Completion of Protective Action

No requirements beyond IEEE Std 603-1998 are necessary.

B.5.3 Quality

B.5.3.1 Software Development

The software development process for the PSMS application software is described in the US-APWR SPM (Reference 10).

B.5.3.1.1 Software Quality Metrics

The process for establishing software quality metrics for the PSMS application software is described in the US-APWR SPM (Reference 10).

B.5.3.2 Software Tools

The software tools are described in the MELTAC Platform Technical Report, MUAP-07005. The use of these tools for developing application software is described in the US-APWR SPM (Reference 10).

B.5.3.3 Verification and Validation

The verification and validation for the digital platform software is described in the MELTAC Platform Technical Report, MUAP-07005. The verification and validation for the system application software is described in the US-APWR SPM (Reference 10).

B.5.3.4 Independent V&V (IV&V) Requirements

The independent verification and validation requirements for the digital platform software are described in the MELTAC Platform Technical Report, MUAP-07005. The basic organization of independent verification and validation for the safety-related I&C system is described in the US-APWR SPM (Reference 10).

B.5.3.5 Software Configuration Management

The software configuration management for the digital platform software is described in the MELTAC Platform Technical Report, MUAP-07005. The software configuration management for the system application software is described in the US-APWR SPM (Reference 10).

B.5.3.6 Software Project Risk Management

The software project risk management for the digital platform software is described in the MELTAC Platform Technical Report, MUAP-07005. The software project risk management for the system application software is controlled by software life cycle process activities described in the US-APWR SPM (Reference 10).

B.5.4 Equipment Qualification

B.5.4.1 Computer System Testing

The computer system testing for the digital platform software is described in the MELTAC Platform Technical Report, MUAP-07005.

B.5.4.2 Qualification of Existing Commercial Computers

There are no commercial computers in the PSMS.

B.5.5 System Integrity

B.5.5.1 Design for Computer Integrity

The computer integrity for the digital platform software is described in the MELTAC Platform Technical Report, MUAP-07005. The computer integrity for the system application software is described in the US-APWR SPM (Reference 10).

B.5.5.2 Design for Test and Calibration

The design for test and calibration for the system application software is described in Section 5.1.9.

B.5.5.3 Fault Detection and Self-Diagnostics

The fault detection and self-diagnosis is described in the MELTAC Platform Technical Report, MUAP-07005.

B.5.6 Independence

The methods used to ensure independence between computers in different trains and between computers in safety-related and non-safety systems are described in Section 4.2.5. The methods include:

a. Electrical Independence
Data communications between computers in different trains or between safety-related and non-safety computers are transmitted through fiber optic cables. The fiber optic cables provide inherent isolation for electrical faults.

b. Data Processing Independence
The PSMS employs communication processors that are separate from the processors that perform safety-related logic functions. The safety-related processors and communication processors communicate via dual ported memory. This ensures there is no potential for communications functions, such as handshaking, to disrupt deterministic safety function processing.

c. No Ability to Transfer Unpredicted Data
There is no file transfer capability in the PSMS. Only predefined communication data sets are used between the PSMS trains and between the PSMS and PCMS. Therefore any unknown data is rejected by the PSMS.

d. No Ability to Alter Safety Software
The software in the PSMS cannot be changed through the communication interface between PSMS trains or the communication interface for the PCMS or the communication interface for the MELTAC engineering tools. The PSMS application software is changeable only through a hardwired connection to the software memory device, which can only be made when the CPU module is removed from the MELTAC controller. The PSMS basic software can only be changed by physically replacing the software memory device, which can only be done when the CPU module is removed from the MELTAC controller.

e. Deleted

The following additional design features are specific to the interface between operational VDUs in the PCMS and the PSMS.

f. Acceptable Safety Function Performance
Signals from the PCMS are enabled or disabled in the communication processors through manual controls on the safety VDUs. Therefore the safety VDU can be used to block any spurious non-safety controls from the PCMS. In addition, the logic in the SLS blocks non-safety signals from the PCMS when any safety function signal is present, such as ESF actuation signal, interlock signal important to safety or manual control signal from the safety VDU.

g. Failures of Non-Safety Systems are Bounded by the Safety Analysis

Any plant condition created by the worst case erroneous/spurious non-safety data set (e.g., non-safety failure commanding spurious opening of a safety relief valve) is bounded by the plant safety analysis. This analysis is based on spurious communication of a single data set (i.e., one erroneous control command) because spurious communication of multiple erroneous control commands is not considered credible. The basis for this credible failure mode is described in Appendix C.

Figure B.5.6-1 Software Isolation (Non-Safety VDU / Safety-Related System)

B.5.7 Capability for Test and Calibration

No requirements beyond IEEE Std 603-1998 are necessary.

B.5.8 Information Displays

No requirements beyond IEEE Std 603-1998 are necessary.

B.5.9 Control of Access

No requirements beyond IEEE Std 603-1998 are necessary.

B.5.10 Repair

No requirements beyond IEEE Std 603-1998 are necessary.

B.5.11 Identification

The identification for the digital platform software is described in the MELTAC Platform Technical Report, MUAP-07005. The identification for the system application software is described in the US-APWR SPM (Reference 10).

B.5.12 Auxiliary Features

No requirements beyond IEEE Std 603-1998 are necessary.

B.5.13 Multi-Unit Stations

No requirements beyond IEEE Std 603-1998 are necessary.

B.5.14 Human Factors

No requirements beyond IEEE Std 603-1998 are necessary.

B.5.15 Reliability

The reliability for the digital platform is described in the MELTAC Platform Technical Report. The reliability method for the system is described in Section 6.5.2.

B.6. Sense and Command Features - Functional and Design Requirements

No requirements beyond IEEE Std 603-1998 are necessary.

B.7. Executive Features - Functional and Design Requirements

No requirements beyond IEEE Std 603-1998 are necessary.

B.8. Power Source Requirements

No requirements beyond IEEE Std 603-1998 are necessary.

Appendix C Prevention of Multiple Spurious Commands and Probability Assessment

C.1. Prevention of Multiple Spurious Commands

C.2. Probability Assessment

Figure C.2-1 Probability Assessment Flow

Appendix D Analysis of Operational VDU (O-VDU) and PCMS Spurious Commands

Appendix E Conformance to ISG-04

This Appendix E describes conformance of the interdivisional communication design in the US-APWR PSMS to Staff Positions of DI&C-ISG-04. The section numbers in this Appendix E follow the section numbers in DI&C-ISG-04. All sections pertain to DI&C-ISG-04 “Task Working Group#4: Highly-Integrated Control Rooms – Communications Issues (HICRs), Interim Staff Guidance, Revision 1”.

The following two types of interdivisional communication designs are applied to the US-APWR safety-related I&C architecture, and the conformance analyses are separately performed for both of the following two application types.

Figure E-1 Component Control Signal Interface from Operational VDU to Safety-Related System

Figure E-2 Operational/Maintenance Bypass, Reset and Lock Signal Interface from Operational VDU to Safety-Related System

Appendix F Safety-Related Digital I&C Design Detail Conformance to Essential Safety Criteria

Figure F.1-1 Independence Design of RPS

Figure F.1-2 Communication Independence Design among Different Train RPS

Figure F.1-3 Communication Independence Design from RPS to Unit Bus

Figure F.1-4 Overall Signal Interfaces of 2-out-of-4 Bypass Logic

Figure F.1-5 MELTAC Platform Basic Software Processes and Execution Order

Figure F.2-1 Independence Design of ESFAS

Figure F.2-2 Independence Design of SLS

Figure F.2-3 Independence Design of COM

Figure F.2-4 Independence Design of Safety VDU

Figure F.2-5 Communication Independence Design from RPS to ESFAS

Figure F.2-6 Communication Independence Design from COM-1 to Unit Bus

Figure F.2-7 Communication Independence Design from Unit Bus to COM-2

Figure F.2-8 Communication Independence Design between Safety VDU Trains

Table F.2-1 Signal List and Functional Independence Design from Operational VDU to PSMS

Table F.2-2 Deleted

Appendix G The Failure Modes and Effects Analyses (FMEA) for PSMS

Figure G.1-1 System Configuration for FMEA of RT and ESF Actuation in PSMS

Table G.2-1 FMEA for RT in PSMS (for Figure G.1-1)
(Sheet 1 of 9)

Table G.2-1 FMEA for RT in PSMS (for Figure G.1-1)
(Sheet 2 of 9)

Table G.2-1 FMEA for RT in PSMS (for Figure G.1-1)
(Sheet 3 of 9)

Table G.2-1 FMEA for RT in PSMS (for Figure G.1-1)
(Sheet 4 of 9)

Table G.2-1 FMEA for RT in PSMS (for Figure G.1-1)
(Sheet 5 of 9)

Table G.2-1 FMEA for RT in PSMS (for Figure G.1-1)
(Sheet 6 of 9)

Table G.2-1 FMEA for RT in PSMS (for Figure G.1-1)
(Sheet 7 of 9)

Table G.2-1 FMEA for RT in PSMS (for Figure G.1-1)
(Sheet 8 of 9)

Table G.2-1 FMEA for RT in PSMS (for Figure G.1-1)
(Sheet 9 of 9)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G.1-1)
(Sheet 1 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G.1-1) (Sheet 2 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G.1-1)
(Sheet 3 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G.1-1)
(Sheet 4 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G.1-1)
(Sheet 5 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G.1-1)
(Sheet 6 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G.1-1)
(Sheet 7 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G.1-1)
(Sheet 8 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G.1-1)
(Sheet 9 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G.1-1)
(Sheet 10 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G.1-1)
(Sheet 11 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G.1-1)
(Sheet 12 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G.1-1)
(Sheet 13 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G.1-1)
(Sheet 14 of 25)

**Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G.1-1)
(Sheet 15 of 25)**

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G.1-1)
(Sheet 16 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G.1-1)
(Sheet 17 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G.1-1)
(Sheet 18 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G.1-1)
(Sheet 19 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G.1-1)
(Sheet 20 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G.1-1)
(Sheet 21 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G.1-1) (Sheet 22 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G.1-1) (Sheet 23 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G.1-1)
(Sheet 24 of 25)

**Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G.1-1)
(Sheet 25 of 25)**

Appendix H Bases for the Selection of the US-APWR PAM Variables

This appendix describes the selection basis of the US-APWR PAM variables. The US-APWR PAM design is discussed in DCD Section 7.5, and PAM list is provided in DCD Table 7.5-3.

Many current operating plants in the US have developed their PAM lists based on the prescriptive list provided in RG 1.97 Rev. 3. However, the more recent guidance intended for new reactors in RG 1.97 Rev. 4 is based on the performance-based approach identified in IEEE Std 497-2002 which is endorsed by RG 1.97 Rev.4. MHI developed the PAM list based on the guidance in RG 1.97 Rev. 4 and IEEE Std 497-2002.

IEEE Std 497-2002 identifies the plant's emergency operating procedures (EOPs) and abnormal operating procedures (AOPs) as sources for determining the required PAM variables for some types of parameters. Typically, the EOPs are derived from an approved set of emergency response guidelines (ERGs). In the case of MHI, the PAM list was developed prior to the existence of an approved set of ERGs for the US-APWR. Therefore, MHI could not use these documents as sources during the development of the PAM list. Instead, MHI utilized the design information in the US-APWR DCD as the primary source material for developing the PAM list following the performance-based criteria in IEEE Std 497-2002.

In addition, MHI utilized Japanese domestic and US operational experience and emergency procedures, and known differences between current operating plants and the US-APWR design to further refine the PAM list and to ensure it was a complete PAM list for the US-APWR. Since this method is slightly different than the method that is described in RG 1.97 Rev. 4, it is possible that it will be viewed as an alternate method. The selection basis for the Type A, B, C, D, and E variables for the US-APWR are described in detail in the sections below.

As an additional confirmation of the adequacy of the US-APWR PAM list, MHI has performed a comparison of the US-APWR PAM list to the generic list of PAM instrumentation in RG 1.97 Rev. 3. For each of the PAM variable types, MHI has identified the differences between the two lists and provided an explanation of these differences.

H.1 Type A Variables

MHI utilized by the performance-based criteria of RG 1.97 Rev. 4 and IEEE Std 497-2002 to select the Type A accident monitoring variables for the US-APWR. IEEE Std497-2002 defines Type A variables as follows.

> Type A variables are those variables that provide the primary information required to permit the control room operating staff to:
>
> a) Take specific planned manually-controlled actions for which no automatic control is provided and that are required for safety-related systems to perform their safety functions as assumed in the plant Accident Analysis Licensing Basis.
>
> b) Take specific planned manually-controlled actions for which no automatic control is provided and that are required to mitigate the consequences of an AOO.

As described above, the Type A variables are based on manual actions. DCD Chapter 15 (the Accident Analysis Licensing Basis) does credit manual operator actions for some accidents. Therefore, any variables that provide information for the operators to perform those credited manual actions would meet the definition of criterion “a” above. The basis for the manual operator action is discussed in DCD Chapter 15 in the relevant section for each of the events that credit a manual action. These credited manual actions are summarized in DCD Table 7.5-5.

Each of the credited manual actions is listed and described below according to the Chapter 15 event.

Inadvertent Decrease in Boron Concentration in RCS (Subsection 15.4.6)
This event is a boron dilution and is classified as an AOO. After the boron dilution begins, the decrease in boron concentration will result in an increase in reactivity. Depending on the Technical Specification Mode of operation that the plant is in at the time of the event, there are different alarms available to prompt the operator that a boron dilution is occurring. The available alarms are the control rod insertion limit alarm, the reactor makeup water flow rate deviation alarm, the boric acid flow rate deviation alarm, the high primary makeup water flow rate alarm, and neutron flux alarms. After receiving one or more of these alarms, the operator would implement the appropriate alarm response procedure (ARP). The ARP requires that the operator verify the occurrence of a boron dilution by monitoring the neutron flux (wide range). To prevent a return to criticality, the operator would take action to terminate the boron dilution event by performing one (or more) of the following actions: closing the charging flow isolation valve, closing the primary makeup water control valve, or stopping the primary makeup water pump. The wide range neutron flux is the PAM variable to be used by the operator to confirm the alarm and ensure that the appropriate manual action is taken. Therefore, the wide range neutron flux meets the criteria for a Type A PAM variable. Then the wide range neutron flux is selected as a Type A PAM variable. Note that the analysis in DCD Subsection 15.4.6 seems to “credit” several main control room alarms. However, these alarms are only credited in the context of determining the amount of time between the occurrence of an alarm and the return to criticality as required by SRP 15.4.6. This does not mean that these alarms, or the associated parameters, are credited as the prompt for the actual manual action. The primary indication that would provide the prompt for the specific manual action to terminate the boron dilution is the wide range neutron flux indication as discussed above.

The US-APWR has several types of neutron detectors; therefore, the rationale for selection of wide range neutron flux is as follows. There are two source range neutron flux detectors, two intermediate range neutron flux detectors, four power range neutron flux detectors, and two wide range neutron flux detectors. The detectors are provided individually; the detectors for wide range neutron flux are not shared with those of power range neutron flux, intermediate range neutron flux, or source range neutron flux. Therefore, the input signals to the alarms for power range neutron flux or source range neutron flux are not related to the input signal for wide range neutron flux. DCD Table 15.4.6-1 indicates that high source range neutron flux and high power range neutron flux alarms occur during the boron dilution event for certain modes of operation. The power range neutron flux is useful only in Mode 1 and source range neutron flux is useful in the shutdown Modes. On the other hand, wide range neutron flux has the ability monitor the whole range. Therefore, by selecting wide range neutron flux as the PAM variable, it is not necessary to have separate PAM variables for different Modes. Also, the wide range neutron flux monitors are already qualified for harsh conditions, while the other flux indications may not be. The wide range neutron flux is sufficiently sensitive to detect the flux changes associated with the boron dilution over time and also for monitoring the reactivity critical safety function (see Type B section of this RAI response). The US-APWR ERGs utilize the wide range neutron flux for these purposes.

Since the event is a boron dilution, the RCS boron concentration is an important parameter for the operator to determine during this event. However, RCS boron concentration is only obtained by periodic sampling of the RCS. Sampling requires some time to perform and thus there is some delay between the actual measurement and the time at which the operator would obtain the result. If the operator delays action to confirm the RCS boron concentration, the boron dilution will have progressed even further during the delay. For this reason, monitoring of the RCS boron concentration by the operator is not credited as the basis for terminating the boron dilution event.

Rod Ejection Accidents (Subsection 15.4.8)
As stated in DCD Subsection 15.4.8.2, a rod ejection accident is initiated by the failure of a CRDM housing and results in an increase in core reactivity and a distortion of the local power distribution. The increase in local power near the ejected rod could possibly lead to fuel failure. The event will also result in a loss of reactor coolant to containment. The combination of these effects can result in radiation being released to the containment. If the break flow of RCS coolant caused by the rod ejection is large, the containment pressure will increase to the setpoint for automatic actuation of containment spray. The containment spray will mitigate the radiation levels inside containment. Since containment spray automatically actuates, no manual operator actions are needed. The consequences of this scenario are bounded by the LOCA analyses in DCD Subsection 15.6.5. However, for the case where the break flow rate caused by the rod ejection is smaller, the containment pressure may not reach the setpoint for automatic initiation of containment spray. Since automatic action may not occur, manual action may be required. As a result, the DCD Subsection 15.4.8 analysis assumes manual operator actions to actuate containment spray and the annulus emergency exhaust system within 35 minutes. The operators perform these actions based on the containment high range area radiation indication after the containment high range area radiation alarm is initiated as indicated in DCD Table 7.5-5. In addition, containment radiation is monitored continuously following an accident as part of the plant critical safety functions and containment high range area radiation is selected as a Type B PAM variable (see Type B explanation).

Following the containment high range area radiation alarm, the operator will confirm whether or not the containment high range area radiation is above a certain setpoint. If so, the operator would manually actuate containment spray and the annulus emergency exhaust system. Therefore, containment high range area radiation is selected as a Type A PAM variable.

CVCS Malfunction that Increases Reactor Coolant Inventory (Subsection 15.5.2)
In DCD Chapter 15, this event credited automatic actions rather than manual actions. For this event, no Type A PAM variables are required.

Failure of Small Lines Carrying Primary Coolant Outside C/V (Subsection 15.6.2)
This event concerns the failure of the RCS sample lines or the CVCS letdown line to the demineralizers that results in RCS coolant leakage outside containment. This is a concern because it is a violation of RCS and containment integrity and can result in radiation release to the environment. In the safety analysis in DCD Chapter 15, the RCS sample line failure is the limiting case. The dose analysis in DCD Subsection 15.6.2 credits a manual operator action to isolate the RCS sample line within 45 minutes. The leakage from this line will reduce the water level in the volume control tank (VCT) and require automatic makeup from the CVCS. The frequent operation of the automatic makeup system may be an early indication to the

operator that there may be some leakage in the reactor coolant system. There are also alarms that may provide some early indication of the increase RCS leakage. One such alarm is the low VCT water level alarm. However, the low VCT water level alarm, and its corresponding indication, is not considered to be the prompt for manual operator action. Upon receipt of the VCT low water level alarm the operator would begin to investigate a possible RCS leak. One of the ways this may be investigated is by a mass balance of the reactor coolant system. As indicated in the discussion in Subsection 15.6.2, the flow rate due to the sample line failure is such that the CVCS can maintain the pressurizer water level. Therefore, the operator would not notice any decrease in pressurizer level (which is already selected as a Type A variable). However, in order to maintain the pressurizer level, the CVCS flow rate will increase to the point where the high charging flow rate alarm occurs. This alarm, or the elevated charging rate prior to alarm occurrence, along with the absence of a decrease in pressurizer level, would indicate to the operator that there may be a break in one of the small lines, such as the sample line. In this case, the operator would take action to isolate the leakage by closing the containment isolation valves associated with these small RCS lines. Once the containment isolation valves are closed, the break would be isolated. With the RCS now intact, the need for additional makeup would cease and the charging flow would decrease. The operator could verify the success of the actions by this decrease in the charging flow rate. Once the containment isolation valves are closed, the event is terminated from the perspective of the Subsection 15.6.2 analysis. For these reasons, MHI considers that the charging flow rate indication to be the primary indication that the operator would use to take the manual actions credited in the Chapter 15 safety analysis. Therefore, the charging flow rate indication meets the criteria for Type A PAM variables. The high alarm setpoint for charging flow rate is set to detect this event based on the assumed leakage outside containment. The setpoint is significantly higher than the normal operating flow rate range such that the alarm would not be expected to occur during normal operations. This eliminates the potential for spurious alarms that may desensitize operators and degrade their ability to respond to the line break event in DCD Chapter 15. On the other hand, the setpoint is not set so high as to allow the line break event in DCD Chapter 15 to occur without detection.

Note that the Chapter 15 analysis assumes the maximum break flow from the RCS sample line in order to maximize the coolant released and thus the dose. If a smaller break or leak were to occur from the RCS sample line, the change in charging flow rate would be smaller and possibly more difficult for the operator to observe. However, due to the size of the line, this smaller break or leak would result in RCS leakage that was within the maximum flow rate in the Technical Specifications. Technical Specification 3.4.13 sets limits on the allowable RCS leakage and requires the operator to take actions if the leakage is outside of these limits. Very small leaks that are within the Technical Specification limits do not fall under the scope of the event in Subsection 15.6.2 and do not apply to PAM. The event analyzed in Subsection 15.6.2 results in leakage rates that are above the Technical Specification limits and therefore require the operator actions credited in the analysis. It is also important to note that Technical Specification 3.4.15 requires certain instrumentation to be available to detect RCS leakage. This required instrumentation, which is outside the scope of the PAM criteria, would be available to the operator to help determine the cause and location of the leakage. The indications in Technical Specification 3.4.15 are in-containment indications, such as containment sump level. The Subsection 15.6.2 event results in leakage outside the containment. However, these Technical Specification instruments would still be helpful to the operator as an increased charging flow rate coupled with no increase in containment sump level would indicate leakage outside of containment. The operator may then take action to close the containment isolation valves of the sample line and confirm the isolation of the leak by the reduction in charging flow.

MHI would like to note that the discussion of these other indications (available due to Technical Specifications) that would be helpful to the operator is applicable only to very small breaks. As described previously, detection of these small breaks falls under the Technical Specifications and is outside the scope of the accident analysis in Chapter 15 (and therefore PAM Type A).

In summary, the accident analysis in Chapter 15 assumes maximum break flow at the time of the sample line rupture outside containment. In this condition, a high charging flow alarm is annunciated. After receiving this alarm, the operator would implement the appropriate ARP. The potential leakage path outside containment is limited to the sample and letdown lines. Therefore, when this charging flow alarm is annunciated, prior to determining the location of the break, the isolation of the sample line is performed by closing containment isolation valves according to the procedure. As a result of this operation, the isolation within 45 minutes as described in DCD Susbection 15.6.2 is possible. For these reasons, charging flow is selected as the Type A PAM variable to support the operator action.

Radiological Consequences of a SG Tube Failure (Subsection 15.6.3)
A steam generator tube rupture (SGTR) is a PA that results in leakage of reactor coolant from the primary side to the secondary side of the SG. Due to this primary-to-secondary leakage, the response to an SGTR requires numerous operator actions. The DCD Chapter 15 analysis assumes the specific manual operator actions listed below. For each of these manual actions listed below, the operator needs to monitor various variables prior to performing the action. This meets the criteria for Type A PAM variables. The Type A PAM variables associated with each manually assumed action in the DCD Subsection 15.6.3 analysis are also described below.

- *Manual Reactor Trip* – The primary coolant entering the SG contains radioactive N-16 which is monitored by the high sensitivity main steam line radiation (N-16) monitors which alarm in the main control room. The operators will then enter the steam generator tube leakage ARP. In the DCD Subsection 15.6.3 analysis, this is assumed to occur at 2 minutes after event initiation. In reality, the N-16 alarms are highly sensitive and would occur almost instantly following the SGTR. Therefore, the 2 minute time assumed in Chapter 15 is conservative. The SGTR will result in a decrease in pressurizer water level due to the primary-to-secondary leakage. The amount of the decrease will vary with the size of the tube rupture. The operator will attempt to maintain pressurizer water level using charging flow. However, if pressurizer water level cannot be maintained, then the operator will manually trip the reactor (and actuate SI) and enter the SGTR EOP. Thus, the operator must be able to monitor pressurizer water level to determine whether to manually trip the reactor. DCD Subsection 15.6.3.4.2 describes the decrease in pressurizer water level as an indication of the event. The SGTR accident analysis for DCD Chapter 15 conservatively shows that the low pressurizer water level alarm occurs within 5 minutes of event initiation. The timing of the occurrence of the pressurizer water level alarm (within 5 minutes) supports the manual operator action time of 15 minutes assumed in DCD Chapter 15 and the alarm is included in DCD Table 7.5-5 for the SGTR event. Therefore, pressurizer water level is selected as a Type A PAM variable. Although the N-16 alarm is assumed to provide an earlier indication of the occurrence of the SGTR, it is not the primary indication which causes the operator to manually trip the reactor. In addition, although the N-16 alarm is available to alert the operators to an SGTR, the operators do not actually monitor N-16 radiation to perform any action and therefore N-16 radiation is not required to be a Type A PAM variable. Note that the SGTR break size analyzed in DCD Subsection 15.6.3 is selected as a bounding case. Larger tube ruptures may result in automatic reactor trip setpoints being reached (such as low pressurizer water level or low pressurizer pressure) and therefore may not require this manual operator action. On the other hand, small tube ruptures may not require a manual reactor trip if pressurizer water level can be maintained by normal charging. Either of these cases is less limiting than the DCD case and therefore not applicable to PAM variable selection since they are not part of the accident analysis licensing basis.

- *Identify and Isolate Ruptured SG* – The next manual operator actions to perform are to first identify and then isolate the ruptured SG. There are several means available to identify the ruptured SG. The primary-to-secondary leakage will result in an increase in the water level in the ruptured SG. Following reactor trip, the main feedwater to all of the SGs will be automatically isolated (on low T_{avg}). When feedwater is isolated, the water levels in the intact SGs will level off whereas the water level in the ruptured SG will continue to increase due to the primary-to-secondary leakage. The differing response of the intact SGs vs. ruptured SG allows for the operator to easily identify the ruptured SG. Thus, the operator must be able to monitor SG water level to determine which SG is ruptured. Therefore, SG water level (narrow range) is selected as a Type A PAM variable. Note that there are several radiation alarms which are also available to assist the operator in identifying the ruptured SG. The N-16 radiation monitors (or the alarm that occurred previously), the main steam line radiation monitors, or the SG blowdown water radiation monitors can be used. However, for the purpose of the DCD Subsection 15.6.3 analysis, these radiation monitors are considered to be backup means to identify the ruptured SG. Since the DCD Subsection 15.6.3 analysis assumes that the ruptured SG can be identified based on SG water level alone, none of the radiation monitors are required to be Type A PAM variables. After identifying the ruptured SG, the operator then manually isolates the ruptured SG by closing the main steam isolation valve, EFW isolation valve, and various other valves as necessary. It is not necessary to monitor any variables in order for the operators to close the valves. If the operator knows which SG is ruptured, then the operator will know which valves to close. The need for monitoring the valve position indications as part of the system status is addressed in the section describing the Type D PAM variables.

- *Cool Down Primary Coolant System* – Eventually the operator will need to depressurize the RCS to reduce the primary-to-secondary leakage (see next operator action). In order to ensure that subcooling is maintained during the depressurization, the RCS temperature must be reduced. In the DCD Subsection 15.6.3 analysis operator action is credited to open the intact SGs' main steam depressurization valves (MSDVs) in order to cool down the RCS. While no specific variables are required to be monitored to open the valves, the operator will need to monitor the RCS hot leg temperature during the cooldown to assess the progress of the cooldown and to determine when to terminate the cooldown. In addition, the operator will need to monitor the main steam line pressures of the intact SGs to verify that SG pressure is decreasing as expected and to ensure that the SG MSDVs have closed properly when the cooldown is terminated. Therefore, both RCS hot leg temperature (wide range) and main steam line pressure are selected as Type A PAM variables.

- *Depressurize Primary Coolant System to Equalize Pressure between Primary and Secondary* – In order to stop the primary-to-secondary leakage, the primary and secondary pressures in the SG must be equalized. This is done by depressurizing the RCS. The DCD Subsection 15.6.3 analysis credits the manual operator action of opening the pressurizer safety depressurization valve (SDV) to reduce the RCS pressure. The RCS depressurization cannot be initiated until the RCS temperature has been adequately reduced. The operator must first verify the RCS hot leg temperature, which is already selected as a Type A PAM variable. Since the goal of this action is to equalize primary and secondary pressure, the operator must carefully monitor both the RCS pressure and main steam line pressures throughout the depressurization process. Therefore, RCS pressure is also selected as a Type A PAM variable. During the depressurization, RCS subcooling will decrease. The operator must monitor the subcooling to prevent subcooling from being lost. If subcooling is lost, the operator must terminate the RCS depressurization. Therefore, RCS degrees of subcooling is selected as a Type A PAM variable. The RCS depressurization will also result in an increase in pressurizer water level. Since pressurizer overfill would complicate the event recovery and could lead to additional coolant loss through the pressurizer safety valves, the operator must terminate the RCS depressurization if pressurizer level becomes too high. Pressurizer water level is already selected as a Type A PAM variable.

- *Terminate Safety Injection Flow* – Even after the primary and secondary pressures are equalized, the primary-to-secondary leakage will continue due to safety injection (SI) flow. SI must be terminated in order to completely stop the primary-to-secondary leakage and terminate this event. SI is terminated based on very specific conditions that are assumed in DCD Subsection 15.6.3.4.2. The SI termination criteria are based on RCS subcooling, EFW flow, SG water level, pressurizer level, RCS pressure. The operator must monitor these parameters in order to determine when it is appropriate to terminate SI. All of the parameters except EFW flow have already been selected as Type A PAM variables. Therefore, EFW flow is also selected as a Type A PAM variable.

As described above, some variables are monitored by the operator in order to take the manual operator actions assumed in the DCD Subsection 15.6.3 analysis. Therefore these variables are designated as Type A PAM variables.

Loss of Coolant Accidents (Subsection 15.6.5)
Although not described in DCD Table 7.5-5, the post-LOCA long term cooling analysis credits a manual operator action to switch from the reactor vessel (RV) injection mode to the simultaneous RV and hot-leg injection mode as described in DCD Subsection 15.6.5.3.2.3. The reason that this action is not included in DCD Table 7.5-5 is that DCD Table 7.5-5 lists the operator actions in the context of the associated prompting alarms. The manual operator action credited for post-LOCA long term cooling is not based on any alarm or indication; the action is performed purely based on time. The analysis credits manual operator action to perform the switchover from the RV injection mode to simultaneous RV and hot-leg injection mode at 4 hours after the LOCA occurs. The timing of the operator action is determined by the solubility limit of boric acid in the core. For cold leg break LOCAs, RV injection mode is not effective in flushing the core and hence the boron concentration in the core may increase. This could result in boron precipitation that could interfere with core cooling. By switching one train of SI to hot-leg injection mode, the core will be flushed and the boron concentration will no longer increase. This switchover does not occur automatically and requires manual operator action at (or before) 4 hours. The operator is not required to monitor any variable to perform this action. Instead, the operator will perform the action at the designated time according to the EOPs. This operator action is included in the LOCA related EOPs of currently operating US and Japanese plants and will be required to be included in the US-APWR ERGs. Therefore, no Type A PAM variable is required to support this manual operator action that is credited in DCD Chapter 15.

An additional consideration for the LOCA event is that the refueling water storage pit (RWSP) level is an important indication in some currently operating plants in order to prompt operator action to realign the suction source of ECCS from the RWSP to the containment sump before the RWSP becomes empty. In the US-APWR, the RWSP is located at the bottom of the containment and the suction of both the SI pumps and the CS/RHR pumps is always from the RWSP. Therefore, it is not necessary to confirm the RWSP level to perform any manual realignment during the LOCA event and RWSP level is not included as a Type A PAM variable for the US-APWR.

Main Steam and Feedwater Line Breaks (Subsections 15.1.5 and 15.2.8)
The analyses of the Steam Line Break (SLB) and Feedwater Line Break (FLB) events assume EFW isolation to the faulted SG. In some operating plants, this action is performed manually. However, in the US-APWR, this action is performed automatically by the low steam line pressure signal EFW isolation function. Therefore, there are no manual actions for these events in DCD Table 7.5-5 and therefore there are no instruments required to be Type A PAM variables.

Mitigation of Consequences of AOOs
For selection criterion “b” for Type A, no explicit operator actions based on primary information from PAM instruments are assumed in any AOO analysis. However, SI termination and long-term core cooling from secondary heat sink are necessary to bring the plant to cold shutdown conditions for some AOOs. Operator actions for SI termination and long-term core cooling are already included in the operator actions assumed in the SGTR analysis. Therefore, almost all of the variables that meet selection criterion “b” are the same as those already selected based on criterion “a”. The only variable that is selected specifically for criterion “b” is reactor coolant cold leg temperature, since it is not explicitly used in the SGTR analysis. Therefore, all of the instruments associated with the mitigation of the consequences of AOOs have been included in the Type A PAM list provided in DCD Tables 7.5-3 and 7.5-6.

Summary for Type A PAM
In summary, MHI has used the performance-based criteria from IEEE Std 497-2002 to select the Type A PAM variables based on the US-APWR accident analysis assumptions in DCD Chapter 15. The SGTR analysis in DCD Subsection 15.6.3 is the key event that determines almost all of the Type A PAM variables. As discussed previously, ERGs for the US-APWR were not available at the time the PAM list was developed. However, the operator actions assumed in DCD Chapter 15 are the same as those used by domestic Japanese plants and also by many US operating plants. Thus MHI believes that the Type A PAM variables do take into account operational experience and previously existing procedures. For these reasons, MHI believes that the US-APWR Type A PAM variables have been selected in a manner consistent with the intent of IEEE Std 497-2002 and RG 1.97 Rev. 4.

NUREG-1431 Table 3.3.3-1 provides a generic list of PAM instrumentation for a Westinghouse NSSS plant based on the guidance in RG 1.97 Rev. 3; however, a reviewer’s note in NUREG-1431 requires that this table be amended by individual licensees to add all RG 1.97 Type A and Category 1 non-Type A variables to this generic list in accordance with the plant’s RG 1.97 Safety Evaluation Report. Therefore the PAM list provided in NUREG-1431 is a minimal list of Category 1 variables (any Type) for a typical Westinghouse NSSS plant. As a final check of the adequacy of the US-APWR Type A PAM variables, MHI performed a detailed comparison of all of the Category 1 variables (any Type) functions in NUREG 1431 Table 3.3.3-1 to the US-APWR Type A PAM variables listed in DCD Table 7.5-3. This comparison is provided in Table H.1-1. MHI has provided the bases for the differences between the Type A variables in the MHI PAM list and the Category 1 PAM for a typical Westinghouse 4 loop PWR plant in Table A.

H.2 Type B Variables

MHI utilized the performance-based criteria of RG 1.97 Rev. 4 and IEEE Std 497-2002 to select the Type B accident monitoring variables for the US-APWR. IEEE Std 497-2002 defines Type B variables as follows.

> Type B variables are those variables that provide primary information to the control room operators to assess the plant critical safety functions. Any plant critical safety functions addressed in the EPGs or the plant specific EOPs that are in addition to those identified above shall also be included.

As described above, the Type B variables are selected based on what the operator needs to monitor plant critical safety functions. The ultimate goal of the plant safety systems is to prevent an uncontrolled release of radioactive material in order to protect the health and safety of the public. This is accomplished by ensuring that certain parameters related to the plant critical safety functions are not exceeded. The plant critical safety functions are based on the very general PWR design principles of 1) Shutdown, (2) Cooldown, and (3) Contain, where each of these concepts is defined as follows.

- "Shutdown" means that the plant should be subcritical in order to reduce the thermal energy in the core to decay heat levels during emergency conditions.
- "Cooldown" means that the heat should be removed from the core (fuel rods) to protect the integrity of the cladding. Decay heat should be removed from the RCS.
- "Contain" refers to the integrity of the RCS and containment vessel. Heat should be removed from the containment to the ultimate heat sink.

IEEE Std 497-2002 defines five critical safety functions as: reactivity control, reactor core cooling, reactor coolant system integrity, primary reactor containment integrity, and radioactive effluent control. MHI uses the same conceptual critical safety functions, but groups them slightly differently in some cases. In MHI's case, the reactor core cooling critical safety function from IEEE Std 497-2002 is separated into the critical safety functions of core cooling and secondary heat sink. This is done in order to emphasize the importance of the secondary system for maintaining core cooling. If the secondary heat sinks (SGs) are maintained available following an accident, they can be used to help ensuring core cooling. Therefore, the secondary heat sink critical safety function identified by MHI is one aspect to maintain reactor core cooling. In IEEE Std 497-2002, primary reactor containment integrity and radioactive effluent control are defined as two separate critical safety functions. However, in RG 1.97 Rev. 3, the description for Type B variables in Table 3 (page 1.97-22) includes radioactive effluent control as part of the critical safety function for maintaining containment integrity. Consistent with MHI operational experience and also with the RG 1.97 Rev. 3 definition, MHI has included radioactive effluent control as part of the containment integrity critical safety function. Although IEEE Std 497-2002 only defines five critical safety functions, the definition for Type B variables indicates that other critical safety functions in addition to these five may be designated. Based on operational experience, MHI has chosen to add a sixth critical safety function for RCS inventory. The purpose of this critical safety function will be described later. Therefore, the six critical safety functions for the US-APWR are identified as follows.

- Reactivity control
- Core cooling
- Secondary heat sink
- RCS integrity
- Containment integrity
- RCS inventory

Although there are some slight differences in grouping as described above, MHI believes that the US-APWR critical safety functions are consistent with those defined in IEEE Std 497-2002. In addition, the US-APWR critical safety functions are identical to those used in many Japanese and US operating plants. The critical safety functions are described as part of the US-APWR design information in DCD Subsections 7.5.1.4 and 7.8.3.2, and DCD Tables 7.8-1 and 7.8-2. The selection of the Type B PAM variables related to these safety functions, based on the IEEE Std 497-2002 criteria, is discussed in the sections below.

Reactivity Control
The reactivity control safety function exists to ensure that the reactor is adequately shutdown and the only source of heat to the RCS is decay heat. The most direct way to determine whether the reactor is shutdown is to measure the neutron flux. Following an accident, the operator can monitor the neutron flux at all times in order to verify that the reactor is shutdown. Neutron flux can be measured over the full scale of reactor power, with some detectors monitoring only certain portions of the scale. The wide range neutron detectors allow the operator to measure the neutron flux from full power all the way to post-trip and shutdown levels. Therefore, wide range neutron flux is selected as a Type B PAM variable.

A boron dilution or an inadequate boron concentration in the RCS following an accident can lead to an increase in the reactivity of the core. If unchecked, this could result in a lack of reactivity control. The increase in reactivity will eventually be noticed by the operator via the wide range neutron flux indication, which is Type B as discussed above. It would also be possible to detect a boron dilution or inadequate boron concentration by monitoring the RCS soluble boron concentration. However, the RCS boron concentration is not monitored continuously in the control room; it is obtained by periodically sampling. Therefore, although it remains important for the operator to be aware of the RCS boron concentration for long term reactivity control, the boron concentration is not the primary means to monitor this critical safety function. RG 1.97 Rev. 3 does classify the RCS soluble boron concentration as a Type B PAM variable, but also denotes it as Category 3, which means that it is a backup variable. RG 1.97 Rev. 4 indicates that backup indications do not need to meet the criteria in the guide.

The critical safety functions are monitored after the reactor is shutdown or expected to be shutdown. In this condition, the control rods are expected to be fully inserted and reactor trip breakers are open. EOPs normally included verification of several different types of indications following a reactor trip, including neutron flux, rod position, and reactor trip breakers. The control rod position indications can be monitored by the operators to confirm that the rods are fully inserted to ensure the reactor is shutdown. Control rod position indications were included in RG 1.97 Rev. 3 as Type B PAM variables. However, they were denoted as Category 3, which means that they are backup variables. According to Section B of RG 1.97 R4, the intent of the PAM variable selection is to select those variables which provide the primary indication to the operators. The RG 1.97 Rev. 4 does not require every indication used in the EOPs to be PAM variables, since many of the indications are considered backup, etc. Since the EOPs may include multiple indications for verification of reactor trip, MHI selected wide range neutron flux as the PAM variable because MHI believes it is the most useful, and therefore, primary indication of reactor trip. The reason is that there may be situations where control rod position may be a somewhat misleading indication. If all the control rod positions said that a control rod group was fully inserted, but one of the rods of that group was stuck, it may not be a definitive indication that the reactor is shutdown. Neutron flux would be definitive as to whether the reactor was shutdown. For the plant critical safety functions, the reactivity control safety function may be violated even with control rods fully inserted during certain events, such as a boron dilution or a recriticality caused by an RCS cooldown. Therefore, the operator should monitor neutron flux rather than control rod position. For these reasons, MHI selected wide range neutron flux and considered the control rod position a backup indication. MHI believes this approach is the reason that RG 1.97 Rev. 3 classified control rod position as “Category 3”. Therefore, the wide range neutron flux remains the primary indication and control rod position indication is not selected as a Type B PAM variable.

Due to the negative moderator temperature coefficients in PWRs, a decrease in RCS temperature can result in an increase in core reactivity. Normally the effect is small, but if a large decrease in RCS temperature occurs, it may have an effect on the reactivity control critical safety function. In order to prevent an uncontrolled cooldown of the RCS, the operators may monitor RCS cold leg temperatures as supporting information for this critical safety function. RCS cold leg temperature is selected as a Type B PAM variable primarily based on the core cooling critical safety function (see discussion below), but is also available as a backup indication to support the reactivity control safety function.

Core Cooling

The core cooling critical safety function exists to ensure that heat can be removed from the core to protect the fuel cladding. Core cooling can be assessed by monitoring the temperatures in the RCS. There are several ways to measure temperature in the RCS. Both RCS hot leg and cold leg temperatures are very useful for the operator to monitor core cooling. Therefore, RCS hot leg (wide range) and RCS cold leg (wide range) temperatures are both selected as Type B PAM variables.

Typically, the temperatures in the core are higher than those in the hot and cold legs. The core exit temperature indication provides a means to measure the temperatures at a point very close to the top of the core. The core exit temperature can then be used to determine if the core cooling critical safety function is satisfied. Therefore, core exit temperature is also selected as a Type B PAM variable.

Another means to ensure that adequate core cooling exists is to maintain subcooled conditions in the RCS. The operator can directly monitor subcooling via the degrees of subcooling monitor. Therefore, degrees of subcooling is selected as a Type B PAM variable. Note that the subcooling indication is actually a calculated value that is determined based on the RCS temperatures and RCS pressure. Therefore, the temperature and pressure indications that feed into the calculation must also be Type B parameters. For this reason, RCS pressure is selected as a Type B PAM variable (RCS temperatures were already selected as Type B as discussed previously).

The operator needs to monitor whether the inventory in the RCS is adequate to keep the core covered. If the core becomes uncovered during an accident core cooling will be lost and the core will heat up rapidly. The reactor vessel water level indication is the most direct way to ensure that the core is covered and thus core cooling is maintained. Therefore, reactor vessel water level is selected as a Type B PAM variable.

Secondary Heat Sink

As described previously, this critical safety function is not explicitly included in the IEEE Std 497-2002 definition, but is included by MHI to emphasize the importance of the secondary side in protecting core cooling. The secondary heat sink critical safety function exists to ensure that one or more SGs can safely remove heat from the RCS. If this critical safety function is lost, the RCS will heat up and then eventually the core cooling critical safety function will also be violated.

The effectiveness of the secondary heat sink can be monitored by the operators by observing various parameters related to the SGs. The SG water level, both wide and narrow range, indicates whether the SGs have sufficient inventory to remove heat from the RCS. Therefore, SG water level (narrow range) and SG water level (wide range) are selected as Type B PAM variables. Even if SG water level is currently adequate during an accident, the SGs may dry out if they are not continuously supplied with water. Following an accident, EFW flow is the means by which the SGs are supplied with water. The operators monitor the EFW flow to ensure that the SGs will not dry out and cause a loss of secondary heat sink. Therefore, EFW flow is selected as a Type B PAM variable. The EFW to the SGs is supplied from two EFW pits. If the EFW pit levels become low, EFW to an SG may be lost. Therefore, EFW pit level is selected as a Type B PAM variable.

In addition, the SGs will not function as a secondary heat sink if the pressure in the main steam lines is either too low or too high. The operator must monitor the main steam line pressures continuously to ensure proper SG function. Therefore, main steam line pressure is selected as a Type B PAM variable.

RCS Integrity

The RCS integrity critical safety function exists to ensure that the RCS remains intact following an accident. If the RCS remains intact, adequate RCS inventory will be maintained, which serves to ensure core cooling. An intact RCS will also prevent the release of any radioactivity. The most direct way for the operator to monitor RCS integrity is to monitor the RCS pressure. An unexpected decrease in RCS pressure would indicate to the operator that a break or leak in the RCS may have occurred. Therefore, RCS pressure is selected as a Type B PAM variable.

If there is a leak or break in the RCS inside containment, the flow of RCS coolant into the containment will cause an increase in containment pressure. By also monitoring containment pressure, the operator can detect a break or leak in the RCS. Therefore, containment pressure is also selected as a Type B PAM variable.

If RCS coolant is entering the containment through a leak or break, it will eventually drain into the RWSP which is inside containment and fulfills the role of a containment sump. An increase in the RWSP level would indicate to the operators that RCS integrity may have been lost. This is a much more indirect means of monitoring RCS integrity as compared to RCS pressure and containment pressure. However, RWSP water level (wide range) and RWSP water level (narrow range) are selected as Type B PAM variables.

Containment Integrity

The containment integrity critical safety function exists to ensure that the containment does not fail and remains leak-proof to prevent radiation from being released to the atmosphere. The containment is designed to withstand expected internal pressures following an accident. If the containment pressure exceeds its design limits, the containment may ultimately fail. The operators monitor containment pressure to ensure that it remains safely below the design pressures following an accident. Therefore, containment pressure is selected as a Type B PAM variable.

As discussed previously, the containment integrity critical safety function also encompasses the function of radioactive effluent control. The containment is therefore designed with isolation valves that can be closed to keep radiation inside the containment building. In order to ensure that there are no open pathways that could allow radiation to escape, the operator can monitor the valve position of each of the containment isolation valves. Therefore, containment isolation valve positions are selected as Type B PAM variables. Note that some containment isolation valves are check valves. Since they are passive valves that fail in a safe position, the operators do not need to monitor the check valve positions and therefore check valves are excluded from Type B.

As part of the function of radioactive effluent control, it is important for operators to have a means to monitor the radiation levels inside containment. The containment high range area radiation monitor provides the capability for the operator to monitor containment radiation. Therefore, containment high range area radiation is selected as a Type B PAM variable.

Note that PAM variable selection is based on design basis accidents. The containment analyses in Chapters 6 and 15 show that containment remains intact for the limiting design basis accident. Therefore, a beyond design basis accident would be required to breach containment. The leak-tightness of containment prior to an event is confirmed by the Technical Specifications and also testing as required in 10 CFR 50 Appendix J. Since the initial condition is that containment is operable, containment integrity can be maintained by ensuring proper closure of containment isolation valves and monitoring containment pressure, which are Type B PAM variables as described above. Monitoring for additional variables needed to address leakage from challenges such as degraded seals or penetrations is beyond a design basis event and is therefore outside of the scope of PAM.

The radiation monitors outside of containment are already assigned as Type E PAM variables. Therefore, additional Type B PAM variables for this item are not needed.

RCS Inventory

As described previously, the RCS inventory critical safety function is not defined in IEEE Std 497-2002 but is added by MHI. The RCS inventory critical safety function exists to complement the core cooling and RCS integrity critical safety functions. If the RCS inventory is too low, it will be difficult to ensure adequate core cooling. For some accidents, safety injection (SI) is used to ensure core cooling initially, but may not be needed at later stages of the accident. In order to terminate SI safely, the operators need to ensure that core cooling will be maintained when SI is terminated. In addition to checking variables related to core cooling and the secondary heat sink, the operators also check RCS inventory by monitoring the pressurizer water level.

An excessive RCS inventory can result in a loss of RCS integrity. If the pressurizer is overfilled, water relief through the pressurizer safety valves may occur. To prevent this loss of

RCS integrity, the operators monitor the pressurizer water level. Therefore, pressurizer water level is selected as a Type B PAM variable.

Summary for Type B PAM

In summary, MHI has used the performance-based criteria from IEEE Std 497-2002 to select the Type B PAM variables based on the US-APWR plant critical safety functions. The US-APWR plant critical safety functions are consistent with those defined in IEEE Std 497-2002 and are documented in DCD Chapter 7. Note that the selection criteria in IEEE Std 497-2002 also states that critical safety functions from the plant specific EOPs should also be included. As discussed previously, ERGs for the US-APWR were not available at the time the PAM list was developed. However, the plant critical safety functions are based on conceptual safety principles that apply to all PWR designs. The US-APWR plant critical safety functions are the same as those used by domestic Japanese plants and also by many US operating plants. Thus MHI believes that the Type B PAM variables do take into account operational experience and previously existing procedures. For these reasons, MHI believes that the US-APWR Type B PAM variables have been selected in a manner consistent with the intent of IEEE Std 497-2002 and RG 1.97 Rev. 4.

The US-APWR Functional Restoration Guidelines (FRGs) are being developed to provide protection of the plant critical safety functions described in DCD Chapter 7. The FRGs establish predefined function-related restoration strategies for responding to emergency transients where the initiating event is unknown and the transient is not predefined. The restoration strategies utilize available plant equipment to return the parameters used for entry conditions back to values sufficient to ensure protection of the plant critical safety function. Therefore, the FRGs utilize the Type B PAM variables to monitor the critical safety functions.

As a final check of the adequacy of the US-APWR Type B PAM variables, MHI performed a detailed comparison between the Type B variables included in the MHI PAM list and those included in RG 1.97 Rev. 3 Table 3. This comparison is provided in Table H.2-1. For each difference, MHI has provided a detailed explanation of the basis for the difference in Table H.2-1.

As described earlier, the US-APWR critical safety functions are also described in DCD Subsections 7.5.1.4 and 7.8.3.2 as part of the design for the safety parameter display system (SPDS) and the diverse actuation system (DAS), respectively. There are some differences between the variables selected for the SPDS and DAS compared to the Type B PAM variables. The SPDS is intended to display key parameters for monitoring the critical safety functions. In some cases, the SPDS includes additional parameters that are useful for the operator but were not selected as Type B PAM variables. For example, the SPDS includes status of reactor trip breakers as a parameter for monitoring the reactivity control safety function. This parameter is included in the SPDS since it may be useful for the operator to confirm that reactor trip has occurred, but it is not necessary to include as a Type B PAM variable since neutron flux provides adequate indication of reactor trip. Therefore, MHI considers the Type B PAM variables to be the primary parameters for monitoring critical safety functions while the SPDS includes all of the primary parameters and some additional secondary parameters for operator convenience. On the other hand, the DAS design is based on the best-estimate approach consistent with BTP 7-19. Therefore, the DAS design does not need to include all of the Type B PAM variables. Only a subset of the Type B PAM variables that are necessary for the monitoring of critical safety functions on a best-estimate basis are selected to be included for the DAS. The details of the DAS are provided in the D3 Topical Report (MUAP-07006) and the D3 Coping Analysis Technical Report (MUAP-07014).

H.3 Type C Variables

MHI utilized the performance-based criteria of RG 1.97 Rev. 4 and IEEE Std 497-2002 to select the Type C accident monitoring variables for the US-APWR. IEEE Std 497-2002 defines Type C variables as follows.

> Type C variables are those variables that provide primary information to the control room operators to indicate the potential for breach or the actual breach of the three fission product barriers (extended range): fuel cladding, reactor coolant system pressure boundary, and containment pressure boundary.

As described in the criteria above, the US-APWR (and all PWRs) has three fission product barriers. The fission product barriers contain the highly radioactive fission products and therefore prevent radiological releases during an accident. The failure or potential failure of each fission product barrier can be determined by the operator by monitoring certain variables. Each fission product barrier is discussed below.

Fuel Cladding
The cladding around the fuel keeps the fission products separate from the RCS coolant. The detailed fuel cladding design is described in DCD Section 4.2. The information in DCD Section 4.2 provides the design basis for evaluating the IEEE Std 497-2002 criteria for Type C variables. The cladding is designed to withstand the high temperatures associated with normal operational conditions. The cladding is also designed to withstand even higher temperatures such as may occur during transients or accidents. However, at extremely high temperatures, cladding failure may occur and fission products could be released into the RCS coolant. If the operator can ensure that temperatures remain below a certain threshold, then the integrity of the fuel cladding will be maintained. Although temperatures in the core cannot be directly measured, the temperatures at the core exit can be used to determine if cladding failure is a possibility. Since the operator monitors core exit temperature in order to ensure that the fuel cladding remains intact, core exit temperature is selected as a Type C PAM variable. This Type C PAM variable allows the operator to monitor for a possible failure of the cladding.

If an actual failure of the cladding has occurred, then fission products will be present in the RCS coolant. Monitoring the RCS coolant for radioactivity allows the operator to detect an actual fuel cladding breach. Therefore, radioactivity concentration or radiation level in circulating primary coolant is selected as a Type C PAM variable. It is also possible to obtain detailed analysis of the primary coolant (gamma spectrum) to monitor for an actual fuel cladding failure by periodic sampling. However, this indication was denoted as a Category 3 Type C PAM variable in RG 1.97 Rev. 3. Category 3 means that it is a backup indication and not the primary source of information. RG 1.97 Rev. 4 states that backup indications do not need to meet the criteria in the guide. Core exit temperature and radioactivity concentration or radiation level in circulating primary coolant are the primary indications. Therefore, analysis of primary coolant (gamma spectrum) is not selected as a Type C PAM variable for the US-APWR.

Reactor Coolant System Pressure Boundary
In the unlikely event that the fuel cladding fails, the RCS pressure boundary is the second fission product barrier that prevents the release of radiation to the environment. The RCS pressure boundary is described in detail in DCD Section 5.2. The information in DCD Section

5.2 provides the design basis for evaluating the IEEE Std 497-2002 criteria for Type C variables. The RCS is maintained at a high pressure. If the pressure boundary fails, the RCS pressure will decrease at a rate dependent upon the size of the break. By monitoring RCS pressure, the operators will be able to identify any failures of the RCS pressure boundary. Therefore, RCS pressure is selected as a Type C PAM variable.

The entire RCS, with the exception of some small sample and letdown lines, is contained within the containment vessel. A breach in the RCS pressure boundary will thus result in the release of high pressure RCS coolant into the containment vessel which is normally maintained at near-atmospheric pressure conditions. This break flow into the containment will result in an increase in the containment pressure at a rate dependent upon the size of the break. By monitoring containment pressure, the operators have an additional means to detect a failure of the RCS pressure boundary. Therefore, containment pressure is selected as a Type C PAM variable.

The release of RCS coolant into the containment vessel will also result in an increase in radiation inside the containment vessel. The increase in containment radiation levels will be especially large if failure of the fuel cladding has also occurred. Containment radiation provides another means to monitor for a failure of the RCS pressure boundary. Therefore, containment high range area radiation is selected as a Type C PAM variable.

As described in the section for Type B, RWSP water level can be used to monitor the RCS integrity. However, the criteria for Type C PAM refer to the primary information to monitor fission product barriers. RWSP water level is considered a backup, not a primary, means to detect a failure of the RCS pressure boundary since RWSP water level does not provide direct information on where the fluid is coming from. Therefore, RWSP level is not selected as a Type C PAM variable.

Note that there are some portions of the RCS that are outside containment, such as small sample lines and the letdown line. Failures of these portions of the RCS pressure boundary outside containment would result in a decrease in RCS pressure but would likely not result in an increase in containment pressure or radiation. However, these lines are automatically isolated by the containment isolation function. Containment isolation may occur based on RCS pressure or containment pressure, which have already been identified as Type C PAM variables. The containment isolation valves are part of the reactor coolant pressure boundary. Similarly, an SGTR is a failure of the RCS pressure boundary that would not cause an increase in containment pressure or radiation.

As a backup to the RCS pressure variable, the operator could detect these scenarios by decreases in pressurizer water level or, in the case of an SGTR, increases in SG water level. Pressurizer water level and SG water level are already Type A PAM variables. As indicated in DCD Table 7.5-2, the requirements for Type A PAM variables already meet all the requirements for Type C variables. Since these other PAM variables are also available as backup indications, no additional Type C PAM variables are needed to detect a failure of the RCS pressure boundary. Note that the Type C variable of RCS pressure and the backup Type A variables of pressurizer water level and SG water level do not detect the full range of RCS leak sizes and locations, particularly for small SGTRs. However, Technical Specification 3.4.13 requires monitoring RCS leakage. For RCS leakage that is less than the Technical Specification limit, although the Type C and backup Type A variables may not be able to detect the leak, no action is required in this case anyway. For RCS leakage in excess of the

Technical Specification limits, the impact on the current Type C and Type A backup variables would be large enough to be detectable using these existing variables.

Containment Pressure Boundary

The containment vessel is the last fission product boundary that prevents the release of radiation to the environment. The containment pressure boundary is described in detail in DCD Section 6.2. The information in DCD Section 6.2 provides the design basis for evaluating the IEEE Std 497-2002 criteria for Type C variables. As described in DCD Section 6.2, the containment is designed to ensure leak-tight integrity under normal operation and during postulated design basis accidents that result in high internal pressures, such as LOCAs. The leak-tightness of the integrity is controlled by Technical Specifications 3.6.1, 3.6.2, and 3.6.3. Together, these Technical Specifications ensure that the containment is intact. For this reason, the design basis accidents, such as LOCAs, assume that the containment is intact at the start of the accident. Technical Specification 3.6.4 also requires the containment pressure to be controlled very close to atmospheric pressure. Note that some leakage is expected to occur though. This leakage is controlled by the containment leakage rate testing program in Technical Specification 5.5.16. The testing program in 5.5.16 indicates that the maximum allowable containment leakage rate is 0.1% of containment air weight per day at a containment internal pressure corresponding to the calculated peak containment internal pressure for design basis LOCA. Since leakage less than this amount is allowed by the Technical Specifications during normal operation and during accidents, the PAM criteria for containment integrity only apply for potential or actual breaches of containment integrity that would result in leakages in excess of that allowed by Technical Specifications.

As indicated by Technical Specification 3.6.4, the containment pressure is kept in a range very close to atmospheric pressure and may in fact be negative. In this case, a potential or even an actual breach in containment would not violate containment integrity since only in-leakage would occur. This means that an elevated containment pressure must occur before a potential or actual breach would violate the containment fission product boundary. Therefore, monitoring containment pressure is necessary. As described previously, the containment vessel is designed to withstand high internal pressures. The analyses in Chapter 6 demonstrate that containment integrity can be maintained even during a LOCA event. However, if the containment pressure becomes too high, the containment will eventually be breached or fail. The operator can monitor the containment pressure to determine if the containment pressure is high enough that a potential for containment breach or failure exists. Therefore, containment pressure is selected as a Type C PAM variable (it was previously selected to support monitoring the RCS pressure boundary as well).

Containment pressure is the primary variable to monitor the potential for containment breach. The criteria for Type C PAM variables also indicate that actual breaches should be addressed as well. As discussed previously, the design of the containment is such that no actual breach of containment can occur during a design basis event. In order for the containment internal pressure to be high enough to cause an actual breach to occur, a beyond design basis event would have to occur. If a breach or failure of containment does occur due to such a beyond design basis event, the breach will result in a decrease in containment pressure. This unexpected decrease in containment pressure would be observable by the operator such that containment pressure would still remain the primary indication even during this beyond design basis accident (i.e., beyond the scope of the PAM requirements). The Technical Specification limits allow for leakage from containment up to certain rates. Any leakage rate less than these limits, regardless of the cause, does not apply the PAM criteria for Type C. Similarly, the other requirement for containment integrity in the Technical Specifications ensures that there can be no breach due to a known leakage path being open, such as an equipment hatch, etc. An inadvertently open containment isolation valve could be considered a small breach that would be difficult to detect by containment pressure. However, the containment isolation valve positions are already monitored as Type B PAM variables for the containment integrity critical safety function. So any failure of a containment isolation valve would be detected by the operator while monitoring the containment isolation valve positions. Therefore, there are no actual breaches of containment that require any additional Type C PAM variables.

Note that RG 1.97 Rev. 3 identified containment effluent radioactivity and effluent radioactivity as two Type C PAM variables for the containment fission product barriers. These variables would allow the operator to detect radiation outside of containment. This might indicate that fission products had escaped from containment and could represent a potential breach of containment. However, it is also possible that this radiation outside containment is not caused by a potential breach of containment. One reason for this is that, as discussed previously, there are some portions of the RCS that are outside of the containment pressure boundary and thus bypass the containment fission product barrier. These pathways are automatically isolated by the containment isolation function which may occur based on containment pressure or RCS pressure. The RCS pressure indication is available to monitor for these situations and is selected as a Type C PAM variable for this reason (although it is already a Type C PAM variable as described previously). In addition, an SGTR may also allow the containment pressure boundary to be bypassed. In the case of an SGTR, the RCS pressure, pressurizer water level, and SG water level are available as backups to detect the SGTR and are Type A PAM variables (RCS pressure is also Type C). Therefore, the containment effluent radioactivity and effluent radioactivity indications are not required as Type C since they are not the primary means to detect these scenarios.

Based on the above reasons, MHI believes that the potential for breaches in the containment fission product barrier are those that are caused by design basis accidents that result in large increases in containment pressure. Therefore, containment pressure is the primary information utilized by the operator and is selected as Type C. There are some scenarios where containment may be bypassed, such that monitoring of RCS pressure is required as Type C (and some other Type A variables are available as backup). The containment effluent radioactivity and effluent radioactivity indications are not required to be Type C. In fact, RG 1.97 Rev. 3 identified these indications as Category 2 Type C which means that they did not have to meet the same qualification requirements as the Category 1 Type C variables (like containment pressure). Then these indications should be considered backup indications. RG 1.97 Rev. 4 states that backup indications do not need to meet the criteria in the guide.

One final point regarding the radiation indications is that the safety analyses in Chapter 15 do consider the release of radiation from containment for offsite dose calculations even though containment integrity is demonstrated to be maintained. These radiation releases are assumed to occur through the known leakage pathways at the leakage rates consistent with the Technical Specifications described above. Since the leakage rate is governed by Technical Specifications, the monitoring of this radiation is not required per the Type C criteria. However, monitoring of radioactivity releases is required as part of the Type E PAM variables. As a result, some of these radiation indications are selected as Type E PAM variables. The selection of the variables necessary to monitor these releases is discussed in the Type E section.

Note that PAM variable selection is based on design basis accidents. The containment analyses in Chapters 6 and 15 show that containment remains intact for the limiting design basis accident. Therefore, a beyond design basis accident would be required to breach containment. The leak-tightness of containment prior to an event is confirmed by the Technical Specifications and also testing as required in 10 CFR 50 Appendix J. Since the initial condition is that containment is operable, containment integrity can be maintained by monitoring containment pressure, which are Type C PAM variables as described above. Monitoring for additional variables needed to address leakage from challenges such as degraded seals or penetrations is beyond a design basis event and is therefore outside of the scope of PAM. The radiation monitors outside of containment are already assigned as Type E PAM variables. Therefore, additional Type C PAM variables for this item are not needed.

Summary for Type C PAM
In summary, MHI has used the performance-based criteria from IEEE Std 497-2002 to select the Type C PAM variables based on the three fission product barriers used in the US-APWR design. As discussed previously, ERGs for the US-APWR were not available at the time the PAM list was developed. However, the fission product barriers are a standard principle of PWR design and do not depend on the ERGs. The means of monitoring the US-APWR fission product barriers are the same as those used by domestic Japanese plants and also by many US operating plants. Thus MHI believes that the Type C PAM variables do take into account operational experience and previously existing procedures. For these reasons, MHI believes that the US-APWR Type C PAM variables have been selected in a manner consistent with the intent of IEEE Std 497-2002 and RG 1.97 Rev. 4.

As a final check of the adequacy of the US-APWR Type C PAM variables, MHI performed a detailed comparison between the Type C variables included in the MHI PAM list and those included in RG 1.97 Rev. 3 Table 3. This comparison is provided in Table H.3-1. For each difference, MHI has provided a detailed explanation of the basis for the difference in Table H.3-1.

H.4 Type D Variables

MHI utilized the performance-based criteria of RG 1.97 Rev. 4 and IEEE Std 497-2002 to select the Type D accident monitoring variables for the US-APWR. IEEE Std 497-2002 defines Type D variables as follows.

> Type D variables are those variables that provide primary information to the control room operators and are required in procedures and licensing basis documentation (LBD) to:
>
> a) Indicate the performance of those safety-related systems and auxiliary supporting features necessary for the mitigation of design basis events.
>
> b) Indicate the performance of other systems necessary to achieve and maintain a safe shutdown condition.
>
> c) Verify safety-related system status.

As described above, there are three criteria identified in IEEE Std 497-2002 for selecting Type D variables. Each of the criteria is discussed below.

Criterion "a"
This criterion is related to systems that are credited for the mitigation of design basis events. The accident analysis licensing basis is described in DCD Chapter 15 events. Some of the analyses in DCD Chapter 15 credit engineered safety features (ESF) to mitigate the event.

The safety injection (SI) system is one of these systems credited in DCD Chapter 15. For example, SI is assumed in the main steam line break analysis in DCD Subsection 15.1.5 and the LOCA analysis in DCD Subsection 15.6.5, as well as a few other analyses. The operators need to be able to monitor the performance of the SI system during an accident, which meets criterion "a" for Type D PAM variables. The SI system has four SI pumps and the operator must be able to verify the proper SI pump flow. Therefore, SI pump discharge flow and SI pump minimum flow are selected as Type D PAM variables.

The SI system also includes four SI accumulators. The accumulators are passive devices that inject water when RCS pressure decreases below the accumulator pressure. The accumulators are assumed in the LOCA analysis in DCD Subsection 15.6.5. In order to determine that the accumulators are operating correctly, the operator can monitor the accumulator water level and accumulator pressure. Therefore, accumulator water level and accumulator pressure are selected as Type D PAM variables.

During the LOCA analysis in DCD Subsection 15.6.5, the accumulators help to ensure adequate coolant inventory in the reactor vessel during the time when the SI pumps have not yet started due to the assumed loss of offsite power. The success of the accumulators can therefore also be monitored by the operators based on the reactor vessel water level. Therefore, reactor vessel water level is selected as a Type D PAM variable.

One notable departure is the variable to monitor flow in the low pressure injection system. The accumulators and high head safety injection system in the US-APWR are designed to replace the entire low head safety injection function. Therefore, the low pressure injection system is not part of the US-APWR design and this monitoring variable is not applicable to the US-APWR.

The reactor trip system is credited to mitigate almost all design basis events in DCD Chapter 15. Reactor trip results in the rapid insertion of the control rods. The success of the reactor trip can be determined by monitoring neutron flux. Therefore, wide range neutron flux is selected as a Type D PAM variable.

The safety valves on the primary side (pressurizer safety valves) and the safety and relief valves on the secondary side (main steam safety valves and main steam relief valves) can be considered ESF and are credited in some design basis accidents. For example, the turbine trip event in DCD Subsection 15.2.2 credits the actuation of both the pressurizer and main steam safety valves. Note that the Chapter 15 safety analyses do not actually credit the main steam relief valves to mitigate a design basis accident, but their set pressure is such that they would be expected to open prior to the main steam relief valves in events like the turbine trip. The safety or relief valves open at a specific setpoint to relieve pressure, then close again when pressure has decreased. It is not typically necessary to monitor the safety valve position to ensure proper safety valve opening and closure. Instead, the operators can monitor the safety valve performance by monitoring other parameters such as the RCS pressure, temperature, and subcooling for the pressurizer safety valves and monitoring the main steam line pressure for the main steam safety valves. Therefore, RCS pressure, reactor coolant hot and cold leg temperature, degrees of subcooling, and main steam line pressure are selected as Type D PAM variables. However, the primary and secondary safety and relief valve positions provide a very efficient way for the operators to verify system status as will be discussed in criterion “c” and are therefore also selected as Type D PAM variables.

Automatic isolation of the main steam lines (by closure of the main steam line isolation valves), the main feedwater lines (by closure of the main feedwater isolation valves), and emergency feedwater lines (by closure of the EFW isolation valves) are also included as ESF and are credited in some design basis accidents. For example, the steam line piping failure event in DCD Subsection 15.1.5 credits the automatic isolation of the main steam and feedwater lines and the EFW line to the faulted SG. Similar to the safety valves described above, the closure of these valves can be verified by the operators by checking variables other than the valve positions. Main steam isolation can be monitored by the operators using main steam line pressure. Main feedwater (MFW) and EFW isolation can be monitored by the operators using SG water level and EFW isolation can also be monitored by EFW flow. Therefore, main steam line pressure, EFW flow, and SG water level (both narrow and wide range) are selected as Type D PAM variables. However, the isolation valve positions provide a very efficient way for the operators to verify system status as will be discussed in criterion “c” and are therefore also selected as Type D PAM variables.

Another ESF used to mitigate design basis events is the containment spray system. The main steam line break (inside containment) and LOCA analysis in DCD Subsections 15.1.5 and 15.6.5, respectively, result in the release of coolant to the containment. The mass and energy release for these events are calculated in DCD Chapter 15 to use for the containment pressure and temperature response analysis in DCD Chapter 6. The analyses credit the containment spray system for mitigating the increase in containment temperature and pressure. Containment spray is provided by the four CS/RHR pumps and the operator must be able to verify the proper CS/RHR pump flow. Therefore, containment temperature, containment pressure, CS/RHR pump discharge flow, and CS/RHR pump minimum flow are selected as Type D PAM variables.

Both the SI pumps and the CS/RHR pumps take suction from the RWSP. In order for the pumps to be able to provide the necessary flow credited in the Chapter 15 analyses, the operators need to monitor the RWSP level while using the SI and containment spray systems. Therefore, RWSP water level (wide range) and RWSP level (narrow range) are selected as Type D PAM variables. Note that it is not necessary for the operator to monitor the RWSP temperature. The SI pumps and CS/RHR pumps were designed to ensure adequate net positive suction head (NPSH) even with a RWSP temperature that bounds the temperatures that may occur during a design basis accident. As discussed previously SI flow and CS/RHR flow are available to monitor the performance of these pumps. Therefore, RWSP temperature is not selected as a Type D PAM variable.

Additionally, the SI pumps and the CS/RHR pumps are cooled by component cooling water (CCW) during their operation. The CCW system is an intermediate system that removes heat from important components and transfers the heat to the essential service water (ESW) system via the CCW heat exchangers. The CCW system also provides cooling to the RCPs. Although the RCPs are not required to be available during any Chapter 15 analysis, cooling of the RCP seals is necessary to prevent a seal leakage LOCA from occurring. As a result, it is necessary for the operator to be able to monitor the CCW and ESW systems following an accident. The CCW system provides cooling to many plant components. The flow to each component can be monitored by the operator. However, this requires the operator to check each component separately. The CCW flow to each component comes from a common header (there are two headers that each supply flow to two trains, although the headers can be cross-connected). Since the valves in the CCW system are normally aligned to cool the components, flow to the component is ensured if there is adequate pressure in the CCW headers. This means that the operator can verify the proper status of the CCW system by checking the pressure in the two CCW headers. This is much simpler than verifying the individual flow to each component. Therefore, CCW header pressure is selected as a Type D PAM variable. Additional justification for this selection is as follows:

- Prior to any design basis accident, the CCW system is operable with pressure, temperatures, and flows in their normal ranges
- Following the occurrence of a design basis accident, various CCW valves are automatically repositioned (e.g., to direct cooling flow to CS/RHR heat exchanger during a LOCA)
- The system pressure indicates that the system is operating successfully because the system is a closed loop system (i.e., a pump failure or break in the system would result in a pressure decrease
- The monitoring of flow to individual components receiving CCW flow is not necessary because appropriate flow can be assumed by verification of proper header pressure along with the automatic valve repositioning
- The appropriate functioning of individual components receiving CCW flow is monitored by that component's own indications (e.g., SI flow is selected to monitor the proper functioning of the SI pump, which is cooled by CCW)

Similarly, the proper status of the ESW system can be verified by checking the pressure in the ESW headers. Therefore, ESW header pressure is selected as a Type D PAM variable. Note that there are other parameters that are available for monitoring the performance of the CCW and ESW systems. For example, some operating plants select CCW temperature and flow together, as was done in RG 1.97 Rev. 3. However, MHI has once again selected the Type D PAM variable based on the desire to use the indication that the operators would use as the primary indication of the performance of the system. MHI has selected the header pressure based on an operational perspective after discussing with plant operators. The conclusion is that CCW header pressure and ESW header pressure give the operator the most immediate and accurate indication of the performance of the system of any available indication. For any condition which would degrade the performance of the CCW or ESW systems, such as partial system blockage, the effect on header pressure would be immediately indicated to the operator. A loss of header pressure would indicate to the operator that there is a problem with the system and allow the operator to recognize the potential impact on the safety systems that are supported by CCW and ESW (e.g., SI). Other conditions, such as heat exchanger fouling, are bounded by the design of the systems. Then it is not necessary to include additional parameters, such as temperature and/or flow, to meet criterion “a”. Therefore, the CCW and ESW header pressures are the primary indications that should be selected based on this criterion and are selected as Type D PAM variables.

Another ESF used to mitigate design basis events is the emergency feedwater (EFW) system. The loss of ac power analysis in DCD Subsection 15.2.6 is one of several Chapter 15 events that credit the EFW system for event mitigation. The EFW system has four EFW pumps, with two of the pumps being motor-driven and the other two being turbine-driven. In the US-APWR design, one EFW pump is aligned to each SG. Regardless of which type of EFW pump is used, the operator must be able to verify that the pump is supplying the proper EFW flow to the SG. Therefore, EFW flow is selected as a Type D PAM variable. The EFW pumps take suction from two EFW pits. In order for the pumps to be able to provide the necessary flow credited in the Chapter 15 analyses, the operators need to monitor the EFW pit level while using the EFW system. Therefore, EFW pit water level is selected as a Type D PAM variable.

As described in DCD Section 9.1.3.1, the cooling portion of the spent fuel pit cooling and purification system (SFPCS) performs a safety-related function to maintain the spent fuel pit (SFP) temperature within the appropriate range. Following certain design basis accidents, such as a loss of offsite power (LOOP), the operators must monitor the SFP conditions to ensure that the cooling function of the SFPCS is not degraded. In the scenario where the cooling function continues to degrade, the SFP water could eventually boil, resulting in a loss of SFP inventory that could result in fuel uncovery. This could result in the release of radiation. The analyses for the design basis accidents in Chapter 15 do not analyze this scenario as SFP temperature is assumed to be maintained in an acceptable range throughout the analysis period. The operators can monitor the SFP pump discharge flow to determine if cooling flow is being provided. Maintenance of SFP pump flow following a design basis accident is one indication that indicates the success of the SFP cooling function. Therefore, SFP pump discharge flow is selected as a Type D PAM variable. However, following a LOOP, the SFP pumps trip on an undervoltage signal. For this reason, it is also necessary for the operators to directly monitor the SFP temperature when no active cooling flow is provided. Therefore, SFP temperature is selected as a Type D PAM variable. In addition, SFP level may decrease due to evaporation, especially under conditions of elevated SFP temperatures. Therefore, SFP water level (narrow range) is also selected as a Type D PAM variable.

Criterion “b”

This criterion is related to the performance of systems necessary to achieve and maintain safe shutdown conditions. DCD Section 7.4 describes the systems that are used to perform normal and safe shutdown for the US-APWR. The control of these systems allow operators to transition to and maintain hot standby, transition to cold shutdown through hot shutdown, and maintain cold shutdown. In DCD Section 7.4, safe shutdown is achieved using only safety-related I&C systems. For the purpose of this criterion, the safe shutdown systems are used to select the Type D PAM variables. DCD Table 7.4-2 provides a list of systems and associated instruments used for normal and safe shutdown. Note that some of the instruments used for safe shutdown can be considered backup indications. This is because the Type D PAM variables selected using this criterion were considered a subset of the safe shutdown instruments in DCD Table 7.4-2.

The first safe shutdown system is the safety injection system (SIS). The SIS can be used to maintain RCS inventory and provide RCS boration in order to ensure sufficient shutdown margin. In the US-APWR, the SIS performs these functions during safe shutdown rather than the CVCS. (These functions are performed by the high head injection system and emergency letdown system, which are parts of the SIS.) DCD Table 7.4-2 indicates several instruments are available to monitor the performance of the SIS. Of these instruments, SI pump discharge flow and SI pump minimum flow are the primary instruments used by the operators. Therefore, SI pump discharge flow and SI pump minimum flow are selected as Type D PAM variables. The SI pump discharge pressure and SI pump suction pressure can be considered backup indications. In addition, the SIS also interfaces with the refueling water system (RWS) since the SI pumps take suction from the RWSP. For this reason, the RWS is included in DCD Table 7.4-2. The RWS can be monitored using the RWSP water level (wide range) instrument. Therefore, RWSP water level (wide range) is selected as a Type D PAM variable. The SIS also includes the SI accumulators. When the accumulators are not required, they must be isolated prior to reaching the low RCS pressures characteristic of shutdown conditions.

Isolating the accumulators prevents inadvertent actuation. Successful isolation can be verified by accumulator pressure as indicated in DCD Table 7.4-2. Therefore, accumulator pressure is selected as a Type D PAM variable.

The next safe shutdown system is the nuclear instrumentation system (NIS). The NIS is used by the operators to verify the shutdown margin and ensure the shutdown state by monitoring the neutron flux. The primary indication for the NIS is the wide range neutron flux. Therefore, wide range neutron flux is selected as a Type D PAM variable.

Next, the long-term core cooling in the RCS must be maintained. As indicated in DCD Table 7.4-2, the operators can verify long-term core cooling by monitoring the RCS temperatures. Both RCS hot leg and cold leg temperatures are very useful for the operator to monitor long-term core cooling. Therefore, RCS hot leg (wide range) and RCS cold leg (wide range) temperatures are both selected as Type D PAM variables.

The operator also needs to monitor whether the inventory in the RCS is adequate. If necessary, the SI system provides makeup flow to maintain RCS inventory. The pressurizer water level indication provides a means to monitor RCS inventory. Therefore, pressurizer water level is selected as a Type D PAM variable. It is also necessary to ensure RCS integrity during long-term core cooling. RCS pressure and pressurizer pressure can both be used for this purpose, as indicated in DCD Table 7.4-2. However, only one of the indications is needed, since the other will be available as a backup. For this reason, RCS pressure is selected as a Type D PAM variable (pressurizer pressure is considered the backup instrument).

Safe shutdown conditions also require long-term heat removal from the RCS. As discussed in DCD Subsection 7.4.1.6.2.2, long-term heat removal can be accomplished by steam release from the SGs to the atmosphere, by providing EFW to the SGs, and by using the RHR system (when conditions allow). Therefore, DCD Table 7.4-2 includes the RHR system (RHRS), the EFW system (EFWS), the main steam system (MSS), and the condensate and feedwater system (CFS) as safe shutdown systems. Each of these systems is discussed as follows.

For the EFWS, the operator must be able to verify that the EFW pumps are supplying the proper EFW flow to the SGs in order to remove heat from the RCS. Therefore, EFW flow is selected as a Type D PAM variable.

In order for the pumps to be able to provide the necessary flow in the long-term, the operators need to monitor the EFW pit level while using the EFW system. Therefore, EFW pit water level is selected as a Type D PAM variable. EFW pump discharge pressure is included in DCD Table 7.4-2, but is not selected as Type D PAM since it is considered a backup indication to EFW flow.

For the CFS, sufficient water level must be maintained in the SGs in order to efficiently remove heat. The operators can verify the SG water level on the wide range. Therefore, SG water level (wide range) is selected as a Type D PAM variable.

For the MSS, the SGs will only function properly if they are maintained at the appropriate pressure. If the pressure is too low or too high, the SGs will not be able to remove enough heat from the RCS. The operators can monitor the main steam line pressure to ensure proper operation of the SGs. Main steam line pressure also confirms that steam flow from the SGs is occurring as expected. Therefore, main steam line pressure is selected as a Type D PAM variable.

Long-term heat removal may also be provided by the RHRS. RHR cooling is typically used as the plant approaches cold shutdown conditions. The operator must be able to verify the RHR system flow to ensure long-term cooling at cold shutdown. Therefore, CS/RHR pump discharge flow and CS/RHR pump minimum flow are selected as Type D PAM variables. From an operational perspective, the RHR system flow gives the operator the most immediate and accurate indication of the performance of the RHR system. A loss of RHR flow would indicate to the operator that there is a problem with the system and allow the operator to recognize the potential impact on long-term heat removal. In addition, the operator monitors the success of long-term heat removal by monitoring the hot and cold leg RCS temperatures as primary information. Since the hot and cold leg RCS temperatures are already selected as Type D PAM variables to satisfy criterion “b” as discussed above, the RHR heat exchanger outlet temperature is not required to provide primary indication of the performance of the RHR system. For these reasons, RHR heat exchanger outlet temperature and the other RHRS instruments listed in DCD Table 7.4-2, except for the pump discharge flow and minimum flow, are considered backup indications and are not selected as Type D PAM variables.

As described previously in the criterion “a” discussion, the essential service water system (ESWS) and component cooling water system (CCWS) are supporting systems for the SIS. DCD Table 7.4-2 indicates that several instruments are available to monitor the ESWS and CCWS under safe shutdown conditions. However, as described previously, the header pressures for these two systems are the primary means for the operator to monitor these two systems. The other indications, including flow, are considered backup. Note that this is not inconsistent with the previous selection of CS/RHR flow described above. The reason for the difference is that the CS/RHR flow is indicative of system performance since the primary function is to supply containment spray. The header pressure is indicative of CCW and ESW system performance and flow indication would not be sufficient to ensure system function. Therefore, ESW header pressure and CCW header pressure are selected as Type D PAM variables.

Criterion “c”

This criterion is related to checking the status of safety systems. Since many safety systems are credited in the Chapter 15 accident analysis, many of the variables for verifying system status have already been selected as Type D variables as part of criterion “a” above. There are a few additional variables to consider though due to criterion “c”.

The US-APWR is designed such that containment isolation valves will automatically close when containment pressure increases to a certain setpoint. This safety feature is described in DCD Subsection 7.3.1.5. The operator verifies this automatic action by checking the position of the containment isolation valves. Therefore, containment isolation valve positions are selected as Type D PAM variables. Note that some containment isolation valves are check valves. Since they are passive valves that fail in a safe position, the operators do not need to monitor the check valve positions and therefore check valves are excluded from Type D. The US-APWR has another set of containment valves known as the containment purge isolation valves. Similar to the containment isolation valves described above, the operator will check the containment purge isolation valve positions to verify the system status. As a result, the containment purge isolation valve position indications are selected as Type D PAM variables.

The US-APWR safety systems are designed to be powered by the Class 1E ac busses. As described in DCD Subsection 8.3.1, the Class 1E ac busses are normally powered by the offsite power supply. In the event where the offsite power supply is lost, the Class 1E ac busses can also be powered by Class 1E gas turbine generators. The US-APWR also has Class 1E dc busses. The Class 1E dc busses are used to provide continuous power for controls, instrumentation, and dc motors as described in DCD Subsection 8.3.2. Since these power sources are necessary for the safety systems to function properly, the operators must be able to monitor the status of the power sources. Therefore, the status of standby power and other energy sources important to safety (Class 1E ac bus voltage and Class 1E dc bus voltage) is selected as a Type D PAM variable.

The US-APWR has a main control room (MCR) isolation function as described in DCD Subsection 7.3.1.5. This function automatically switches the MCR HVAC system to pressurization mode when the radiation levels outside the MCR are high. This design feature reduces the dose to MCR personnel during design basis accidents. The MCR isolation function results in the repositioning of several dampers in the MCR HVAC system. The operator can use the MCR HVAC damper position indications in order to verify the status of the MCR HVAC system. Therefore, these MCR HVAC damper positions meet criterion “c”. As a result, the MCR HVAC damper position indications are selected as Type D PAM variables. Note that these indications are selected to allow the operator to monitor the performance of the MCR HVAC system in limiting the MCR operators exposure to radiation. The actual monitoring of radiation in the control room is discussed in the section on Type E PAM variables.

It is noted that the MCR process monitors (i.e., MCR outside air intake radiation detector) is located in the process lines, outside of the MCR. Therefore, when the MCR is isolated by the MCR isolation with high MCR outside air intake radiation, the radiation level of the process monitor will be high. This does not tell the operator whether the MCR HVAC system is operating correctly or not, it would only indicate the need for the MCR HVAC system to operate. In a similar way, the MCR area monitor is located in the MCR. The radiation level in the MCR depends on the specific accident event so that the radiation level inside the MCR will not always be low when the MCR isolation is initiated. Therefore, both the MCR process monitor and area monitor are not reliable for monitoring for the achievement of the safety function. In addition, MCR isolation will occur upon ECCS actuation as described in DCD Chapter 7. ECCS actuation can occur for events where there is no significant radiation. In those cases, the radiation detectors would not provide any information regarding the MCR HVAC status. Instead, MHI added the MCR HVAC Damper Position as the Type D variable for the direct measurement of the system. Therefore, both MCR process monitor and area monitor are not assigned as Type D variables, only Type E.

In a similar manner to the MCR explanation above, the TSC process monitor (i.e., TSC outside air intake radiation detector) is located in the process lines, outside of the TSC. Therefore, when the TSC is isolated by the TSC isolation with high TSC outside air intake radiation, the radiation level of the process monitor will be high. This does not tell the operator whether the TSC HVAC system is operating correctly or not, it would only indicate the need for the TSC HVAC system to operate. In a similar way, the TSC area monitor is located in the TSC. The radiation level in the TSC depends on the specific accident event so that the radiation level inside the TSC will not always be low when the TSC isolation is initiated. Therefore, both the TSC process monitor and area monitor are not reliable for monitoring for the achievement of the isolation function. In addition, the TSC and the function in the TSC is categorized as non-safety, therefore, there is no safety function to monitor. Therefore, both TSC process monitor and area monitor are not assigned as Type D variables, only Type E.

The US-APWR reactor coolant system is equipped with pressurizer safety valves and safety depressurization valves. These valves provide the capability to relieve excessive pressure in the primary system. The safety valves open and close automatically, so it is not typically necessary to monitor the valve positions. The safety depressurization valves are normally closed and only opened by operator action, so it is expected that the operator would not need to check the valve positions. A pressurizer safety valve or safety depressurization valve that did not properly open or close would result in an impact on RCS pressure and other primary system parameters, such as temperature or subcooling, that could be detected by the operator. However, in order to very quickly and simply verify the system status, the operator could just monitor the valve position indications. Therefore, these position indications meet criterion “c” for Type D PAM variables. As a result, the pressurizer safety valve and safety depressurization valve position indications are selected as Type D PAM variables.

The US-APWR main steam supply system is equipped with main steam safety, relief, and depressurization valves. These valves provide the capability to relieve excessive pressure in the main steam lines. The safety and relief valves open and close automatically, so it is not typically necessary to monitor the valve positions. The depressurization valves are normally closed and only opened by operator action, so it is expected that the operator would not need to check the valve positions. The main steam system also contains main steam isolation valves and other associated valves that are automatically closed on a main steam isolation signal to isolate steam flow from the steam generators as described in DCD Subsection 7.3.1.5. Any of the main steam isolation valves or a main steam safety, relief, or depressurization valve that was in the incorrect position would result in an impact on main steam line pressure and other secondary system parameters that could be detected by the operator. However, in order to very quickly and simply verify the system status, the operator could just monitor the valve position indications. Therefore, these position indications meet criterion “c” for Type D PAM variables. As a result, the main steam isolation valve (and associated valve) position indications, main steam safety valve position indications, main steam relief valve position indications, and main steam depressurization valve position indications are selected as Type D PAM variables.

The US-APWR main feedwater system is equipped with main feedwater isolation valves. These valves and other associated valves are automatically closed on a main feedwater isolation signal to isolate feedwater flow to the steam generators as described in DCD Subsection 7.3.1.5. Any of the main feedwater isolation valves that were in the incorrect position would result in an impact on SG water level and other secondary system parameters that could be detected by the operator. However, in order to very quickly and simply verify the system status, the operator could just monitor the valve position indications. Therefore, these position indications meet criterion “c” for Type D PAM variables. As a result, the main feedwater isolation valve (and associated valve) position indications are selected as Type D PAM variables. In a similar way, the emergency feedwater system is equipped with emergency feedwater valves. These valves are automatically closed on an emergency feedwater isolation signal and are automatically opened on an emergency feedwater actuation signal as described in DCD Subsection 7.3.1.5. The emergency feedwater actuation signal also results in the automatic closure of several associated valves that are not closed on the main feedwater isolation signal but help to ensure the SGs are isolated. Although the impact of an incorrect valve could be detected by secondary system parameters, the operators can verify the system status using the valve positions, thus meeting criterion “c”. As a result, the emergency feedwater isolation valve (and associated valve) position indications are selected as Type D PAM variables.

As discussed in criterion “b”, the RHR system is used to provide long-term cooling at cold shutdown. Under the temperature and pressure conditions associated with cold shutdown, it is important to protect against overpressure conditions in the RCS. The pressurizer safety valves, described as part of criterion “a”, are not available in these conditions. Therefore, the US-APWR has a Low Temperature Overpressure Protection system which consists of CS/RHR pump suction relief valves that are capable of mitigating pressure transients during cold shutdown. Monitoring the valve positions provides a very efficient and simple way for the operators to verify the system status. As a result, the CS/RHR pump suction relief valve position indications are selected as Type D PAM variables.

Summary for Type D PAM

In general, the Type D PAM variables are checked during the performance of EOPs. In many US and Japanese plants, the status of many systems are checked at the very beginning of the EOPs, usually in the first EOP entered. This is based on operating experience. Consistent with this operating experience, MHI has developed the list of Type D PAM variables so that they can be quickly checked during the EOPs to ensure systems are operating as expected, in accordance with the IEEE Std 497-2002 criteria. For the US-APWR, the majority of these systems are checked in the entry procedure E-0, Reactor Trip or Safety Injection. A few systems related to maintaining long-term safe shutdown conditions are checked during later performance of FRGs. During the audit in February 2012, the NRC staff was able to look at the current US-APWR E-0 and FRGs and verify that the Type D PAM variables were used to monitor the status of safety systems as expected. This provided additional confirmation that the Type D PAM variables were selected in a manner consistent with the intent of IEEE Std 497-2002 and RG 1.97 Rev. 4.

As a final check of the adequacy of the US-APWR Type D PAM variables, MHI performed a detailed comparison between the Type D variables included in the MHI PAM list and those included in RG 1.97 Rev. 3 Table 3. This comparison is provided in Table H.4-1. For each difference, MHI has provided a detailed explanation of the basis for the difference in Table H.4-1. One notable difference that was discussed previously was that the US-APWR does not have a low pressure injection system and therefore has no Type D PAM variables associated with this system. Another notable departure from the RG 1.97 Rev. 3 Type D variable list involves the chemical volume and control system (CVCS). The SI system (the high head injection system and emergency letdown system) of the US-APWR has a required safety function to ensure a means for boration and RCS inventory control if the normal CVCS is unavailable. The ability of the SI system to perform this function is monitored by indications such as SI flow, RCS pressure, pressurizer water level, and RWSP water, which are all selected as Type D PAM variables as described in detail above. Since the US-APWR SI system performs the necessary RCS inventory and boration functions, the CVCS-related monitoring variables are not necessary for the US-APWR design and thus are not included in the MHI Type D PAM variable list.

H.5 Type E Variables

MHI utilized the performance-based criteria of RG 1.97 Rev. 4 and IEEE Std 497-2002 to select the Type E accident monitoring variables for the US-APWR. IEEE Std 497-2002 defines Type E variables as follows.

> Type E variables are those variables required for use in determining the magnitude of the release of radioactive materials and continually assessing such releases.

The selection of these variables shall include, but not be limited to, the following:

a) Monitor the magnitude of releases of radioactive materials through identified pathways (e.g., secondary safety valves, and condenser air ejector).

b) Monitor the environmental conditions used to determine the impact of releases of radioactive materials through identified pathways (e.g., wind speed, wind direction, and air temperature).

c) Monitor radiation levels and radioactivity in the plant environs.

d) Monitor radiation levels and radioactivity in the control room and selected plant areas where access may be required for plant recovery.

As described above, there are four criteria identified in IEEE Std 497-2002 for selecting variables related to monitoring radiological releases. Each of the criteria is discussed below.

Criterion “a”

The US-APWR is designed to prevent the release of radioactive material in general. However, radioactive material may be released during some accidents. The radioactive materials are released through known pathways, depending on the accident. By monitoring these pathways, the operator will be able to determine if/when radioactive materials have been released.

For some accidents that result in radioactive material release, the radioactive material will be released into the containment vessel. For example, a LOCA will result in the release of primary coolant into containment. Since the primary coolant may be radioactive, especially if fuel damage has occurred, the radiation levels in the containment will increase. Since the containment vessel is one pathway where radiation may be released, the operators monitor the radiation in the containment. The containment high range area radiation indication is the best means available for the operator to monitor containment radiation. Therefore, containment high range area radiation is selected as a Type E PAM variable.

A SGTR results in primary-to-secondary leakage. This allows radioactive primary coolant to enter the main steam system. As a result, the main steam system is another pathway for radioactive material release. The main steam lines are monitored for radiation as described in DCD Subsection 11.5.2.2.4. Therefore, main steam line radiation is selected as a Type E PAM variable.

Steam from the main steam system is condensed in the condenser. Non-condensable gases are removed from the condenser and vented using condenser vacuum pumps. The operators monitor the exhaust from these pumps for radiation as described in DCD Subsection 11.5.2.4.2. In the case of an SGTR, the exhaust radiation may be high due to the primary-to-secondary leakage. Therefore, condenser vacuum pump exhaust line radiation (including high range) is selected as a Type E PAM variable.

Similar to the condenser exhaust fan, the gland seal system (GSS) exhaust fan also removes non-condensable gases from the secondary side. A SGTR may result in high radiation in the GSS due to the primary-to-secondary leakage. The operators monitor the GSS exhaust for radiation as described in DCD Subsection 11.5.2.4.3. Therefore, GSS exhaust fan discharge line radiation (including high range) is selected as a Type E PAM variable.

Another pathway for radioactive material release is the plant vent. The plant vent receives the discharge from the containment purge, auxiliary building, control building, fuel building, and the condenser air removal filtration system. Radioactive materials that are released in any of these buildings will be collected by the HVAC system in the building and directed to the plant vent for release. The plant vent is equipped with several different radiation monitors corresponding to different radiation ranges as described in DCD Subsection 11.5.2.4.1. The combination of these monitors allows the operators to monitor radiation during normal operation and following accidents. Therefore, the plant vent radiation gas radiation (including high range) is selected as a Type E PAM variable.

In addition, the plant air vent high concentration sampling system is also selected as a Type E PAM variable.

There are no other release points in the US-APWR.

Criterion "b"

Following an accident that results in radiological releases, the operators and plant staff need to be able to monitor the local environmental conditions. The spread of radioactive materials will very much depend on the wind speed and direction and other meteorological parameters, such as estimation of atmospheric stability. Therefore, these parameters are selected as Type E PAM variables. However, the actual instruments to measure these parameters will be very site specific. The location for placing these monitors will also highly depend on the site specific plant location. Therefore, the description of the instruments to measure these parameters cannot be part of the standard design of the US-APWR. Instead, this information must be provided by the COL applicant as described in DCD Subsection 7.5.1.1. This COL applicant requirement is described in COL Item 7.5(1). As a result, MHI has selected the Type E PAM variables based on criterion "b" for the standard plant design. However, MHI expects that the COL applicants will provide additional information regarding the selection of these meteorological parameters as Type E PAM variables based on criterion "b" in their PAM lists.

Criterion "c"

The operators need to monitor the plant environs to determine radiation levels and radioactivity following an accident. Therefore, plant and environs radiation is selected as a Type E PAM variable. Plant and environs radioactivity is also selected as a Type E PAM variable. Note that this instrumentation is portable.

Another way in which the operators can monitor the plant environs is by indications of airborne radio halogens and particulates. This indication is provided by portable sampling and then is analyzed onsite. Therefore, airborne radio halogens and particulates (portable sampling with onsite analysis capability) is selected as a Type E PAM variable.

Criterion "d"

Operators respond to a plant accident from the main control room (MCR). The US-APWR is designed such that the operators can shutdown the plant to cold shutdown from the MCR as described in DCD Subsection 7.4.1.1. In order to protect the operators from radiation, the US-APWR includes design features to prevent radioactive materials from entering the MCR. (The selection of PAM variables for these design features was discussed in the Type D section.) Although these design features exist, the operators still need to be able to monitor the radiation levels in the MCR in order to ensure their safety. Any radiation monitors for the MCR would thus meet criterion "d".

Radiation within the control room itself is monitored by the MCR area radiation indication. Therefore, MCR area radiation is selected as a Type E PAM variable.

The HVAC system for the MCR has an air intake that could possibly be a pathway for radioactive materials to enter the MCR. This pathway is monitored using the MCR outside air intake radiation indication. Therefore, MCR outside air intake radiation is selected as a Type E PAM variable.

The criterion also identifies other areas where actions for plant recovery may need to be performed. As discussed previously, the US-APWR can be safely shutdown from the MCR (or also the remote shutdown room). However, during an accident, the MCR operators may consult with the staff in the technical support center (TSC). Although actions are not performed in the TSC, it is also necessary to monitor the radiation in the TSC to protect TSC staff from radiation. Therefore, TSC area radiation is selected as a Type E PAM variable.

Similar to the MCR, the TSC also has an air intake where radioactive materials could enter the TSC. Therefore, TSC outside air intake radiation is selected as a Type E PAM variable.

The MCR and TSC are the only areas where actions for plant recovery are expected. There are no other specific areas where planned actions for plant recovery are required. For this reason, no other specific area radiation indications are selected based on criterion “d”. However, depending on the accident scenario, it is possible that plant personnel may have to enter some areas. In those cases, radiation exposure will be monitored by using portable radiation monitors and air sampling. Those portable instruments are already selected as Type E PAM variables based on criterion “c” as discussed above.

Summary for Type E PAM

In summary, MHI has used the performance-based criteria from IEEE Std 497-2002 to select the Type E PAM variables based on the US-APWR design information in the DCD. As discussed previously, ERGs for the US-APWR were not available at the time the PAM list was developed. However, the method of monitoring radioactive releases in the US-APWR is the same as those used by domestic Japanese plants and also by many US operating plants. Thus MHI believes that the Type E PAM variables do take into account operational experience and previously existing procedures. For these reasons, MHI believes that the US-APWR Type E PAM variables have been selected in a manner consistent with the intent of IEEE Std 497-2002 and RG 1.97 Rev. 4.

As a final check of the adequacy of the US-APWR Type E PAM variables, MHI performed a detailed comparison between the Type E variables included in the MHI PAM list and those included in RG 1.97 Rev. 3 Table 3. This comparison is provided in Table H.5-1. For each difference, MHI has provided a detailed explanation of the basis for the difference in Table H.5-1.

Miscellaneous Requirements

As discussed previously, RG 1.97 Rev. 3 provided a prescriptive list of PAM variables. Some of the variables included in RG 1.97 Rev. 3 were placed on the PAM list in order to satisfy requirements related to TMI. These TMI-related requirements are defined in 10 CFR 50.34(f). By utilizing the RG 1.97 Rev. 3 PAM list, some of the TMI-related requirements were also met at the same time. For example, 10 CFR 50.34(f)(2)(xvi) requires that containment hydrogen concentration be displayed in the control room and the RG 1.97 Rev. 3 PAM list includes containment hydrogen concentration as a Type C variable. Since MHI utilized the performance-based approach in RG 1.97 Rev. 4 and IEEE Std 497-2002, some of the variables related to these TMI requirements, such as containment hydrogen concentration, were not included in the US-APWR PAM list. However, MHI does address the TMI-related requirements elsewhere in the DCD. DCD Tier 2 Chapter 1 Table 1.9.3-2 provides the reference to the appropriate section in the DCD that addresses each of the TMI-related requirements from 10 CFR 50.34(f). Table 1.9.3-2 indicates that the containment hydrogen concentration requirement is met as described in DCD Subsection 6.2.5. Therefore, MHI is in compliance with all of the TMI-related requirements of 10 CFR 50.34(f).

IEEE Std 497-2002 and RG 1.97 Rev. 4 also briefly address the concept of a common mode or common cause failure of instrumentation channels. The use of identical software in redundant instrumentation channels is acceptable as long as an analysis has been performed to demonstrate defense-in-depth against common cause failure. MHI has performed a detailed defense-in-depth and diversity (D3) analysis as described in DCD Section 7.8. The review of MHI's D3 design and analysis is being addressed as part of the review of DCD Section 7.8 and is therefore outside the scope of the PAM list.

Summary

MHI has developed the PAM list in DCD Table 7.5-3 based on the performance-based approach identified in IEEE Std 497-2002 and RG 1.97 Rev. 4. IEEE Std 497-2002 indicated that the plant procedures (EOPs and AOPs) can be used as source documents for the performance-based approach. However, the plant procedures are not the only source documents. Other source documents identified in IEEE Std 497-2002 include plant accident analysis licensing basis, plant critical safety functions (which are defined in IEEE Std 497-2002), and design basis documentation (of fission product barriers). MHI did not have US-APWR specific procedures available at the time the PAM list was developed. Therefore, MHI did not use EOPs or AOPs as source documents. However, MHI did use the other source documents as described in IEEE Std 497-2002. In the case where IEEE Std 497-2002 recommended using procedures as the source documents, MHI used other design basis documentation as the source documents. In addition, MHI utilized the operating experience and knowledge of US and Japanese plants during the process. As a result, MHI believes that the PAM list has been selected in a manner consistent with the intent of IEEE Std 497-2002 and RG 1.97 Rev. 4.

Table H.1-1 Basis for Differences between NUREG-1431 Table 3.3.3-1 and the US-APWR Type A PAM List (Sheet 1 of 7)

RG 1.97 Function	Purpose	NUREG-1431 Table 3.3.3-1 Variable	Corresponding US-APWR Type A PAM Variable	Basis for Difference
Reactivity Control	Indication of subcritical conditions	Power Range Neutron Flux	Wide Range Neutron Flux	Wide range neutron flux is used to confirm the appropriate operator action to terminate a boron dilution following an alarm associated with the boron dilution. Therefore, the selection criterion a) of IEEE Std 497-2002 is applicable. This is a Type A variable for the US-APWR. Note that wide range neutron flux covers the full power range as well as extending below the power range.
Reactivity Control	Indication of subcritical conditions	Source Range Neutron Flux	-	Neither selection criteria a) nor b) of IEEE Std 497-2002 are applicable to this parameter because there are no manual actions based on this parameter in the safety analysis. Therefore, this is not a Type A variable for the US-APWR.
Core Cooling	Indication of core cooling; Manual action; Long-term core cooling	RCS Hot Leg Temperature	Reactor Coolant Hot Leg Temperature (Wide Range)	Intact loop hot leg temperature is used to determine when to terminate the RCS cooldown and when to initiate RCS depressurization in the SGTR analysis. Therefore, the selection criterion a) of IEEE Std 497-2002 is applicable. This is a Type A variable for the US-APWR.

Table H.1-1 Basis for Differences between NUREG-1431 Table 3.3.3-1 and the US-APWR Type A PAM List (Sheet 2 of 7)

RG 1.97 Function	Purpose	NUREG-1431 Table 3.3.3-1 Variable	Corresponding US-APWR Type A PAM Variable	Basis for Difference
Core Cooling	Indication of core cooling; Long-term core cooling	RCS Cold Leg Temperature	Reactor Coolant Cold Leg Temperature (Wide Range)	This parameter is not explicitly assumed in the safety analysis. However, monitoring of this parameter is necessary for cooling down after mitigating an AOO. Therefore, the selection criterion b) of IEEE Std 497-2002is applicable. This is a Type A variable for the US-APWR.
Core Cooling; Maintaining RCS Integrity; RCS Pressure Boundary; Primary Coolant System	-SGTR Safety Analysis Manual Action -RCS Depressurization based on EOPs for SGTR event	RCS Pressure (Wide Range)	Reactor Coolant Pressure	No difference. This is a Type A variable for the US-APWR.
Core Cooling	To ensure RCS inventory	Reactor Vessel Water Level	-	Neither selection criteria a) nor b) of IEEE Std 497-2002 are applicable to this parameter because there are no manual actions based on this parameter in the safety analysis. Therefore, this is not a Type A variable for the US-APWR. Note that RV Water Level is a Type B and D variable for the US-APWR.

Table H.1-1 Basis for Differences between NUREG-1431 Table 3.3.3-1 and the US-APWR Type A PAM List (Sheet 3 of 7)

RG 1.97 Function	Purpose	NUREG-1431 Table 3.3.3-1 Variable	Corresponding US-APWR Type A PAM Variable	Basis for Difference
Core cooling; Maintaining RCS Integrity; RCS Pressure Boundary	Indication of core cooling function for RWSP switchover and status of ECCS recirculation delivery	Containment Sump Water Level (Wide Range)	-	Neither selection criteria a) nor b) of IEEE Std 497-2002 are applicable to this parameter since the US-APWR RWSP is located inside containment and does not require manual action to switch over to the recirculation sump. Therefore, this is not a Type A variable for the US-APWR. Note that RWSP level is a Type B and D variable for the US-APWR.
Maintaining Containment and RCS Integrity; RCS Pressure Boundary	Indication of containment integrity function	Containment Pressure	-	Neither selection criteria a) nor b) of IEEE Std 497-2002 are applicable to this parameter because there are no manual actions based on this parameter in the safety analysis. Therefore, this is not a Type A variable for the US-APWR. Note that Containment Pressure is a Type B, C, and D variable for the US-APWR.

Table H.1-1 Basis for Differences between NUREG-1431 Table 3.3.3-1 and the US-APWR Type A PAM List (Sheet 4 of 7)

RG 1.97 Function	Purpose	NUREG-1431 Table 3.3.3-1 Variable	Corresponding US-APWR Type A PAM Variable	Basis for Difference
Containment Isolation/Integrity	Indication of containment integrity function	Penetration Flow Path Containment Isolation Valve Position	-	Neither selection criteria a) nor b) of IEEE Std 497-2002 are applicable to this parameter because there are no manual actions based on this parameter in the safety analysis. Therefore, this is not a Type A variable for the US-APWR. Note that C/V Isolation Valve Position is a Type B and D variable for the US-APWR.
Containment Radiation; RCS Pressure Boundary	Identify challenge to fission product barrier	Containment Area Radiation (High Range)	Containment High Range Area Radiation	No difference. Containment high range area radiation is used to prompt manual operator actions during a rod ejection event. Therefore, the selection criterion a) of IEEE Std 497-2002 is applicable. This is a Type A variable for the US-APWR.
Primary Coolant System; RCS Pressure Boundary	To ensure proper operation of the pressurizer	Pressurizer Level	Pressurizer Water Level	No difference. Pressurizer level is also used to prompt manual operator actions during a steam generator tube rupture event. Therefore, the selection criterion a) of IEEE Std 497-2002 is applicable. This is a Type A variable for the US-APWR.

Table H.1-1 Basis for Differences between NUREG-1431 Table 3.3.3-1 and the US-APWR Type A PAM List (Sheet 5 of 7)

RG 1.97 Function	Purpose	NUREG-1431 Table 3.3.3-1 Variable	Corresponding US-APWR Type A PAM Variable	Basis for Difference
Secondary System; RCS Pressure Boundary	Verification of heat sink availability	Steam Generator Water Level (Wide Range)	-	Neither selection criteria a) nor b) of IEEE Std 497-2002 are applicable to this parameter because there are no manual actions based on this parameter in the safety analysis. SG narrow range level is applied in the safety analysis instead of this parameter. Therefore, this is not a Type A variable for the US-APWR. Note that SG Wide Range Level is a Type B and D variable for the US-APWR.
Auxiliary Feedwater System	Indication of ability to maintain SG heat sink and indication of long-term AFW operation	Condensate Storage Tank Level	-	The EFW pit has sufficient water to maintain long term core cooling to mitigate AOOs and PAs. Therefore, neither selection criteria a) nor b) are applicable to this parameter because there are no manual actions based on this parameter in the safety analysis. Therefore, this is not a Type A variable for the US-APWR. Note that EFW Pit Water Level is a Type B and D variable for the US-APWR.

Table H.1-1 Basis for Differences between NUREG-1431 Table 3.3.3-1 and the US-APWR Type A PAM List (Sheet 6 of 7)

RG 1.97 Function	Purpose	NUREG-1431 Table 3.3.3-1 Variable	Corresponding US-APWR Type A PAM Variable	Basis for Difference
Core Cooling; Fuel Cladding Integrity; Maintain RCS Integrity; RCS Pressure Boundary; Primary Coolant System	Indication of core cooling	Core Exit Temperature – Quadrant [1]-[4]	-	Neither selection criteria a) nor b) are applicable to this parameter because there are no manual actions based on this parameter in the safety analysis. Therefore, this is not a Type A variable for the US-APWR. Note that Core Exit Temperature is a Type B and C variable for the US-APWR.
Auxiliary Feedwater System	Verification of automatic actuation and ability to satisfy heat sink requirements	Auxiliary Feedwater Flow	EFW Flow	No difference. This parameter is used to determine if the ECCS termination criteria are met in the SGTR analysis. EFW Flow is a Type A parameter for the US-APWR.
Secondary System	Verification of manual action for SGTR termination (along w/ RCS Pressure)	-	Main Steam Line Pressure	This parameter is used to determine when to terminate the RCS cooldown and when to initiate RCS depressurization in the SGTR analysis. Therefore, this is a Type A variable for the US-APWR.
Secondary System; RCS Pressure Boundary	Verification of heat sink availability	-	SG Water Level (Narrow Range)	This parameter is used to identify the ruptured SG in the SGTR analysis. This parameter is also monitored by the operator to determine if the ECCS termination criteria are met in the SGTR analysis. Therefore, this is a Type A variable for the US-APWR.

Table H.1-1 Basis for Differences between NUREG-1431 Table 3.3.3-1 and the US-APWR Type A PAM List (Sheet 7 of 7)

RG 1.97 Function	Purpose	NUREG-1431 Table 3.3.3-1 Variable	Corresponding US-APWR Type A PAM Variable	Basis for Difference
Core Cooling	Indication of core cooling	-	Degrees of Subcooling	This parameter is monitored by the operator to determine if the criteria for terminating the RCS depressurization or terminating ECCS are met in the SGTR analysis. Therefore, this is a Type A variable for the US-APWR.
RCS Pressure Boundary	Verification of manual action for isolation of failure of small lines carrying primary coolant outside containment	-	Charging Flow	This parameter is monitored by the operator to determine if isolation of the RCS sample line or CVCS letdown line is necessary in the analysis of the radiological consequences of the failure of small lines carrying primary coolant outside containment. Therefore, this is a Type A variable for the US-APWR.

Table H.2-1 Basis for Type B Differences between RG 1.97 Rev.3 and the US-APWR PAM List (Sheet 1 of 3)

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Reactivity Control			
Neutron Flux	Function detection; accomplishment of mitigation	Wide Range Neutron Flux	No difference This is a Type B variable for the US-APWR.
Control Rod Position	Verification	-	This is considered a Category 3 or backup indication in RG 1.97 Rev. 3. Reactivity control is directly monitored by neutron flux. Control rod position provides back-up indication of reactor shutdown. Since the primary indication is neutron flux, which is already a PAM variable, control rod indication is not included in the US-APWR PAM list.
RCS Soluble Boron Concentration	Verification	-	This is considered a Category 3 or backup indication in RG 1.97 Rev. 3. Reactivity control is directly monitored by neutron flux. RCS soluble boron concentration is not monitored continuously, but only obtained periodically. Since the primary indication is neutron flux, which is already a PAM variable, RCS soluble boron concentration is not included in the US-APWR PAM list.
RCS Cold Leg Water Temperature	Verification	Reactor Coolant Cold Leg Temperature (Wide Range)	No difference. This is a Type B variable for the US-APWR.
Core Cooling			
RCS Hot Leg Water Temperature	Function detection; accomplishment of mitigation; verification; long-term surveillance	Reactor Coolant Hot Leg Temperature (Wide Range)	No difference. This is a Type B variable for the US-APWR.
RCS Cold Leg Water Temperature	Function detection; accomplishment of mitigation; verification; long-term surveillance	Reactor Coolant Cold Leg Temperature (Wide Range)	No difference. This is a Type B variable for the US-APWR.
RCS Pressure	Function detection; accomplishment of mitigation; verification; long-term surveillance	Reactor Coolant Pressure	No difference. This is a Type B variable for the US-APWR.
Core Exit Temperature	Verification	Core Exit Temperature	No difference. This is a Type B variable for the US-APWR.

Table H.2-1 Basis for Type B Differences between RG 1.97 Rev.3 and the US-APWR PAM List (Sheet 2 of 3)

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Coolant Inventory	Verification; accomplishment of mitigation	RV Water Level	Reactor vessel water level is a key indication of adequate inventory for core cooling. There is no difference in the intent of these two variables.
Degrees of Subcooling	Verification and analysis of plant conditions	Degrees of Subcooling	No difference. This is a Type B variable for the US-APWR.
Maintaining Reactor Coolant System Integrity			
RCS Pressure	Function detection; accomplishment of mitigation	Reactor Coolant Pressure	No difference. This is a Type B variable for the US-APWR.
Containment Sump Water Level	Function detection; accomplishment of mitigation; verification	Refueling Water Storage Pit Water Level (Wide Range) Refueling Water Storage Pit Water Level (Narrow Range)	Unlike some current operating plants, the US-APWR RWSP is located inside containment. The US-APWR RWSP essentially combines the functions of the sump and RWSP. Therefore, the RWSP water level meets the intent of this monitoring variable and there is no difference between RG 1.97 Rev 3 and the US-APWR PAM list.
Containment Pressure	Function detection; accomplishment of mitigation; verification	Containment Pressure	No difference. This is a Type B variable for the US-APWR.
Maintaining Containment Integrity			
Containment Isolation Valve Position (excluding check valves)	Accomplishment of isolation	Containment Isolation Valve Position (Excluding Check Valves)	No difference. This is a Type B variable for the US-APWR.
Containment Pressure	Function detection; accomplishment of mitigation; verification	Containment Pressure	No difference. This is a Type B variable for the US-APWR.
Other			
-	-	Pressurizer Water Level	This parameter is important to monitor because it is related to the SI termination criteria. The SI termination criteria are related to maintaining adequate RCS inventory to assure core cooling. In addition, this parameter is also related to RCS integrity by preventing water relief through pressurizer safety valves.

Table H.2-1 Basis for Type B Differences between RG 1.97 Rev.3 and the US-APWR PAM List (Sheet 3 of 3)

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
-	-	Main Steam Line Pressure	This parameter is important to monitor the efficiency of the secondary heat sink for removing the core decay heat. Adequate secondary heat sink ensures that core cooling can be maintained.
-	-	SG Water Level (Wide Range)	This parameter provides indication of the secondary heat sink availability for removing core decay heat. Adequate secondary heat sink ensures that core cooling can be maintained.
-	-	SG Water Level (Narrow Range)	This parameter provides indication of the secondary heat sink availability for removing core decay heat. Adequate secondary heat sink ensures that core cooling can be maintained.
-	-	EFW Flow	This parameter provides verification of the automatic actuation of EFW for secondary heat sink availability. Adequate secondary heat sink ensures that core cooling can be maintained.
-	-	EFW Pit Water Level	This parameter provides indication of the secondary heat sink availability for removing core decay heat. Adequate secondary heat sink ensures that core cooling can be maintained.
-	-	Containment High Range Area Radiation	This parameter provides indication of the radiation level in containment. This parameter is related to containment integrity by ensuring containment is isolated when radiation levels are high.

Table H.3-1 Basis for Type C Differences between RG 1.97 Rev.3 and the US-APWR PAM List (Sheet 1 of 3)

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Fuel Cladding			
Radioactivity Concentration or Radiation Level in Circulating Primary Coolant	Detection of breach	Radioactivity Concentration or Radiation Level in Circulating Primary Coolant	No difference. This is a Type C variable for the US-APWR.
Core Exit Temperature	Detection of breach	Core Exit Temperature	No difference. This is a Type C variable for the US-APWR.
Analysis of Primary Coolant (Gamma Spectrum)	Detail analysis; accomplishment of mitigation; verification; long-term surveillance	-	The concentration of each radioactive nuclide can be derived from periodic RCS sampling. However, this is considered a Category 3 or backup indication in RG 1.97 Rev. 3. The primary indications for monitoring fuel cladding are core exit temperature and radioactivity concentration or radiation level in circulating primary coolant. Therefore, analysis of primary coolant (gamma spectrum) is not included as a Type C PAM variable for the US-APWR.
Reactor Coolant Pressure Boundary			
RCS Pressure	Detection of potential for or actual breach; accomplishment of mitigation; long-term surveillance	Reactor Coolant Pressure	No difference. This is a Type C variable for the US-APWR.
Containment Pressure	Detection of breach; accomplishment of mitigation; long-term surveillance	Containment Pressure	No difference. This is a Type C variable for the US-APWR.
Containment Sump Water Level	Detection of breach; accomplishment of mitigation; long-term surveillance	-	Containment pressure is a more direct indication of a potential reactor coolant pressure boundary breach. Therefore, RWSP level is not included as a Type C variable for the US-APWR.
Containment Area Radiation	Detection of breach; verification	Containment High Range Area Radiation	No difference. This is a Type C variable for the US-APWR.
Effluent Radioactivity - Noble Gas Effluent from Condenser Air Removal System Exhaust	Detection of breach; verification	-	Coolant leakage into the secondary system due to an actual breach of the reactor coolant pressure boundary can be detected by RCS pressure, SG water level, and/or pressurizer water level. These variables are already Type A and/or Type C PAM variables. Therefore, it is not necessary to include effluent radioactivity as a Type C variable.

Table H.3-1 Basis for Type C Differences between RG 1.97 Rev.3 and the US-APWR PAM List (Sheet 2 of 3)

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Containment			
RCS Pressure	Detection of potential for breach; accomplishment of mitigation	Reactor Coolant Pressure	No difference. This is a Type C variable for the US-APWR.
Containment Hydrogen Concentration	Detection of potential for breach; accomplishment of mitigation; long-term surveillance	-	This variable is not used for design basis events (it is only used for beyond design basis accidents). Therefore, it does not need to be a Type C variable. However, the US-APWR does have the ability to monitor containment hydrogen concentration as described in DCD Subsection 6.2.5 in order to fulfill the TMI-related requirements of 10 CFR 50.34(f).
Containment Pressure	Detection of potential for or actual breach; accomplishment of mitigation	Containment Pressure	No difference. This is a Type C variable for the US-APWR.
Containment Effluent Radioactivity - Noble Gas Effluent from Identified Release Points	Detection of breach; accomplishment of mitigation; verification	-	Containment effluent radioactivity may be used to detect a containment breach. However, this is considered a Category 2 or backup indication in RG 1.97 Rev. 3. The primary indication for monitoring containment pressure boundary is containment pressure. Therefore, containment effluent radioactivity is not included as a Type C PAM variable for the US-APWR. Note that for the purpose of monitoring the release of radioactivity from pathways controlled by Technical Specifications, the plant vent receives the discharge from the containment purge, auxiliary building, control building, fuel building, and the condenser air removal filtration system. This variable can be measured by the plant vent radiation monitors (including high range) as part of the Type E variables for that purpose.

Table H.3-1 Basis for Type C Differences between RG 1.97 Rev.3 and the US-APWR PAM List (Sheet 3 of 3)

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Effluent Radioactivity - Noble Gases (from buildings or areas where penetrations and hatches are located, e.g., secondary containment and auxiliary buildings and fuel handling buildings that are in direct contact with primary containment)	Indication of breach	-	Coolant leakage outside of containment into secondary containment or the auxiliary or fuel handling buildings due to an actual breach of the reactor coolant pressure boundary can be detected by RCS pressure, SG water level, and/or pressurizer water level. These variables are already Type A and/or Type C PAM variables. In addition, effluent radioactivity is considered a Category 2 or backup indication in RG 1.97 Rev. 3. Therefore, it is not necessary to include effluent radioactivity as a Type C variable.

Table H.4-1 Basis for Type D Differences between RG 1.97 Rev.3 and the US-APWR PAM List (Sheet 1 of 6)

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Residual Heat Removal (RHR) or Decay Heat Removal System			
RHR System Flow	To monitor operation	CS/RHR Pump Discharge Flow CS/RHR Pump Minimum Flow	No difference. This is a Type D variable for the US-APWR.
RHR Heat Exchanger Outlet Temperature	To monitor operation and for analysis	-	Proper operation of the RHR system is verified by the CS/RHR flow rate. Additionally, T_{hot} and T_{cold} are available to monitor RHR system performance with respect to decay heat removal. Therefore, it is not necessary to include the RHR heat exchanger outlet temperature as a Type D variable in the US-APWR PAM list.
Safety Injection System			
Accumulator Tank Level and Pressure	To monitor operation	Accumulator Water Level, Accumulator Pressure	No difference. This is a Type D variable for the US-APWR.
Accumulator Isolation Valve Position	Operation status	-	Accumulator water level and accumulator pressure are available to monitor the accumulator operation status. Therefore, it is not necessary to include accumulator isolation valve position as a separate Type D variable in the US-APWR PAM list.
Boric Acid Charging Flow	To monitor operation	-	The safety injection system delivers boric acid water to the RCS in the US-APWR. Safety injection pump discharge flow and safety injection pump minimum flow are available to monitor the flow. Therefore it is not necessary to include this as a Type D variable in the US-APWR PAM list.
Flow in HPI System	To monitor operation	Safety Injection Pump Discharge Flow Safety Injection Pump Minimum Flow	No difference. This is a Type D variable for the US-APWR.
Flow in LPI System	To monitor operation	-	The US-APWR design allows the accumulators and high head safety injection system to fully replace the safety function associated with the low head safety injection system. Therefore, the US-APWR PAM list does not need any variables to indicate low pressure injection (LPI) system performance.

Table H.4-1 Basis for Type D Differences between RG 1.97 Rev.3 and the US-APWR PAM List (Sheet 2 of 6)

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Refueling Water Storage Tank Level	To monitor operation	Refueling Water Storage Pit Water Level (Wide Range) Refueling Water Storage Pit Water Level (Narrow Range)	No difference. This is a Type D variable for the US-APWR.
Primary Coolant System			
Reactor Coolant Pump Status	To monitor operation	-	The safety analysis does not rely on the RCPs to mitigate design basis events. The RCPs are also not necessary to achieve and maintain safe shutdown conditions. In addition, CCW header pressure is available to monitor CCW performance related to its function to provide seal cooling to the RCP in order to maintain its RCS pressure boundary function. Therefore, RCP status is not included as a PAM variable for the US-APWR.
Primary System Safety Relief Valve Positions (including power operated relief valve (PORV) and code valves) or Flow Through or Pressure in Relief Valve Lines	Operation status; to monitor for loss of coolant	Pressurizer Safety Valve Position, Safety Depressurization Valve Position	No difference. This is a Type D variable for the US-APWR.
Pressurizer Level	To ensure proper operation of pressure	Pressurizer Water Level	No difference. This is a Type D variable for the US-APWR.
Pressurizer Heater Status	To determine operating status	-	Pressurizer water level and RCS pressure are indicative of the performance of the pressurizer heaters. Therefore it is not necessary to separately include the heater status indications in the PAM list.
Quench Tank Level	To monitor operation	-	This component is not necessary to mitigate design basis events and is also not necessary to achieve and maintain safe shutdown conditions. Therefore, it is not included in the US-APWR PAM list.
Quench Tank Temperature	To monitor operation	-	Same as above
Quench Tank Pressure	To monitor operation	-	Same as above

Table H.4-1 Basis for Type D Differences between RG 1.97 Rev.3 and the US-APWR PAM List (Sheet 3 of 6)

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Secondary System (Steam Generator)			
Steam Generator Level	To monitor operation	SG Water Level (Wide Range), SG Water Level (Narrow Range)	No difference. This is a Type D variable for the US-APWR.
Steam Generator Pressure	To monitor operation	Main Steam Line Pressure	No difference. This is a Type D variable for the US-APWR.
Safety/Relief Valve Positions or Main Steam Flow	To monitor operation	Main Steam Safety Valve Position, Main Steam Relief Valve Position, Main Steam Depressurization Valve Position	No difference. This is a Type D variable for the US-APWR.
Main Feedwater Flow	To monitor operation	-	SG water level and main steam line pressure are indicative of adequate feedwater flow. In addition, the EFW system is used to provide flow to the SGs and EFW flow indication is available. Since these variables are already available to monitor SG operation, it is not necessary to separately include MFW flow in the PAM list.
Auxiliary Feedwater or Emergency Feedwater System			
Auxiliary or Emergency Feedwater Flow	To monitor operation	EFW Flow	No difference. This is a Type D variable for the US-APWR.
Condensate Storage Tank Water Level	To ensure water supply for auxiliary feedwater	EFW Pit Water Level	No difference. This is a Type D variable for the US-APWR.
Containment Cooling Systems			
Containment Spray Flow	To monitor operation	CS/RHR Pump Discharge Flow CS/RHR Pump Minimum Flow	No difference. This is a Type D variable for the US-APWR.
Heat Removal by the Containment Fan Heat Removal System	To indicate accomplishment of cooling	-	The containment fan heat removal system is not credited in design basis events since containment spray is credited to cool the containment and maintain containment integrity. Therefore this variable is not included in the PAM list.
Containment Atmosphere Temperature	To monitor operation	Containment Temperature	No difference. This is a Type D variable for the US-APWR.

Table H.4-1 Basis for Type D Differences between RG 1.97 Rev.3 and the US-APWR PAM List (Sheet 4 of 6)

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Containment Sump Water Temperature	To monitor operation	-	Containment pressure, containment temperature, and CS/RHR pump flow are utilized to monitor containment cooling system performance. In the US-APWR, the RWSP also serves as the normal suction source for the SI pumps. The design of the SI and CS/RHR pumps is such that NPSH is ensured even for RWSP water temperatures that bound accident conditions. Therefore it is not necessary to include this variable in the US-APWR PAM list.
Chemical and Volume Control System (CVCS)			
Makeup Flow - In	To monitor operation	-	Since RCS inventory control and boration are provided by the safety injection system in the US-APWR, the monitoring variables related to CVCS are not necessary PAM variables for the US-APWR design.
Letdown Flow - Out	To monitor operation	-	Same as above
Volume Control Tank Level	To monitor operation	-	Same as above
Cooling Water System (CCW)			
Component Cooling Water Temperature to ESF System	To monitor operation	-	CCW header pressure provides primary indication of the performance of the cooling water system. Monitoring header pressure gives the operator the most immediate and accurate indicate of the performance of the system of any available indication. Therefore it is not necessary to separately include this other variable to monitor CCW system performance in the PAM list.
Component Cooling Water Flow to ESF System	To monitor operation	-	Same as above
Radwaste Systems			
High-Level Radioactive Liquid Tank Level	To indicate storage volume	-	The US-APWR design precludes the need for this variable. This component is not necessary to mitigate design basis events and is also not necessary to achieve and maintain a safe shutdown condition. Further addition of radioactive waste to the liquid or gaseous radwaste system following an accident is precluded by design and is not postulated. Therefore, this variable is not included in the US-APWR PAM list.

Table H.4-1 Basis for Type D Differences between RG 1.97 Rev.3 and the US-APWR PAM List (Sheet 5 of 6)

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Radioactive Gas Holdup Tank Pressure	To indicate storage capacity	-	Same as above
Ventilation Systems			
Emergency Ventilation Damper Position	To indicate damper status	-	Containment Isolation Valve Position provides indication of containment integrity. The combination of isolation valve position status and a lack of radioactive release as indicated by the plant vent monitors provides verification of proper automatic ventilation path isolation. Therefore, damper position indication is not included in the US-APWR PAM list.
Power Supplies			
Status of Standby Power and Other Energy Sources Important to Safety (electric, hydraulic, pneumatic) (voltages, currents, pressures)	To indicate system status	Status of Standby Power and Other Energy Sources Important to Safety Class 1E ac Bus Voltage Class 1E dc Bus Voltage	No difference. This is a Type D variable for the US-APWR.
Other			
-	-	Reactor Coolant Hot Leg Temperature (Wide Range)	This variable indicates the performance of the primary coolant system for maintaining core cooling.
-	-	Reactor Coolant Cold Leg Temperature (Wide Range)	Same as above
-	-	Reactor Coolant Pressure	This variable indicates the performance of the primary coolant system for maintaining core cooling and RCS integrity.
-	-	Degrees of Subcooling	This variable is used to indicate the performance of the primary coolant system for core cooling.
-	-	RV Water Level	This variable provides direct indication of inventory available for maintaining core cooling.
-	-	Wide Range Neutron Flux	This variable directly indicates reactivity control and allows for the monitoring of the performance of the control rod assemblies.
-	-	Containment Pressure	This variable is used to indicate the containment integrity status.
-	-	Containment Isolation Valve Position (Excluding Check Valves)	This variable is used to indicate the containment integrity status.

Table H.4-1 Basis for Type D Differences between RG 1.97 Rev.3 and the US-APWR PAM List (Sheet 6 of 6)

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
-	-	CCW Header Pressure	This variable is used to indicate the performance of the CCW system.
-	-	ESW Header Pressure	This variable is used to indicate the performance of the ESW system.
-	-	Containment Purge Isolation Valve Position.	This variable is used to indicate the system status of the containment purge system.
-	-	Main Steam Isolation Valve Position	This variable is used to indicate the system status of the MSS system. All associated valves closed by the main steam line isolation signal are also included.
-	-	Main Feedwater Isolation Valve Position	This variable is used to indicate the system status of the MFW system. All associated valves closed by the main feedwater isolation signal are also included.
-	-	Emergency Feedwater Isolation Valve Position	This variable is used to indicate the system status of the EFW system. All associated valves repositioned by the emergency feedwater actuation signal or emergency feedwater isolation signal are also included.
-	-	MCR HVAC Damper Position	This variable is used to indicate the system status of the MCR HVAC system.
-	-	CS/RHR Pump Suction Relief Valve Position	This variable is used to indicate the system status of the RHR system.
-	-	SFP Pump Discharge Flow	This variable is used to indicate the system status of the cooling portion of the SFPCS.
-	-	SFP Temperature	This variable is used to indicate the system status of the cooling portion of the SFPCS.
-	-	SFP Water Level (Narrow Range)	This variable is used to indicate the system status of the cooling portion of the SFPCS.

Table H.5-1 Basis for Type E Differences between RG 1.97 Rev.3 and the US-APWR PAM List (Sheet 1 of 4)

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Containment Radiation			
Containment Area Radiation - High Range	Detection of significant releases; release assessment; long-term surveillance; emergency plan actuation	Containment High Range Area Radiation	No difference. This is a Type E variable for the US-APWR.
Area Radiation			
Radiation Exposure Rate (inside buildings or areas where access is required to service equipment important to safety)	Detection of significant releases; release assessment; long-term surveillance	-	The MCR and TSC are the main areas where access is required. The radiation in the MCR and TSC are selected as Type E PAM variables for the US-APWR (described in the "other" section below). If access to other areas is necessary, personnel protection will be provided by the use of portable radiation monitors and air sampling which are selected as Type E PAM variables. No other area radiation monitors are required. Therefore, it is not necessary to include this variable in the US-APWR PAM list.
Airborne Radioactive Materials Released from Plant			
Noble Gases and Vent Flow Rate			
Containment or Purge Effluent	Detection of significant releases; release assessment	-	The plant vent receives the discharge from the containment purge, auxiliary building, control building, fuel building, and the condenser air removal filtration system. These variables can be measured by the plant vent radiation monitors (including high range) and therefore are not included as separate Type E variables for the US-APWR.
Reactor Shield Building (if in design)	Detection of significant releases; release assessment	-	
Auxiliary Building (including any building containing primary system gases, e.g., waste gas decay tank)	Detection of significant releases; release assessment; long-term surveillance	-	
Condenser Air Removal System Exhaust	Detection of significant releases; release assessment	-	

Table H.5-1 Basis for Type E Differences between RG 1.97 Rev.3 and the US-APWR PAM List (Sheet 2 of 4)

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Common Plant Vent or Multipurpose Vent Discharging Any of Above Releases (if containment purge is included)	Detection of significant releases; release assessment; long-term surveillance	-	This variable can be measured by the plant vent radiation monitors (including high range) and therefore is not included as a separate Type E variable for the US-APWR.
Vent From Steam Generator Safety Relief Valves or Atmospheric Dump Valves	Detection of significant releases; release assessment	-	This variable is measured by the main steam line monitors. Therefore it is not included as a separate Type E variable for the US-APWR.
All Other Identified Release Points	Detection of significant releases; release assessment; long-term surveillance	-	This variable can be measured by the plant vent radiation monitors (including high range) and therefore is not included as a separate Type E variable for the US-APWR.
Particulates and Halogens			
All Identified Plant Release Points (except steam generator safety relief valves or atmospheric steam dump valves and condenser air removal system exhaust). Sampling with Onsite Analysis Capability	Detection of significant releases; release assessment; long-term surveillance	-	The main release point is the vent stack. This variable can be measured by the plant vent sampler (accident sampler). Therefore it is not included as a separate Type E variable for the US-APWR. Note that the other release points are the main steam safety valves and relief valves which are specifically excluded from this category in RG 1.97 Rev. 3. Release from those points can be determined by the portable instruments which are already identified as Type E variables.
Environs Radiation and Radioactivity			
Airborne Radiohalogens and Particulates (portable sampling with onsite analysis capability)	Release assessment; analysis	Airborne Radio Halogens and Particulates (Portable Sampling with Onsite Analysis Capability)	No difference. This is a Type E variable for the US-APWR.
Plant and Environs Radiation (portable instrumentation)	Release assessment; analysis	Plant and Environs Radiation (Portable Instrumentation)	No difference. This is a Type E variable for the US-APWR.

Table H.5-1 Basis for Type E Differences between RG 1.97 Rev.3 and the US-APWR PAM List (Sheet 3 of 4)

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Plant and Environs Radioactivity (portable instrumentation)	Release assessment; analysis	Plant and Environs Radioactivity (Portable Instrumentation)	No difference. This is a Type E variable for the US-APWR.
Meteorology			
Wind Direction	Release assessment	Meteorological Parameters (Wind Direction, Wind Speed, Estimation of Atmospheric Stability)	No difference. This is a Type E variable for the US-APWR. Note that the description of this variable will be provided by the COL applicant since it is site specific.
Wind Speed	Release assessment	Meteorological Parameters (Wind Direction, Wind Speed, Estimation of Atmospheric Stability)	No difference. This is a Type E variable for the US-APWR. Note that the description of this variable will be provided by the COL applicant since it is site specific.
Estimation of Atmospheric Stability	Release assessment	Meteorological Parameters (Wind Direction, Wind Speed, Estimation of Atmospheric Stability)	No difference. This is a Type E variable for the US-APWR. Note that the description of this variable will be provided by the COL applicant since it is site specific.
Accident Sampling Capability (Analysis Capability On Site)			
Primary Coolant and Sump ・Gross Activity ・Gamma Spectrum ・Boron Content ・Chloride Content ・Dissolved Hydrogen or Total Gas ・Dissolved Oxygen ・pH	Release assessment; verification analysis	-	These parameters can be measured by sampling. Many operating plants have received NRC approval for eliminating the PASS requirements specified in RG 1.97 Rev. 3. Therefore, these parameters are also not included in the US-APWR Type E PAM list.
Containment Air ・Hydrogen Content ・Oxygen Content ・Gamma Spectrum	Release assessment; verification analysis	-	These parameters can be measured by sampling. Many operating plants have received NRC approval for eliminating the PASS requirements specified in RG 1.97 Rev. 3. Therefore, these parameters are also not included in the US-APWR Type E PAM list.

Table H.5-1 Basis for Type E Differences between RG 1.97 Rev.3 and the US-APWR PAM List (Sheet 4 of 4)

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Other			
-	-	MCR Area Radiation	To monitor radiation and radioactivity levels in the control room.
-	-	MCR Outside Air Intake Radiation	To monitor radiation and radioactivity levels in the control room.
-	-	TSC Area Radiation	To monitor radiation and radioactivity levels in the technical support center.
-	-	TSC Outside Air Intake Radiation	To monitor radiation and radioactivity levels in the technical support center.
-	-	Plant Vent Radiation Gas Radiation (Including High Range)	To monitor the magnitude of releases of radioactive materials through identified pathways.
-	-	Main Steam Line Radiation	To monitor the magnitude of releases of radioactive materials through identified pathways.
-	-	GSS Exhaust Fan Discharge Line Radiation (Including High Range)	To monitor the magnitude of releases of radioactive materials through identified pathways.
-	-	Condenser Vacuum Pump Exhaust Line Radiation (Including High Range)	To monitor the magnitude of releases of radioactive materials through identified pathways.
-	-	Plant Air Vent High Concentration Sampling System	To monitor the magnitude of releases of radioactive materials through identified pathways.

Appendix I Reduction of Response Time and Operator's Workload by Utilizing Integrated Operational VDU (O-VDU)

Table I-1 Comparison of Sequential Time Line of Actions between O-VDU Operations and S-VDU Operations (Sheet 1 of 5)

Table I-1 Comparison of Sequential Time Line of Actions between O-VDU Operations and S-VDU Operations (Sheet 2 of 5)

Table I-1 Comparison of Sequential Time Line of Actions between O-VDU Operations and S-VDU Operations (Sheet 3 of 5)

Table I-1 Comparison of Sequential Time Line of Actions between O-VDU Operations and S-VDU Operations (Sheet 4 of 5)

Table I-1 Comparison of Sequential Time Line of Actions between O-VDU Operations and S-VDU Operations (Sheet 5 of 5)

Appendix J Analyses for PCMS Failures

J.0 Purpose

The purpose of this Appendix is to describe the effect of Plant Control and Monitoring System (PCMS) failures, including operational VDU failures, in the US-APWR. The safety-related I&C system, non-safety I&C system and diverse I&C system are referred to as the Protection and Safety Monitoring System (PSMS), PCMS and the Diverse Actuation Systems (DAS), respectively, as described in this Technical Report and DCD Chapter 7.

The PCMS failure mode and effect analysis (FMEA) in Section J.1 of this Appendix is to demonstrate that the US-APWR is adequately protected from multiple random hardware failures or a software design defect, that adversely affects single or multiple control functions within a single PCMS control group. This analysis demonstrates that transients resulting from these failures meet the DCD Chapter 15 anticipated operational occurrence (AOO) acceptance criteria using the FMEA method.

Section J.2 of this Appendix shows that the US-APWR is adequately protected from multiple hardware failures or a software design defect that adversely affects multiple control functions within multiple PCMS control groups (i.e., a common cause failure (CCF) of multiple PCMS controllers). This analysis demonstrates that transients resulting from these failures are bounded by the DCD Chapter 15 postulated accident (PA) acceptance criteria using best estimate methods.

Section J.3 of this Appendix shows that the US-APWR is adequately protected from multiple hardware failures or a software design defect that results in multiple spurious control commands from single or multiple operational VDUs (i.e., a CCF of the operational VDUs) that adversely affects the safety-related components controlled by all four trains of the PSMS as well as the non-safety components controlled by the PCMS. This analysis demonstrates that transients resulting from these failures are bounded by the DCD Chapter 15 PA acceptance criteria using best estimate methods.

J.1 Events Initiated by Single PCMS Control Group Failures

J.1.1 Evaluation Condition

US-APWR control functions are segmented into the different control groups of the PCMS, and these control groups are electrically isolated from each other. Also, any single failures of common inputs for different control groups cannot affect the control functions in all control groups due to how the signal selection algorithm (SSA) functions in each control group. The control functions, which may cause a plant transient due to a failure, uses three or four sensor input signals for these control functions. The SSA excludes a failed input signal as described in DCD Subsection 7.1.3.16 and Subsection 4.2.5 of this Technical Report. Because it is rejected by the SSA function, which is duplicated and segmented in each control group, the failed input signal has no impact on any control functions. In addition, if the SSA function block in one PCMS control group fails, the other control groups still perform the required PCMS functions using their own SSA function blocks.

Each basic software block (e.g., AND function, Latch function, PID function, SSA function) is stored in the memory of a controller as part of that controller’s basic software. Each controller has its own copy of the basic software block. The controller uses its copy of the basic software block for all of its control functions. Therefore, the spurious actuation of multiple functions in one controller may be caused by the failure of one basic software block (e.g., a memory bit failure for that basic software block), if that failure is not detected by the self-diagnostic functions, such as the memory parity error detection. Therefore, for multiple functions in a single controller to be adversely affected, two random hardware failures are needed: (1) a basic software block memory failure and (2) a failure of self-diagnostics circuit.

Each control group of the PCMS consists of redundant controllers. If a failure in the main controller is detected by self-diagnostic functions, all control functions will be automatically switched to the back-up controller as described in Subsection 5.1.8 of this Technical Report. Due to the segmentation of redundant controllers, a single random failure in one controller does not cause a similar failure in the back-up controller. Therefore, single random failures in one of these redundant controllers that are detected by the self-diagnostic functions, including memory failure that affects a basic software block, does not cause a malfunction, including a spurious actuation, of any control group of the PCMS. Therefore, for both redundant controllers within a PCMS control group to be adversely affected, two random failures are needed: (1) a failure in the first controller and (2) failure of self-diagnostics to detect that failure and transfer to the backup controller, or correct transfer with a random failure of the backup controller.

The application software of each control group is developed in a dedicated manner for each PCMS control group by connection and combination of the basic software blocks. Therefore, a design defect in the application software limits the consequences of control function failures to a single PCMS control group (i.e., it does not cause a CCF of multiple PCMS control groups).

The basic software blocks (e.g., AND function, Latch function, PID functions) are commonly used for different PCMS control functions in a single PCMS control group and in multiple PCMS control groups. Therefore, a software design defect in a commonly used basic software block can cause a failure of multiple control functions in multiple PCMS control groups (i.e., a CCF). The basic software design defect (i.e., a CCF) is analyzed in Section J.2.

As described above, a PCMS control group failure will not result from a single hardware failure, but Section J.1 conservatively assumes single control group failures which may be caused by multiple hardware failures. These failures can lead to multiple control function failures within one control group of the PCMS

The analysis in this Section J.1 demonstrates that the transients caused by these failures meet the AOO acceptance criteria. These transients are not considered as new AOOs, because they can only result from multiple hardware failures in the PCMS. Therefore, this analysis demonstrates that the safety functions and their corresponding response times which are credited in the Chapter 15 analysis are sufficient to protect the plant if multiple hardware random failures within the PCMS occur.

Section J.1 also demonstrates that single or multiple control function failures which may occur due to an application software design defect, of which effects are limited to one PCMS control group, cannot result in consequences that are more severe than those described in the DCD Chapter 15 AOO acceptance criteria.

The FMEA method is utilized to identify the transients that may result from failure of a single PCMS group and to demonstrate that the US-APWR is adequately protected from these events. The system configuration for the PCMS modeled in the FMEA is the same as Figure 4.1-1 of this Technical Report. The FMEA method and contents of the FMEA table are described in Section 6.5.1 of this Technical Report.

In summary, Section J.1 demonstrates that the US-APWR is adequately protected from failures in a single PCMS control group, including an application software design defect and multiple hardware failures. The FMEA for PCMS in Section J.1 demonstrates that transients caused by these failures meet the DCD Chapter 15 AOO acceptance criteria.

J.1.2 Analysis and Conclusion

J.1.2.1 Hardware Failure and Software Defect in One PCMS Control Group

The following control groups are included in the PCMS. Each control group contains one or multiple control functions. A failure of each control group, including all functions within that control group, is considered individually in this Section J.1. The results are shown in Table J.1-1. Postulated design defects that lead to multiple control group failures (CCF) are addressed in Section J.2.

(1) Reactor Control System Failure:
There is no failure that results in consequences more severe than the DCD Chapter 15 AOO acceptance criteria.

(2) Control Rod Drive Mechanism (CRDM) Control System Failure:
There is no failure that results in consequences more severe than the DCD Chapter 15 AOO acceptance criteria.

(3) Incore Nuclear Instrumentation System (ICIS) Failure:
There is no control function. Therefore, the failure does not cause any plant transients.

(4) Radiation Monitoring System (RMS) Failure:
There is no control function. Therefore, the failure does not cause any plant transients.

(5) Rod Position Indication (RPI) System Failure:
There is no control function. Therefore, the failure does not cause any plant transients.

(6) BOP Control System Failure:
There is no failure that results in consequences more severe than the DCD Chapter 15 AOO acceptance criteria.

(7) Turbine Electro-hydraulic Governor (EHG) Control System Failure:
There is no failure that results in consequences more severe than the DCD Chapter 15 AOO acceptance criteria.

(8) Turbine Protection System Failure:
There is no failure that results in consequences more severe than the DCD Chapter 15 AOO acceptance criteria.

(9) Turbine Supervisory Instrument System Failure:
There is no control function. Therefore, the failure does not cause any plant transients.

(10) Electrical Control System Failure:
There is no failure that results in consequences more severe than the DCD Chapter 15 AOO acceptance criteria.

(11) Auto Voltage Regulator and Automatic Load Regulator (AVR/ALR) System Failure:
There is no failure that results in consequences more severe than the DCD Chapter 15 AOO acceptance criteria.

(12) Generator Transformer Protection System Failure:
There is no failure that results in consequences more severe than the DCD Chapter 15 AOO acceptance criteria.

The following HSIS computer groups are included in the PCMS. Each HSIS group contains multiple HSIS functions. Each failure of each HSIS group, including all functions within that group, is considered individually. As shown below, with the exception of O-VDUs, these computers perform no control functions; therefore, they have no potential to cause plant transients. The failure of these computers is included in this section only for completeness, in order to address all PCMS components. Since these HSIS computer groups cannot cause transients, they are not addressed again in Section J.2. Postulated O-VDU failures are addressed in Section J.3.

(13) Alarm VDU Failure:
There is no control function. Therefore, the failure does not cause any plant transients.

(14) Alarm VDU Computer Failure:
There is no control function. Therefore, the failure does not cause any plant transients.

(15) Alarm Logic Compute Failure:
There is no control function. Therefore, the failure does not cause any plant transients.

(16) Large Display Computer Failure:
There is no control function. Therefore, the failure does not cause any plant transients.

(17) Large Display Computer (TSC) Failure:
There is no control function. Therefore, the failure does not cause any plant transients.

(18) Large Display Panel Failure:
There is no control function. Therefore, the failure does not cause any plant transients.

(19) Operational VDU Panel Failure:
There is no control function. Therefore, the failure does not cause any plant transients.

(20) Operational VDU Computer Failure:
As described in Appendix C of this Technical Report, single random failures do not result in multiple spurious commands; failures that result in single spurious commands are bounded by the AOOs in Chapter 15. Regardless, as stated in Section D.2(b), Appendix D of this Technical Report postulates multiple spurious operational VDU commands and demonstrates that those

spurious commands cannot adversely affect the safety functions of the PSMS. Section J.3 of this Appendix postulates these same multiple spurious operational VDU commands and demonstrates that those spurious commands cannot cause plant transients that are not bounded by the PA acceptance criteria in Chapter 15.

(21) Operational VDU (TSC) Failure:
There is no control function. Therefore, the failure does not cause any plant transients.

(22) Operational VDU Computer (TSC) Failure:
There is no control function. Therefore, the failure does not cause any plant transients.

(23) Operational Procedure VDU Failure:
There is no control function. Therefore, the failure does not cause any plant transients.

(24) Operational Procedure VDU Computer Failure:
There is no control function. Therefore, the failure does not cause any plant transients.

(25) Process Recording Computer Failure:
There is no control function. Therefore, the failure does not cause any plant transients.

(26) Unit Management Computer Failure:
There is no control function. Therefore, the failure does not cause any plant transients.

J.1.2.2 Conclusion

The PCMS FMEA shows the US-APWR is adequately protected from PCMS failures, including multiple random hardware failures and an application software design defect, and concludes that failures/defects that results in the failure of one single PCMS control group do not result in consequences more severe than the DCD Chapter 15 AOO acceptance criteria.

Table J.1-1 FMEA of PCMS for Single Control Group Failure (Sheet 1 of 5)

Table J.1-1 FMEA of PCMS for Single Control Group Failure (Sheet 2 of 5)

Table J.1-1 FMEA of PCMS for Single Control Group Failure (Sheet 3 of 5)

Table J.1-1 FMEA of PCMS for Single Control Group Failure (Sheet 4 of 5)

Table J.1-1 FMEA of PCMS for Single Control Group Failure (Sheet 5 of 5)

J.2 Events Initiated by Multiple PCMS Control Group Failures

J.2.1 Introduction

The US-APWR DCD Chapter 15 evaluates events initiated by a single failure of the plant systems, which includes the control systems in the PCMS, using the guidance in the SRP. The D3 Coping Analysis Technical Report (MUAP-07014) evaluates events in accordance with the SRP BTP 7-19 which requires an evaluation of the concurrent occurrence of a Chapter 15 event with a CCF in the PSMS alone, or a CCF in the PSMS and PCMS which disables the mitigating functions in the PSMS and similarly disables the PCMS which may aggravate the analyzed transients. MHI analyzed all the Chapter 15 initiating events in MUAP-07014, but MUAP-07014 does not include other events which may be initiated by failures within the PCMS that may be caused by a software design defect or multiple hardware failures. Section J.1 evaluates transients that may be caused by a software design defect and multiple hardware failures that affect a single PCMS control group. This Section J.2 discusses events due to a software defect and multiple hardware failures that results in multiple PCMS control group failures (i.e., a CCF).

J.2.2 Best Estimate Assumption of Plant Conditions

J.2.3 Consequences of PCMS Software CCF

J.2.4 Acceptance Criteria

J.2.4.1 Fuel Integrity

J.2.4.2 RCS Pressure and Secondary Pressure

J.2.4.3 Radiological Consequences

J.2.4.4 CV Integrity

J.2.5 Summary

MHI evaluated the events initiated by multiple control group failures due to a PCMS CCF and concluded that the Chapter 15 PA acceptance criteria for fuel integrity, RCS and secondary pressures, radiological consequences, and CV integrity are met.

Table J.2-1 Effects on Plant Condition due to Multiple Control Group / O-VDU Failures (Sheet 1 of 4)

Table J.2-1 Effects on Plant Condition due to Multiple Control Group / O-VDU Failures (Sheet 2 of 4)

Table J.2-1 Effects on Plant Condition due to Multiple Control Group / O-VDU Failures (Sheet 3 of 4)

Table J.2-1 Effects on Plant Condition due to Multiple Control Group / O-VDU Failures (Sheet 4 of 4)

J.3 Events Initiated by Operational VDU Failures

J.3.1 Introduction

The operational VDUs of the US-APWR, which are non-safety equipment, have the capability to control the safety-related components of all four trains as well as non-safety components. In accordance with the 4th bullet of Section 3.1.5 in ISG-04, the operational VDUs require multiple control actions to generate control commands. In accordance with the 5th bullet of Section 3.1.5 in ISG-04, the PSMS controllers detect and block commands that do not pass the communication error checks. The effectiveness of these features in limiting the failures from operational VDUs to single spurious control commands is demonstrated in Appendix C, and single spurious control commands are bounded by the AOOs in Chapter 15.

Regardless of the effectiveness of these features in preventing multiple spurious control commands, postulated multiple spurious control commands are demonstrated, in Appendix D, to have no adverse effect on the safety functions of the PSMS. However, these PSMS safety functions can only be considered effective if the accidents they are credited to mitigate have been analyzed. Therefore, in accordance with the guidance of the last bullet in DI&C-ISG-04 Section 3.1.5, this section demonstrates that postulated multiple spurious command signals from the operational VDUs meet the PA acceptance criteria.

This analysis considers that the following features of the safety-related systems limit the impacts from the spurious command signals of the operational VDUs:

- Safety-related automatic signals (e.g., ESF actuation signals, interlocks important to safety) ensure that the safety-related components are in the required positions or are actuated to the required positions through the priority logic within the safety-related I&C systems.
- Bypass or reset of the safety-related automatic signals from the operational VDU requires the permissive signals on the safety VDUs through the priority logic within the safety-related I&C systems. Therefore, it is assumed that all ESFAS signals are operable.
- The operator can disconnect the operational VDU command signals on the safety VDUs through the priority logic within the safety-related I&C systems so that the operator can manually rearrange the components to the required alignment after disconnecting the operational VDUs.
- Control power supplies are normally off for some of the components in order not to change their positions due to the spurious operations or signals. The operational VDUs have no capability to turn these control power supplies on.

J.3.2 Best Estimate Assumption of Plant Conditions

J.3.3 Consequences of Operational VDU CCF

J.3.4 Acceptance Criteria

J.3.5 Evaluation

J.3.5.1 Fuel Integrity

J.3.5.2 RCS Pressure and Secondary Pressure

J.3.5.3 Radiological Consequences

J.3.5.4 C/V Integrity

J.3.5 Summary

MHI evaluated the events initiated by multiple system failures due to an operational VDU CCF and concluded that the acceptance criteria for fuel integrity, RCS and secondary pressures, radiological consequences, and CV integrity are met.