

HSI System Description and HFE Process

Non-Proprietary Version

July 2011

**©2007-2011 Mitsubishi Heavy Industries, Ltd.
All Rights Reserved.**

Revision History

Revision	Date	Page (Section)	Description
0	April 2007	All	Original issued
1	July 2007	<p>All</p> <p>8</p> <p>(3.4)</p> <p>15</p> <p>(4.1)</p> <p>19</p> <p>(4.2.2)</p> <p>21-22</p> <p>(4.3.1 b.)</p> <p>41</p> <p>(4.5.3)</p> <p>76</p> <p>(4.10.3)</p> <p>82</p> <p>(4.11.4)</p> <p>85</p> <p>(4.12)</p> <p>87</p> <p>(5.0)</p> <p>100</p> <p>(5.3.2.1)</p> <p>135</p> <p>(5.10.2.1)</p>	<p>The following items are revised based on NRC comments or correcting erratum.</p> <p>Pictures were replaced to color version.</p> <p>Descriptions were corrected.</p> <p>A description about the operational VDU qualification was added.</p> <p>A description about RSC was added.</p> <p>A reason applying noise level “raised” was added.</p> <p>Physical tag descriptions were added.</p> <p>Further notes of the minimum inventory HSI were added.</p> <p>Descriptions were corrected.</p> <p>A Minimum Inventory HSI process was added.</p> <p>Descriptions were added.</p> <p>Further notes of the automation rule were added.</p> <p>Descriptions that accidents are including CCF condition were added.</p>
2	September 2008	<p>2-3</p> <p>(3.1)</p> <p>14</p> <p>(Fig. 4.0-2)</p> <p>45</p> <p>(4.6.2)</p> <p>57</p> <p>(4.8)</p> <p>11-148</p> <p>(4.X & 5.X)</p>	<p>Added the specific subsection.</p> <p>Updated the schedule</p> <p>Clarified the descriptions</p> <p>Added the descriptions of computer Based Operating Procedure</p> <p>Placed reference # which are listed in Section 6.0 in appropriate portion of section 4 & section 5</p>
3	October 2009	<p>vii</p> <p>viii</p>	<p>Revise description of SDCV.</p> <p>Revise the sentence regarding Basic HSI and Licensing document.</p>

Revision	Date	Page (Section)	Description
3 (continued)		2	Revise description.
		(3.0)	
		6	Change from “is” to “are”.
		(3.3)	
		11	Add a plan for submitting HSI/HFE documentation.
		(4.0)	
		15	Delete descriptions of assumption of average visual ability.
		(4.1)	
		18	Add descriptions of Maintenance Console.
		(4.2.1)	
		21	Add clarification of the procedure access and use evaluation.
		(4.2.5)	
		24	Delete ITV console and move DHP panel.
		(4.3.1)	
		25	Delete ITV from table.
		(4.3.1)	
		25	Add descriptions of Maintenance Console.
		(4.3.1)	
		26	Add a description regarding Operating Procedure VDUs.
		(4.3.2)	
		30-31	Delete descriptions of the navigation path to screen list menu. (Screen list menu display can be selected from any operational display in the same way as the top navigation display. It was based on phase 1b test)
		(4.4.2 a)	
		40	Change name of switch window control button from “Erase” to “Exit”.(It was based on phase1b test)
		(4.5.3)	
		41	Revise description.
		(4.5.3)	
		41	Add descriptions that Component Control Design Guide describes the standard control design.
		(4.5.3)	
		42	Add “The EXIT”
		(4.5.3)	
		44	Add reference.
		(4.5.3)	
		50	Delete audible tone sounding.
		(4.7.1)	
		53	Add explanation for Mode Rule.
		(4.7.2)	
		56	Delete “and continuing to sound”.
		(4.7.2)	
		57	Add automated sound stop.
		(4.7.5)	
		59	Add criterion based on DI&C ISG-05.
		(4.8)	
		64	Add description of LDP.
		(4.9.2.1)	

Revision	Date	Page (Section)	Description
3 (continued)		69 (4.9.3)	Add description of alarms and OK monitor.
		70 (4.9.3)	Add BISI monitor.
		71 (4.9.3)	Update Figure 4.9-7.
		72 (4.9.3)	Update Figure 4.9-8.
		79 (4.10.1)	Add reference 43.
		79 (4.10.2)	Add "typical".
		79-80 (4.10.2)	Add description of color coding.
		80 (4.10.2)	Revise Figure 4.10-1.
		80 (4.10.3)	Add "typical".
		80 (4.10.3)	Add description of the CSF alarms.
		80 (4.10.4)	Add BISI function.
		83 (4.11.2)	Revise figure 4.11-2.
		84 (4.11.3)	Revise sentence of the Limiting Condition for Operation (LCO) for loss of all non-safety HSI.
		84 (4.11.3)	Add "approximately".
		85 (4.11.4)	Revise sentence of the Limiting Condition for Operation (LCO) for loss of all digital non-safety and safety HSI.
		91 (5.0)	Add description of detail on involvement of plant personnel in plant modifications.
		91-92 (5.1.11)	Add generic HFE program goals of the program.
		93-94 (5.1.2.2)	Revise responsibilities of HFE Design Team Manager.
		94 (5.1.2.2)	Revise responsibilities of HFE V&V Team Manager.
		95 (5.1.2.2)	Add Clarification of the HFE team's organizational placement and authority.
		95 (5.1.2.2)	Add Clarification on responsibilities, qualifications, and credentials for HFE team positions.
		96 (5.1.3)	Add clarification of general process procedures .
		97 (5.1.3)	Add clarification of HFE requirements for subcontractors.
		100 (5.1.5)	Add clarification of HFE facilities, equipment, tools, and techniques.

Revision	Date	Page (Section)	Description
3 (continued)		101	Add HSI design implementation activities.
		(5.1.5)	
		103	Add description of scope of OER and the specific plan for OER.
		(5.2)	
		105	Add clarification of the concept of operations.
		(5.3)	
		112	Revise description of scope of task analysis.
		(5.4.2)	
		119	Add description regarding GOMS.
		(5.4.3.2)	
		125	Revise Figure 5.5-2.
		(5.5.2)	
		130	Add description of Risk-important HAs integration.
		(5.6.5)	
		132	Add clarification of the concept of operations.
		(5.7.2)	
		133	Add clarification of the functional requirements specification process.
		(5.7.3)	
		133-134	Add clarification of the analysis of personnel task requirements process.
		(5.7.3.1)	
		134	Add clarification of the how other HSI design requirements.
		(5.7.3.1)	
		137	Add clarification of the HSI detailed design and integration process.
		(5.7.3.2)	
		138	Add clarification of the HSI test and evaluation methodologies.
		(5.7.3.3)	
		138-139	Add clarification of the HSI design documentation process.
		(5.7.3.4)	
		141	Revise stop valve.
		(5.7.3.4)	
		143	Add clarification of the entry conditions for EOPs .
		(5.8.1)	
		144	Add clarification of the basis for procedure development.
		(5.8.2)	
		144	Add clarification of the procedure access and use evaluation.
		(5.8.2)	
		145	Add clarification of the process for modifying procedures.
		(5.8.2)	
		146	Add clarification of the basis for the training program.
		(5.9.1)	
		146	Add R.G. 1.149.
		(5.9.2)	
		146	Add description regarding part-task simulator.
		(5.9.2)	
		147	Revise description regarding basic function of simulator.
		(5.9.2)	
		148	Add clarification of the facilities and resources for training.
		(5.9.3)	

Revision	Date	Page (Section)	Description
3 (continued)		149 (5.9.5)	Add clarification of the overall training approach.
		149 (5.9.7)	Add clarification of the periodic retraining plan.
		150 (5.10)	Add clarification of the overall V&V plan.
		154 (5.10.2.2.2)	Add clarification of the procedure V&V process.
		155 (5.10.2.2.4)	Add clarification of the performance measurement process.
		156 (5.10.2.2.4)	Add description of questionnaires and verbal debrief sessions.
		159 (5.10.2.2.4)	Add clarification of the Situation Awareness and Cognitive Workload measurement methodologies.
		162 (5.11)	Add clarification of design implementation plan.
		162 (5.11)	Add description of the plant modernization.
		163 (5.12)	The words “existing applicant” will be changed to “potential applicant to apply HSI modernization”.
		166 (7.0)	Add reference.
		171 (Appendix C)	Revise sentences.
		172 (Appendix C)	Revise sentences.
		174-181 (Appendix D)	Add table including scope of the Basic HSI System.
4	July 2011	General	The following items are revised based on NRC comments. Revised capitalizations of following words for editorial correction; “System” to “system” Revised words “Topical Reports” to “reports” or “topical and technical reports” or “technical reports”. Revised capitalizations “Topical Report” to “topical report”.
		xviii	Added “(HSIS)” Replaced following words; “Video” with “Visual” “Video” with “selectable and SDCV Visual”

Revision	Date	Page (Section)	Description
4 (continued)		xix	Replaced following words with “US Basic HSIS” for Responses to DCD RAI No.728 (Q:18-106) and Responses to Topical Report RAI (Q18.0-92). <ul style="list-style-type: none"> • Japanese APWR design • Basic HSI System • Japanese standard HSI design • Reference plants
		62	
		100	
		106	
		136	
		141	
		146	
		154	
		166	
		175-176	
		178-185	
		xx	Revised description about reports. Added reference numbers.
		xxviii	
		1 (2.0)	Revised “Descriptions” to “Discrepancy” Replaced following word; "consists of" with "include"
		2 (3.1)	Replaced following word; "Equipment" with "equipment" (GDC 5)
		3 (3.1)	Replaced following word; "consists of" with "include"
		4 (3.1)	Revised description about GDC 22 Deleted “generally”. (Item 2 (xx))
		5 (3.2)	Deleted “with”. (Item 3 (3))
		7-8 (3.4)	Revised description about SECY.
		11 (4.0)	Revised BTP numbers.
		14 (4.0)	Deleted “prepared a”.
		15 (4.1 a)	Revised Figure 4.0-2 for Responses to Topical Report RAI (Q:18.0-89).
		17 (4.1)	Added “that”.
			Added new section “4.1.h. Overriding automatic systems” for Responses to DCD RAI No.412 (Q:18-52).

Revision	Date	Page (Section)	Description
4 (continued)		18 (4.2.1)	Revised following words; "centralised" to "centralized" "temporarily" to "temporary" Deleted "the".
		19 (4.2.1)	Revised following word; " effect " to " affect "
		20 (4.2.2)	Added descriptions about physical means in the RSR for Responses to DCD RAI No.344 (Q:18- 42).
		21 (4.2.3)	Revised following word; "consist of" to "equipped with"
		21 (4.2.4)	Revised descriptions about EOF.
		21 (4.2.5)	Deleted "of". Revised descriptions about local controls.
		23 (4.3.1 a)	Revised descriptions about viewing angle.
		23 (4.3.1 b)	Revised following word; "at" to "in"
		26 (Table 4.3-1) 62 (4.8) 83 (4.10.3)	Replaced the word "emergency response" to "accident management" for Responses to DCD RAI No.728 (Q:18-110).
		27 (4.3.2)	Revised "Shift Technical Advisor Console" to "shift technical advisor console". Deleted "unit" and "desk areas". Added "Main feedwater isolation". Revised "engineering" to "engineered". Added "and ESF system"
		28 (4.3.2)	Revised Figure 4.3-4.
		30 (4.4.1)	Deleted "the". Revised following word; "a" to "the"

Revision	Date	Page (Section)	Description
4 (continued)		31 (4.4.2 a)	Revised following for Responses to Topical Report RAI(Q:18.0-89); "item (2)" to "item (C)".
		33 (Table 4.4-2)	Added "(.
		33 (4.4.2 b)	Revised description about safety VDU.
		36 (Table 4.4-3)	Revised following words; "occurs" to "occur" "selects" to "is selected" "numbers" to "number" "overflow" to "overflows"
		37 (4.4.2 d)	Revised Figure 4.4-4.
		38 (4.5.2 a)	Revised "consistent" to "fixed". Revised following words for Responses to Topical Report RAI(Q:18.0-89); "unusually" to "unusual"
		41 (4.5.3 a)	Revised Figure 4.5-3. Added "as".
		42 (4.5.3 a)	Deleted descriptions as follows; "dynamic active safety" "physically and statically" [] "the unusual" "that" Revised following words; [] "covered by" to "hidden behind"
		43 (4.5.3 a)	Revised "on" to "off" Revised "popup" to "pops up"
		44 (4.5.3 a)	Deleted "respectively".
		45 (4.5.3 b)	Revised "return" to "are resumed" Revised following words for Responses to Topical Report RAI(Q:18.0-89); "rating" to "rate".

Revision	Date	Page (Section)	Description
4 (continued)			Added following words; "1/10th of the..." "respectively"
		46 (4.5.3 c)	Added "and". Deleted "also". Revised following words; "is" to "become" "made consistent" to "designed consistently"
		47 (4.6.1)	Revised and added description about safety VDU screens.
		47 (4.6.2)	Revised description about Operational VDUs Connect/Disconnect.
		48 (4.6.3)	Added new subsection "4.6.3 Bypass Permissive"
		49 (4.6.4)	Revised description about Monitor Screen.
		50 (4.6.5)	Revised title number "c. Operation Screen" to "4.6.5 Operation Screen". Revised description about Operation Screen.
		51 (4.6.5)	Revised Figure 4.6-5. Revised Figure 4.6-6.
		52 (4.6.6)	Added new section "4.6.6 Task-based Screen".
		52 (4.6.7)	Added new section "4.6.7 Multidivisional Safety VDU Screen". Added new Figure "4.6-7 Typical Multidivisional Safety VDU Screen".
		53 (4.7)	Replaced following word; "are" with "is"
		53-54 (4.7.1 a) (4.7.1 b)	Revised following words; "coding" to "coded" "become" to "becomes" "confirm" to "confirms" "can be" to "are" "acknowledge" to "acknowledges" Deleted following words; "respectively"

Revision	Date	Page (Section)	Description
4 (continued)			"can"
		55 (4.7.1 b)	Revised "Fast-out" to "First-out" in Figure 4.7-1 item(1) for Responses to Topical Report RAI(Q:18.0-89).
		58 (Table 4.7-1)	Revised Table 4.7-1 for Responses to Topical Report RAI(Q:18.0-89).
		59 (4.7.2 b)	Deleted "and"
		60 (4.7.3)	Added following words; "are" "their" Revised following words; "frequency" to "frequencies" "cycle" to "cycles"
		60 (4.7.5)	Revised following words for Responses to Topical Report RAI(Q:18.0-89); "identify" to "identifies" "delete" to "deletes" Added "that" and "the". Revised description of last sentence.
		61 (4.8)	Revised description of first sentence. Revised description of first bullet. Revised following words; "Distinctive" to "Specific" "executing" to "to execute"
		62 (4.8)	Revised "...for the degraded HSI conditions described..." to "...in case of the degraded HSI conditions to be described...". Revised following words; "transition" to "move" "for" to "of" "transition" to "access" Deleted "procedure" and " ," Added "that".
		64-65 (Table 4.8-1)	Revised "Operational" to "Operating".
		66 (4.9.1)	Revised following words; "followings" to "the following" Deleted "available to".

Revision	Date	Page (Section)	Description
4 (continued)		67 (4.9.2.1)	Revised “a numerical value and a trend arrow” to “numerical values and trend arrows”.
		70 (4.9.3 b)	Revised description of first sentence.
		70 (4.9.3 c)	Revised “in” to “on”.
		71 (4.9.3 d)	Revised “operation difficulties” to “operation to be difficult”.
		71 (4.9.3 e)	Revised “is blinking” to “blinks”.
		74 (Figure 4.9-7)	Added “the”.
		79 (Table 4.9-1)	Delete “Rate”
		82 (4.10.2)	Revised “HPI” to “HSI”. Added “Main feedwater isolation”.
		83 (4.10.4)	Revised “nearby” to “near”.
		85 (4.11.2)	Revised following words; “tangent” to “transient” “The” to “the”
		86 (Figure 4.11-2)	Revised Figure 4.11-2.
		88 (4.11.4)	Revised description of third sentence for Responses to Topical Report RAI(Q:18.0-89).
		89 (4.11.4)	Revised following words; “repair failures” to “failures are repaired” “section 5” to “Section 5”
		89 (4.11.5)	Revised “due to” to “for”
		91 (4.12 a)	Revised “Non-Safety” to “Non-safety”

Revision	Date	Page (Section)	Description
4 (continued)		92 (4.12 d)	Revised capitalizations “section” to “Section”. Revised description of last paragraph for Responses to Topical Report RAI(Q:18.0-94).
		94 (5.0)	Revised description of first paragraph for Responses to Topical Report RAI(Q:18.0-95).
		94 (5.1.1.1)	Revised following words; “result s” to “result” “maintain s” to “maintain” “provides” to “provide”
		95 (5.1.1 ii)	Revised “feedback” to “fed back”.
		95 (5.1.1.1 iii)	Revised description of second paragraph for Responses to Topical Report RAI(Q:18.0-89).
		95 (5.1.1.2)	Revised description of third bullet for Responses to Topical Report RAI(Q:18.0-89).
		95-96 (5.1.1.2)	Revised “HEDs” to “Human Engineering Discrepancy (HED) “. Added last two bullets about hardware capability restriction for Responses to DCD RAI No.281 (Q:18-6) and Responses to Topical Report RAI(Q:18.0-4).
		96 (5.1.1.3)	Revised capitalization “section” to “Section”.
		96 (5.1.1.4)	Revised description of first paragraph for Responses to Topical Report RAI(Q:18.0-89).
		96 (5.1.1.5)	Revised “section” to “Section”.
		98 (5.1.2.2 (4))	Deleted “ , ”.
		99 (5.1.3 a)	Revised “Figure 5.1-1” to “Figure 5.1-2” in the 3rd and 4th bullet for Responses to Topical Report RAI(Q:18.0-89).
		99-100 (5.1.3 d)	Revised description of second sentence for Responses to Topical Report RAI(Q:18.0-90).
		100 (5.1.3 e)	Deleted “ , ”.

Revision	Date	Page (Section)	Description
4 (continued)		103 (5.1.4)	Revised font format to bold for Responses to Topical Report RAI(Q:18.0-89).
		103 (5.1.5)	Revised "...US-APWR –unique..." to "...US-APWR's unique...".
		104 (5.1.5)	Deleted "...". Revised description of item (iii) for Responses to Topical Report RAI(Q:18.0-89).
		108 (5.3)	Revised description of first paragraph. Deleted "be" for Responses to Topical Report RAI(Q:18.0-89). Revised "refers" to "refer". Revised "are followings" to "are as follows".
		109 (5.3.1)	Added space and period. Revised "Reference" to "References".
		111 (5.3.2)	Revised "erroneous of" to "errors in".
		112 (5.3.2.1)	Revised "carefully" to "careful".
		112 (5.3.2.2)	Deleted second sentence of first paragraph for Responses to DCD RAI No.594 (Q:18-79).
		113 (5.3.2.2)	Revised "an important" to "a significant".
		113 (5.3.2.4)	Revised "of" to "about".
		115 (5.4.1)	Deleted "be".
		115 (5.4.2)	Revised "to the 1)... 2)..." to "to 1) the... 2) the...".
		117 (5.4.3)	Added description about staffing conditions for Responses to DCD RAI No.412 (Q:18-60).
		118 (5.4.3.1)	Added "an". Revised "because it" to "that".
		119 (5.4.3.1)	Revised "supervisor" to "senior".

Revision	Date	Page (Section)	Description
4 (continued)		124 (5.4.3.2)	Deleted "is used".
		126 (5.5)	Revised description for Responses to DCD RAI No.75 (Q:18-1) and Responses to DCD RAI No.725 (Q:18-102).
		126 (5.5.2)	Deleted "is".
		127 (5.5.2)	Added "shown in the".
		129 (5.6.1)	Revised "Reference" to "References".
		131 (5.6.3)	Deleted "by". Revised "an understandable" to "easy-to-read".
		131 (5.6.4)	Revised "Supervisor" to "Senior".
		132 (5.6.4)	Revised description of last sentence.
		135 (5.7.1)	Revised "Reference" to "References".
		136 (5.7.3)	Revised "chapter" to "Section".
		136 (5.7.3.1)	Revised "is" to "are" in 1st and 3rd bullet.
		138 (5.7.3.2)	Revised following words; "perceived interpreted" to "perceived" "must" to "needs to" "is" to "are"
		139 (5.7.3.2)	Deleted "individual!". Revised following words; "followings" to "the following" "from" to "of"
		140 (5.7.3.2)	Revised "that" to "which".

Revision	Date	Page (Section)	Description
4 (continued)		141 (5.7.3.2)	Added description about historical practice of panel layout for Responses to DCD RAI No.412 (Q:18-59).
		141 (5.7.3.3)	Added "(Phase 3)".
		145 (5.8.1 a)	Revised following words; "computerised" to "computerized" "visualisation" to "visualization"
		146 (5.8.1 b)	Revised following words; "followings" to "the following" "those include" to "involving" Deleted "respectively" and "in".
		146 (5.8.2)	Added "a".
		148 (5.8.2)	Revised description of first sentence. Remove last paragraph to section 5.8.3 for Responses to DCD RAI No.367 (Q:18-44).
		148 (5.8.3)	Added new subsection "5.8.3 Operating Procedure Maintenance" for Responses to DCD RAI No.367 (Q:18-44).
		149 (5.9.2)	Added "the".
		150 (5.9.3)	Added "taught".
		151 (5.9.3)	Revised "used for" to "used in the".
		152 (5.9.5)	Added "is".
		152 (5.9.7)	Revised "unnecessary" to "not necessary". Deleted " ,".
		153 (5.9.8)	Added new section "5.9.8 Training Effectiveness" for Responses to DCD RAI No.370 (Q:18-47_6) .
		154 (5.10)	Revised "Phase 2/3" to "Phase 2 and 3".

Revision	Date	Page (Section)	Description
4 (continued)		155 (5.10.1)	Revised following words; “,” to “of” “is” to “are”
		163 (5.10.2.2.4 e)	Deleted “mark.” Added period.
		166 (5.11)	Deleted “.”. Revised “assess” to “assessed”.
		170 (6.0)	Added reference “44. MUAP-08014, Human System Interface Verification and Validation (Phase 1a)” for Responses to Topical Report RAI(Q:18.0-92). Added reference “45. MUAP-09019, HSI Design” for Responses to Topical Report RAI(Q:18.0-92).
		172 (Appendix A)	Deleted “(Alarm display)”.
		173 (Appendix B)	Revised description in part a, second paragraph for Responses to Topical Report RAI(Q:18.0-91).
		175 (Appendix C)	Revised “is currently occurring” to “occurred”. Added reference numbers for Responses to Topical Report RAI(Q:18.0-92). Deleted “by”. Deleted “will”.
		176 (Appendix C)	Revised “by 6/2012” to “by 12/2017”.
		177 (Figure C-1)	Revised title of Figure C-1
		179 (Appendix D)	Revised description in “item a. Calling Up Switches” column. (Item 4.5.2, “Plant Specific HSI”) for Responses to Topical Report RAI(Q:18.0-89)
		179 (Appendix D)	Revised description in “item b. Controller and Mode Selector” column. (Item 4.5.2, “Plant Specific HSI”) for Responses to Topical Report RAI(Q:18.0-89)

© 2007-2011
MITSUBISHI HEAVY INDUSTRIES, LTD.
All Rights Reserved.

This document has been prepared by Mitsubishi Heavy Industries, Ltd. ("MHI") in connection with its request to the US Nuclear Regulatory Commission ("NRC") for a pre-application review of the US-APWR nuclear power plant design. No right to disclose, use or copy any of the information in this document, other than that by the NRC and its contractors in support of MHI's pre-application review of the US-APWR, is authorized without the express written permission of MHI.

This document contains technology information and intellectual property owned by MHI and Mitsubishi Electric Corporation ("MELCO") relating to the US-APWR and it is delivered to the NRC on the express condition that it not be disclosed, copied or reproduced in whole or in part, or used for the benefit of anyone other than MHI without the express written permission of MHI, except as set forth in the previous paragraph.

This document is protected by the laws of Japan, US copyright law, international treaties and conventions, and the applicable laws of any country where it is being used.

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

Abstract

This topical report describes the functional design of the MHI Human System Interface (HSI) System (HSIS) and the Human Factors Engineering (HFE) process used to create this system and apply it to specific nuclear power plants. The hardware and the software used to implement the HSI system's functional design are described in other topical and technical reports. MHI seeks NRC approval of the HSI system design and its design process for application to the HSI system of the US-APWR and replacement of current HSI systems in operating plants. The HSI system is essentially the same as the HSI system developed by MHI and MELCO for nuclear power plants in Japan. For applications in the US, this report demonstrates conformance of the HSI system design and design process with all applicable US Codes and Standards. These include the applicable provisions of:

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

MHI, MELCO and Japanese PWR Owner Group utilities have developed an advanced HSI system that reflects past human factors studies and employs state of the art electronics technology. The HSI system includes of an operator console, a supervisor console and a Large Display Panel (LDP). It features soft controls for the manipulation through Visual Display Unit (VDUs) with touch panels. The HSI system has been evaluated by Japanese utility operators using a prototype main control board driven by a plant simulator. The facility for this evaluation was prepared by MELCO.

Most of the HSI system is fully computerized, although there are some portions that utilize conventional switches and indicators. The fully computerized portion of the HSI system provides significant benefits to the safety of nuclear power, such as the reduction in operations and maintenance work load, which reduces the potential for human error. Based on the experience in Japan, MHI and MELCO's computerized digital HSI system improves the operability, reliability and availability of plant operations.

This topical report describes the functional design of MHI and MELCO's HSI system, which includes:

- Non-safety HSI based on Visual Display Units which allow monitoring and control of both non-safety and safety functions
- A non-safety Large Display Panel which provides spatially dedicated continuously visible (SDCV) HSI for information important to plant operability and safety
- Safety related HSI based on selectable and SDCV Visual Display Units which allow monitoring and control of safety functions
- Safety related HSI based on spatially dedicated continuously visible information and conventional controls for system level actuation of Reactor Trip and Engineered Safety Feature Actuation Systems
- The ability to monitor and control critical safety functions through systems that are diverse from the HSI and supporting systems described above.

In addition, this topical report describes the HFE design process which considers all elements of NUREG-0711, as follows:

- Human Factors Engineering Program
- Operating Experience Review (OER)
- Functional Requirements Analysis and Function Allocation
- Task Analysis
- Staffing and Qualification
- Human Reliability Analysis (HRA)
- HSI Design
- Operating Procedure Development Plan
- Procedures for Normal Operation
- Procedures for Accident Operation
- Training Program Development Plan
- Human Factors Verification and Validation
- Design Implementation Plan
- Human Performance Monitoring Plan

The HSI system takes advantage of digital technology capabilities that were not available for analog systems. Some of the design aspects of the system may not be readily familiar to those acquainted with previous analog designs. Therefore this document puts special emphasis on the explanation of the technical aspects of the HSI system design and its conformance to codes and standards. The following are key areas in which the design presents significant innovations:

- Multi-channel operator stations
- HSI system's ability to accommodate reduced operator staffing
- Operation under degraded conditions
- Common cause failure modes for Defense-in-Depth and Diversity (D3) analysis
- Minimum inventory of HSI
- Computer based procedures

MHI specifically seeks NRC approval of the HSI system design in these areas.

This report distinguishes between the descriptions applicable to the US-APWR and those relevant to operating plants, where there is a clear need for such a distinction. Where there are no distinctions, the description is generically applicable to the US-APWR and a broad range of operating plants. This generically applicable portion of the design is referred to as the US Basic HSIS. When the US Basic HSIS described in this topical report is referenced in a plant-specific licensing document, such as the US-APWR Design Certification Document or an operating plant Licensing Amendment Request, the Plant Licensing Documentation will identify any areas of this topical report that are not applicable. The Plant Licensing Documentation will describe the completely integrated plant specific HSI system, which includes the specific HSI Inventory (ie. indications, alarms and controls) that are provided using the US Basic HSIS design techniques described in this document. Therefore, the methods described in this document for displaying, alarming and controlling plant components and plant process variables are part of the US Basic HSIS, but any graphics which depict plant systems are only typical, since graphics for a plant specific HSI system will reflect plant specific process system designs.

The complete MHI digital instrumentation and control (I&C) design is described in four reports which have been submitted to the NRC for licensing approval:

- Safety I&C System Description and Design Process (Reference 1)
- Safety System Digital Platform - MELTAC – (Reference 2)
- HSI System Description and HFE Process(Human Factor Engineering) Process (this report)
- Defense in Depth and Diversity (Reference 3)

This document identifies the additional HSI and HFE related information to be submitted for NRC approval in future Plant Licensing Documentation. This Plant Licensing Documentation, in combination with the contents of this topical report and the contents of the other topical and technical reports identified above, is expected to be sufficient to allow the NRC to make a final safety determination. Other documentation generated during the design process is available for NRC audit, as may be needed to allow the NRC to fully review the HSI system design and the HFE design process.

Table of Contents

List of Tables	xxiv
List of Figures	xxv
List of Acronyms	xxvii
1.0 PURPOSE	1
2.0 SCOPE	1
3.0 APPLICABLE CODES, STANDARDS AND REGULATORY GUIDANCE	2
3.1 Code of Federal Regulations	2
3.2 Staff Requirements Memoranda	5
3.3 NRC Regulatory Guides	5
3.4 NRC Branch Technical Positions	7
3.5 NUREG-Series Publications (NRC Reports)	8
3.6 IEEE Standards	9
3.7 Other Industry Standards	10
4.0 DESIGN DESCRIPTION	11
4.1 Design Basis	15
4.2 HSI System Facilities	18
4.2.1 Main Control Room	18
4.2.2 Remote Shutdown Room	20
4.2.3 Technical Support Center	20
4.2.4 Interface with Emergency Operation Facility	21
4.2.5 Local Control	21
4.3 Layout Design	23
4.3.1 Main Control Room Layout	23
4.3.2 Operator Console Layout	27
4.4 Display Overview and Navigation	30
4.4.1 Display Overview	30
4.4.2 Display Navigation System	30
4.5 Operational VDU Display Design	38
4.5.1 Operation Devices	38
4.5.2 Operation Method	38
4.5.3 Switch Features	41
4.6 Safety VDU Display Design	47
4.6.1 Operable Devices	47
4.6.2 Operational VDUs Connect/Disconnect	47
4.6.3 Bypass Permissive	48
4.6.4 Monitor Screen	49
4.6.5 Operation Screen	50
4.6.6 Task-based Screen	52
4.6.7 Multidivisional Safety VDU Screen	52
4.7 Alarm System	53
4.7.1 Alarm Display System	53
4.7.2 Alarm Prioritization	56
4.7.3 Coding by Alarm Sound	60
4.7.4 First-out Alarms Displaying	60
4.7.5 Acknowledging and Resetting Alarms & Stopping Alarm Sound	60
4.7.6 Avoiding Nuisance Alarms	60

4.7.7 Link to Related Display	60
4.8 Computer-Based Operating Procedure	61
4.9 Large Display Panel	66
4.9.1 Purpose of Large Display Panel Installation	66
4.9.2 Large Display Panel Screen Display Features.....	66
4.9.3 Alarm Display on the Large Display Panel.....	69
4.10 Automatic Checking of Actuators	82
4.10.1 Integration of Monitoring and Operation.....	82
4.10.2 Automatic Checking of Actuators for Events	82
4.10.3 Automatic Verification of Critical Safety Functions.....	83
4.10.4 Bypassed and Inoperable Status Indication (BISI).....	83
4.11 Response to HSI Equipment Failures.....	84
4.11.1 Standard Configuration	84
4.11.2 Degraded HSI Systems by a Single Failure.....	85
4.11.3 Loss of All Non-safety HSI	87
4.11.4 Loss of All Digital Non-safety and Safety HSI (CCF)	88
4.11.5 Loss of MCR	89
4.12 Key Technical Issues.....	91
5.0 HFE DESIGN PROCESS.....	94
5.1 Human Factors Engineering Program management	94
5.1.1 Human Factors Engineering Program.....	94
5.1.2 Human Factors Engineering Design Team and Organization.....	96
5.1.3 Human Factors Engineering Processes and Procedures	99
5.1.4 Human Factors Engineering Issues Tracking	103
5.1.5 Human Factors Engineering Technical Program and Milestones	103
5.2 Operating Experience Review (OER).....	106
5.3 Functional Requirements Analysis and Function Allocation	108
5.3.1 Functional Requirements Analysis.....	108
5.3.2 Function Allocation.....	111
5.4 Task Analysis.....	115
5.4.1 Objective of Task Analysis	115
5.4.2 Scope of Task Analysis.....	115
5.4.3 Methodology for Task Analysis	116
5.5 Staffing and Qualification Requirements	126
5.5.1 Operator Staffing Level	126
5.5.2 Number of Operators per Shift.....	126
5.6 Human Reliability Analysis	129
5.6.1 Objectives of HRA.....	129
5.6.2 Scope of HRA	129
5.6.3 HRA Methodology	130
5.6.4 HRA using THERP.....	131
5.6.5 HRA Integration	133
5.7 HSI Design	135
5.7.1 HSI Design Objective	135
5.7.2 Scope of HSI Design.....	135
5.7.3 HSI Design Methodology	136
5.8 Operating Procedure Development Plan.....	145
5.8.1 Procedures to be Developed	145
5.8.2 Procedures Development Process.....	146
5.8.3 Operating Procedure Maintenance	148

5.9 Training Program Development Plan.....	149
5.9.1 Training Program	149
5.9.2 Operator Training Simulator Fidelity	149
5.9.3 Class Room Training for Operators and Technicians	150
5.9.4 Instructor Qualifications and Training.....	151
5.9.5 Role of the HFE Design Team in the Training Development Program	151
5.9.6 Training Program Modifications	152
5.9.7 Retraining.....	152
5.9.8 Training Effectiveness.....	153
5.10 Human Factors Verification and Validation.....	154
5.10.1 Principle of Verification and Validation (V&V)	154
5.10.2 Implementation Plan for HFE V&V	157
5.10.3 Organization of V&V Team	165
5.11 Design Implementation Plan.....	166
5.12 Human Performance Monitoring Plan.....	167
6.0 REFERENCES.....	168
7.0 FUTURE LICENSING SUBMITTALS.....	171
Appendix A History of Development of Japanese PWR Main Control Room by Mitsubishi and Japanese PWR Power Utilities.....	172
Appendix B HFE V&V Experience in Japan	173
Appendix C Phased Implementation Plan	175
Appendix D Scope of the US Basic HSI System and Plant Specific HSI System	178

List of Tables

Table 4.0-1	Comparison of NUREG0711 HFE Program Elements to HFE Program Plan for Japanese PWRs and Additional HFE Program Plan Activities for US Applications	...13
Table 4.3-1	Typical HSI Equipment at Various Locations	...26
Table 4.4-1	Main Purpose of VDUs	...30
Table 4.4-2	Specifications of Operational VDU icons	...33
Table 4.4-3	Specifications of Alarm VDU icons	...36
Table 4.7-1	Static Alarm Priority	...58
Table 4.8-1	Specifications of Operating Procedure VDU icons	...64
Table 4.9-1	Parameters on LDP	...76
Table 5.1-1	Example of Comment Sheet in Review Process	..102
Table 5.2-1	Example of OER Analysis	..107
Table 5.4-1	Task Considerations	..116
Table 5.4-2	Example of Task Analysis Sheet	..120
Table 5.4-3	Task Analysis Summary Sheet	..121
Table 5.4-4	Extended Human Information Processing Model	..124
Table 5.4-5	Example of Detail Task Analysis (Workload) Sheet	..125
Table 5.6-1	Example of Human Reliability Analysis Sheet	..134
Table 5.7-1	Example of Color Coding Rule	..143
Table 5.7-2	Example of Component Symbol (Pump)	..143
Table 5.7-3	Example of Component Symbol (Valve)	..144
Table 7.0-1	Future Licensing Submittals	..171

List of Figures

Figure 4.0-1	HFE Design Process of Past Mitsubishi PWR HSI	...12
Figure 4.0-2	Submittal and Audit Plan for the US-APWR Design Certification	...14
Figure 4.3-1	Distance between Each Console and Large Display Panel	...24
Figure 4.3-2	Voice Level as a Function of Distance and Ambient Noise Level	...24
Figure 4.3-3	Typical Layout of the US-APWR Main Control Room	...25
Figure 4.3-4	Equipments Arrangement of Operator Console	...28
Figure 4.3-5	Equipments Arrangement of Supervisor Console and Shift Technical Advisor Console	...28
Figure 4.3-6	Screen Arrangement of Large Display Panel	...29
Figure 4.4-1	Screen Request Methods for Operational VDU	...32
Figure 4.4-2	Screen Request Methods (Safety VDU)	...34
Figure 4.4-3	Screen Request Methods (Alarm VDU)	...35
Figure 4.4-4	Screen Request Methods (Operating procedure VDU)	...37
Figure 4.5-1	Example of ON/OFF Switch Popup	...39
Figure 4.5-2	Example of Controller Screen	...40
Figure 4.5-3	Example of ON/OFF Switch	...41
Figure 4.5-4	Soft Operation Switch Moving Feature	...42
Figure 4.5-5	Tag Popup Window	...44
Figure 4.5-6	Example of Tag Status Display	...44
Figure 4.5-7	Example of Controller	...45
Figure 4.6-1	Screen Transition of Request Area	...49
Figure 4.6-2	Monitor Screen Menu	...49
Figure 4.6-3	Example of Specific Monitor Screen	...50
Figure 4.6-4	Operation Screen Menu	...50
Figure 4.6-5	Operation Component Menu	...51
Figure 4.6-6	Example of Specific Operation Screen	...51
Figure 4.6-7	Typical Multidivisional Safety VDU Screen	...52
Figure 4.7-1	Alarm VDU Screen Specifications	...55
Figure 4.7-2	Dynamic Alarm Prioritization	...59
Figure 4.8-1	Computer-based Operating Procedure	...63
Figure 4.9-1	Large Display Panel Specifications (Overall)	...68
Figure 4.9-2	LDP Component Alarm Status Display	...69
Figure 4.9-3	LDP Process Parameter Alarm Status Display (1/2)	...70
Figure 4.9-4	LDP Process Parameter Alarm Status Display (2/2)	...71
Figure 4.9-5	LDP Shared Alarm Status Display	...72
Figure 4.9-6	Large Display Panel Specifications (Left Wing)	...73
Figure 4.9-7	Large Display Panel Specifications (Center Wing)	...74
Figure 4.9-8	Large Display Panel Specifications (Right Wing)	...75
Figure 4.10-1	OK Monitor Display Format	...83
Figure 4.11-1	Standard Configurations for the Plant Operation	...84
Figure 4.11-2	Overall I&C System of the US-APWR	...86
Figure 4.11-3	Configurations in Case of Operational VDU Loss	...88
Figure 4.11-4	Configurations in Case of CCF	...89
Figure 4.11-5	Configurations in Case of MCR Loss	...90

Figure 5.1-1	Organization of HFE Design Team	...96
Figure 5.1-2	General Process Procedure of HFE Design	..101
Figure 5.1-3	Overall Design Process	..105
Figure 5.3-1	Hierarchical Structure of Safety Plant Functions	..110
Figure 5.4-1	Task Analysis in HFE Process Flow	..117
Figure 5.4-2	Symbols Used in Operational Sequence Diagram (OSD)	..118
Figure 5.4-3	Model of Human Information Processor by Card et al.	..123
Figure 5.5-1	Operation Personnel Staffing and Organization (Minimum)	..127
Figure 5.5-2	Operation Personnel Staffing and Organization (Typical)	..128
Figure 5.6-1	HRA in HFE Process Flow	..130
Figure 5.6-2	HEP Evaluation in THERP	..131
Figure 5.10-1	Overview of Verification and Validation Activities	..156
Figure B-1	HFE Verification and Validation Flow in the Development Phase	..173
Figure B-2	The Facility Used in Development Phase	..174
Figure C-1	The Facility used for Phase 1 V&V in U.S.	..177

List of Acronyms

AOO	Anticipated Operational Occurrences
ARP	Alarm Response Procedure
ATWS	Anticipated Transient Without Scram
BHEP	Basic Human Error Probability
BISI	Bypassed or Inoperable Status Indication
CCF	Common Cause Failure
CCW	Component Cooling Water
C/C	Control Center
COL	Combined License
CBP	Computer-based Operating Procedure
COTS	Commercial-Off-The-Shelf
CPU	Central Processing Unit
CV	Containment Vessel
D3	Defense-in-Depth and Diversity
DAC	Design Acceptance Criteria
DAS	Diverse Actuation System
DBA	Design Basis Accident
DC	Design Certification
DCD	Design Control Document
DF	Dependency Factor
DHP	Diverse HSI Panel
DMC	Date Management Console
DTM	Design Team Manager
ECCS	Emergency Core Cooling System
EF	Error Factor
EFC	Error-Forcing Contexts
EFW	Emergency Feed Water
ELM	Engineering Line Manager
EOF	Emergency Operations Facility
EP	Back Feed Electric Power
EPM	Engineering Project Manager
ESF	Engineered Safety Feature
ESFAS	Engineered Safety Feature Actuation System
FMEA	Failure Modes and Effects Analyses
FC	Fail to Close
FC	First Concrete
FO	Fail to Open
F.O.	First Out
FTA	Fault Tree Analysis
GOMS	Goals, Operators, Methods, and Selection rules
GUI	Graphical User Interfaces
HA	Human Action

HAZOP	Hazards and Operability Analysis
HDSR	Historical Data Storage and Retrieval
H.E	Human Error
HED	Human Engineering Discrepancy
HEP	Human Error Probability
HEPA	High-Efficiency Particulate Air
HFE	Human Factors Engineering
HFEVMTM	HFE V&V Team Manager
HRA	Human Reliability Analysis
HSI	Human System Interface
HSIS	Human System Interface System
HVAC	Heating, Ventilation, and Air Conditioning
I&C	Instrumentation and Control
ITAAC	Inspections, Tests, Analyses, and Acceptance Criteria
ITV	Industrial Television
LBB	Leak Before Break
LBLOCA	Large Break Loss Of Coolant Accident
LC	Locked to Close
LCO	Limiting Condition for Operation
LDP	Large Display Panel
LER	Licensee Event Report
LERF	Large Early Release Frequency
LO	Locked to Open
LOCA	Loss Of Coolant Accident
MCB	Main Control Board
MCR	Main Control Room
M/C	Metal Clad Geer
MELCO	Mitsubishi Electric Corporation
MELTAC	Mitsubishi Electric Total Advanced Controller
MHI	Mitsubishi Heavy Industries
MSLB	Main Steam Line Break
NIS	Nuclear Instrumentation System
NPP	Nuclear Power Plant
OER	Operation Experience Review
OSD	Operational Sequence Diagram
PAM	Post Accident Monitor
PCMS	Plant Control and Monitoring System
PM	Project Manager
PRA	Probabilistic Risk Assessment
PRC	Process Recording Computer
PSF	Performance Shaping Factor
PSMS	Protection and Safety Monitoring System
QA	Quality Assurance

RCS	Reactor Coolant System
R.G.	Regulatory Guide
RHR	Residual Heat Removal
RMS	Radiation Monitoring System
RO	Reactor Operator
RPS	Reactor Protection System
RSC	Remote Shutdown Console
RSR	Remote Shutdown Room
RSS	Remote Shutdown Station
RT	Reactor Trip
RTB	Reactor Trip Breaker
RWSP	Refueling Water Storage Pit
SAR	Safety Analysis Report
SAT	Systematic Approach to Training
SDCV	Spatially Dedicated Continuously Visible
SER	Safety Evaluation Report
SFP	Spent Fuel Pit
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SLS	Safety Logic System
SBO	Station Black Out
SPDS	Safety Parameter Display System
SRO	Senior Reactor Operator
SS	Shift Supervisor
STA	Shift Technical Advisor
Tcold	Reactor Coolant Inlet Temperature
T/C	Thermocouple
Thot	Reactor Coolant Outlet Temperature
THERP	Technique for Human Error Rate Prediction method
TMI	Three Mile Island
TR	Topical Report
TSC	Technical Support Center
UMC	Unit Management Computer
UPS	Uninterruptible Power Supply
UV	Under Voltage
V&V	Verification and Validation
VDU	Visual Display Unit
VTM	V&V Team Manager

1.0 PURPOSE

The purpose of this topical report is to describe the Mitsubishi Heavy Industries (MHI) Human System Interface (HSI) System (HSIS) design and the Human Factors Engineering (HFE) design process used by MHI for that system. MHI seeks approval from the US Nuclear Regulatory Commission for the use of the MHI HSI system for new nuclear plants and for operating nuclear plants.

The design process described in this report is applicable to the MHI Human System Interface designs for both new and existing operating plants. The system descriptions are directly applicable to the MHI US-APWR. For operating plants the basic design features that ensure regulatory compliance are maintained, as described in this report. However, due to plant differences, specific changes in implementation detail will be described in Plant Licensing Documentation (e.g., License Amendment Request or Final Safety Analysis Report).

2.0 SCOPE

In this report the complete set of safety and non-safety HSI components is referred to as the HSI system. The safety-related HSI elements described in this report are part of the Protection and Safety Monitoring System (PSMS). The PSMS includes the Reactor Protection System, the Engineering Safety Feature Actuation System, the Safety Logic System and the Safety-Grade HSI system. The non-safety HSI elements described in this report are part of the Plant Control and Monitoring System (PCMS) or the Diverse Actuation System (DAS). The PCMS includes reactor and turbine control systems. The DAS provides backup monitoring and control for critical safety functions.

The HSI for the PSMS is built on the MELTAC Platform, which is described in a separate Digital Platform technical report. In addition, the MELTAC Platform is applied to portions of the HSI for the Plant Control and Monitoring System. The MELCO computer used for non-safety applications is a different design than that used for safety-related applications. There are also differences in Quality Assurance processes for the design and manufacturing of both. The DAS, including its HSI, is diverse from the PCMS and the PSMS. These safety and non-safety systems are described in this report only to the extent necessary to understand their HSI. Other reports describe the design of the hardware and software of these systems and the design process used to create that hardware and software.

This report includes two parts. The first part, Section 4, describes the HSI system design. The second part, Section 5, describes the design process used in creating that design.

3.0 APPLICABLE CODES, STANDARDS AND REGULATORY GUIDANCE

This section identifies the HSI system's compliance with applicable codes, standards and regulatory guidance. Unless specifically noted, the latest version of the codes and standard or regulatory guidance issued as of the date of this document is the applicable one. The following terminology is used in this section:

Plant Licensing Documentation – This refers to plant level documentation that is specific to a group of plants or a single plant, such as the Design Control Document (DCD), Combined Licensing (COL) Application, Final Safety Analysis Report, or License Amendment Request.

HSI System - This refers to the functional design of the safety and non-safety HSI components that are the subject of this topical report. The "HSI System" includes the MHI safety related and non-safety related HSI. The terms "PSMS HSI", "PCMS HSI" and "DAS HSI" refer to different elements of the overall HSI system.

The codes and standards applicable to MHI's complete digital I&C system are described in other topical and technical reports. The codes and standards identified below are those that directly affect the functional design of the HSI system.

3.1 Code of Federal Regulations

1. 10 CFR 50 Appendix A: General Design Criteria for Nuclear Power Plants

- GDC 1 : Quality Standards and Records
The Quality Assurance program for the MHI system meets the requirements of 10 CFR 50 Appendix B.
- GDC 5 : Sharing of Structures, Systems, and Components
In general, there is no sharing of this equipment among nuclear power units. Any sharing is discussed in specific Plant Licensing Documentation.
- GDC 12 : Suppression of Reactor Power Oscillations
HSI for specific reactor trip functions is described in Plant Licensing Documentation.
- GDC 13 : Instrumentation and Control
HSI for specific instrumentation and control functions are described in Plant Licensing Documentation.
- GDC 19 : Control Room
The HSI system provides the safety-related and non-safety related Human System Interface for the control room. The Human Factors Engineering design aspects of the HSI and the control room design are described in this report Subsection 4.2.1 and Section 4.3.
- GDC 20 : Protection System Functions
HSI for specific protection system functions is described in Plant Licensing Documentation.

- GDC 21 : Protection System Reliability and Testability
The HSI for manual test features for the areas that are not covered by automated tests are described in this report. Most manual tests may be conducted with the plant on line, and with the protection functions bypassed or out of service. Equipment that cannot be tested with the plant on line can be tested with the plant shut down.
- GDC 22 : Protection System Independence
Redundant protection system divisions are provided for all automated and manual protective functions. The non-safety related HSI (Section 4.5) and safety related HSI (Section 4.6) used for plant or protection system monitoring and used to take manual protective actions provide an integrated human systems interface, while maintaining the independence of the protection system divisions.
- GDC 23 : Protection System Failure Modes
All detected failures are alarmed. The HSI for failure detection and alarms are described in this report Section 4.11.
- GDC 24 : Separation of Protection and Control Systems
Where safety sensors are shared between control and protection systems, signal selection logic in the control system prevents erroneous control actions due to single sensor failures. The HSI used for sensor monitoring and failure alarms is described in this report Section 4.7 and Subsection 4.9.3.
- GDC 25 : Protection System Requirements for Reactivity Control Malfunctions
HSI features to monitor and alarm reactivity control malfunctions are described in this report Section 4.7 and Subsection 4.9.3.

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

- (iii) Control room design
The Human Factors design aspects of the HSI and the control room are described in this document Section 4.2.1 and 4.3.
- (iv) Safety Parameter Display Console
The PCMS HSI described in this report provides safety parameter displays in the control room Section 4.5 and 4.9.
- (v) Bypassed and inoperable safety system status indication
This indication is provided by the PCMS HSI.
- (xi) Relief and safety 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
The HSI for items xi thru xiv and xvii through xx above are described in this topical report. Specific display designs are described in Plant Licensing Documentation.

3. 10 CFR 50.36 Technical specifications

1) Safety limits, limiting safety system settings, and limiting control settings.

The HSI system is used to monitor safety limits and control limits.

3) Surveillance requirements

The HSI system provides extensive automatic testing, as discussed above with respect to GDC 21. It is used for periodic surveillances 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.

4. 10 CFR 50.55.a

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

The HSI system 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 the equipment comprising the system.

(h) Invokes IEEE Std. 603-1991

See compliance with IEEE 603-1991

5. 10 CFR 50.62 ATWS Rule

The Diverse Actuation System is used to actuate plant systems for Anticipated Transient Without Scram (ATWS) mitigation. The DAS HSI is described briefly in this topical report and in more depth in the topical report for Defense in Depth and Diversity.

6. 10 CFR 50.54(m)(2)(iii)

Section 5.4 of the topical report describes how the HSI system supports the following minimum Main Control Room staffing requirements:

(iii) When a nuclear power unit is in an operational mode other than cold shutdown or refueling, as defined by the unit's technical specifications, each licensee shall have a person holding a senior operator license for the nuclear power unit in the control room at all times. In addition to this senior operator, for each fueled nuclear power unit, a licensed operator or senior operator shall be present at the controls at all times. That section of the report also describes how this HSI supports higher staffing levels. Actual staffing levels are described in Plant Licensing Documentation.

7. 10 CFR 52.47

(a)(2) Level of Detail

The information provided in this topical report, together with the additional information described in other digital system topical and technical reports and DCD, are sufficient to allow the NRC staff to reach a final conclusion on all safety questions associated with the design before certification of the US-APWR design is granted. 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 HSI system is expected to be applied to conventional I&C safety and

non-safety functions typical of current operating plants and new evolutionary plants. In the longer term, the HSI system is expected to be applied to such innovative safety functions as may be typical of new passive plants. All specific plant safety functions are described in the Plant Licensing Documentation.

8. 10 CFR 52.79(c) ITAAC in Combined Operating License Applications
The inspections, tests, analyses and acceptance criteria that demonstrate that the HSI system has been constructed and will operate in conformity with the Commission's regulations will be provided in the Plant Licensing Documentation.

3.2 Staff Requirements Memoranda

9. SRM to SECY 93-087
Item II.Q: Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems
Diverse monitoring and diverse manual control functions are provided by this HSI.

Item II.T Control Room Annunciator (Alarm) Reliability
Alarm annunciators are generally provided by the PCMS HSI. For alarms which is indicated in the safety VDU is shown in Section 4.6. Any exceptions to this are described in the Plant Licensing Documentation.

3.3 NRC Regulatory Guides

10. R.G. 1.8 Personnel Selection and Training
The HSI system copes with operating staffs and training system for operator staffs. The Reg. Guide endorses ANSI/ANS-3.1-1993 and ANSI/ASME NQA-1-1983. See with these ANSI Standards.
11. R.G. 1.22 Periodic Testing of Protection System Actuation Functions
See GDC 21. Protection actuation functions are completely testable through a combination of overlapping automatic and manual tests. Manual tests can only be conducted when a division is bypassed. Divisions are interlocked to prevent concurrent bypassing of redundant functions in more than one redundant division. The HSI system supports manual tests, and displays and alarms for interlocks and automatic test results.
12. R.G. 1.47 Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems
See compliance with 10 CFR 50.34 (f)(2)(v). The PCMS HSI provides alarms 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 division level. The ability to manually actuate bypassed or inoperable alarms at the division level is provided for conditions that are not automatically detected.
13. R.G. 1.62 Manual Initiation of Protective Actions
The PSMS HSI provides manual initiation at the system level for all reactor protection system (RPS) and engineered safety feature actuation system (ESFAS) safety functions by conventional Spatially Dedicated Continuously Visible (SDCV) switches located in the main control room. Additional system level manual initiation switches may also be located

at the Remote Shutdown panel, depending on the specific plant design; these are described in the Plant Licensing Documentation.

14. R.G. 1.97 Instrumentation for Light Water Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident (endorses IEEE Std. 497-2002)
The PCMS HSI displays signals from accident monitoring instrumentation of all variable Types. In addition, the PSMS HSI displays signals for Type A and B variables and meets all applicable Class 1E requirements. Display designs for specific accident monitoring instrumentation are described in the Plant Licensing Documentation.
15. R.G. 1.105 Setpoints for Safety-Related Instrumentation (endorses ISA-S67.04-1994 and ANS-10.4-1987)
The uncertainties associated with the PSMS and PCMS are described in the Safety System and Digital Platform technical reports. They include uncertainties for signal conditioning modules, signal splitters, instrument loop power suppliers and analog to digital converters. The displays and alarms from the PSMS HSI and PCMS HSI are generated from the digital values within the controllers of these systems. Therefore, there are no additional uncertainties associated with the HSI for these systems. The uncertainties associated with the DAS HSI are negligible in meeting the acceptance criteria of BTP-19.
16. R.G. 1.114 Guidance to Operators at the Controls and to Senior Operators in the Control Room of a Nuclear Power Unit.
See compliance with 10 CFR 55.54
17. R.G. 1.118 Periodic Testing of Electric Power and Protection Systems (endorses IEEE 338-1987)
See compliance with GDC 21, 10 CFR 50.36 and R.G. 1.22. All safety functions are tested either automatically or manually. Manual tests do not require any system reconfiguration, such as jumpers or fuse removals, which have a potential for human performance errors.
18. R.G. 1.149, Rev.3 Nuclear Power Plant Simulators for Use in Operator Training (endorses ANSI/ANS-3.5-1998)
The HFE program plans to develop operator training program are described in this report Section 5.9 and Plant Licensing Documentation.
19. R.G. 1.152 Criteria for Programmable Digital Computers in Safety Systems of Nuclear Power Plants (endorses IEEE 7-4.3.2-2003)
The methods used for specifying, designing, verifying, validating and maintaining software for the PSMS HSI complies with these Regulatory Guide requirements. The life cycle process for the digital platform software is described in the Digital Platform technical report. The life cycle process for the system application software is described in the Safety I&C System Description and Design Process technical report. The methods used for controlling cyber threats throughout the life cycle are described in these documents.
20. R.G. 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 603-1991 is discussed below.
21. R.G. 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)

The PSMS HSI 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 Digital Platform technical report. The design processes for plant systems are described in the Safety I&C System Description and Design Process technical report.

22. R.G. 1.174 An approach for using probabilistic risk assessment in risk-informed decisions on plant specific changes to the licensing basis
The HFE program approaches risk-informed view of points in task analysis, HRA, etc.

23. R.G. 1.177 An Approach for Plant-Specific, Risk-Informed Decision making: Technical Specifications
The HFE program approaches risk-informed view of points in task analysis, HRA, etc.

24. R.G. 1.187 Guidance for Implementation of 10 CFR 50.59, Changes, Tests, and Experiments R.G. 1.196 Revision 02 Control Room Habitability at Light-water Nuclear Power Reactors
Control Room Habitability systems ensure the main control room (MCR) environment is adequate to allow operators to maintain plant control limits during normal operation and to maintain plant safety limits during and after anticipated transients or design basis accidents. The systems to ensure Control Room Habitability are described in Plant Licensing Documentation.

3.4 NRC Branch Technical Positions

25. BTP 7-1 Guidance on Isolation of Low-Pressure Systems from the High-Pressure Reactor Coolant System
26. BTP 7-2 Guidance on Requirements of Motor-Operated Valves in the Emergency Core Cooling System Accumulator Lines
27. BTP 7-3 Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps out of Service
28. BTP 7-4 Guidance on Design Criteria for Auxiliary Feedwater Systems
29. BTP 7-5. Guidance on Spurious Withdrawals of Single Control Rods in Pressurized Water Reactors
30. BTP 7-6 Guidance on Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode

The HSI system provides displays, alarms and controls for the plant components that address BTP 7-1 thru 7-6, above. Specific HSI designs are described in Plant Licensing Documentation.

31. BTP 7-8 Guidance for Application of Regulatory Guide 1.22
All functions of the protection system are testable at power. The HSI system supports this testing.
32. BTP 7-9 Guidance on Requirements for Reactor Protection System Anticipatory Trips
There are no non-safety anticipatory trips used in the reactor protection system. Any exception to this will be described in Plant Licensing Documentation. If any non-safety trips are used in the protection system the HSI system would support such trips. .
33. BTP 7-10 Guidance on Application of Regulatory Guide 1.97
The HSI system complies with this BTP for displays and alarms for all instrumentation

signals. However, R.G. 1.97 Revision 4 has superseded Revisions 2 and 3, for which this BTP was written. Therefore, where there are conflicts, the HSI system meets the requirements of R.G. 1.97 Revision 4.

34. BTP 7-12 Guidance on Establishing and Maintaining Instrument Setpoints
See compliance with R.G. 1.105.
35. BTP 7-16 Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52
See compliance with 10 CFR 52.47. This Design Acceptance Criterion applies only to HSI system final display designs and HFE validation. The level of detail needed for the NRC staff to make a final safety determination is described in Plant Licensing Documentation.
36. BTP 7-17 Guidance on Self-Test and Surveillance Test Provisions
See compliance with GDC 21, 10 CFR 50.36, R.G. 1.22 and R.G. 1.15. Surveillance testing, taken together with automatic self-testing, provides a mechanism for detecting all failures. The HSI system supports both functions.
37. BTP 7-19 Guidance on Evaluation of Defense in Depth and Diversity in Digital Computer Based I&C Systems
The Defense-in-Depth and Diversity (D3) topical report describes the diversity within the safety and non-safety I&C systems, including the diversity between the PSMS HSI, PCMS HSI and DAS HSI. That report also describes the methodology for coping with an Anticipated Operation Occurrence (AOO) or Postulate Accident (PA) concurrent with a common cause failure (CCF) of the PSMS and PCMS. The D3 Coping Analysis method includes justification for credited manual operator actions which is evaluated through the HFE Program described in this report. Coping for all Anticipated Operation Occurrences and Postulate Accidents is described in Plant Licensing Documentation. This report describes the functional design of the PSMS HSI, PCMS HSI and DAS HSI.
38. BTP 7-21 Guidance on Digital Computer Real Time Performance
The real-time performance for the HSI system complies with this BTP. The method for determining response time performance for the PSMS HSI is described in the Safety I&C System Description and Design Process technical report. The response time performance for digital platform components is described in the Digital Platform technical report.

3.5 NUREG-Series Publications (NRC Reports)

39. NUREG-0654, Criteria for Preparation and Evaluation of Radiological Emergency
The HSI system is used for monitoring and managing radiological emergencies.
40. NUREG-0696 Functional Criteria for Emergency Response Facilities
The PCMS HSI provides plant information at the Emergency Response Facilities such as Technical Support Center, Emergency Operating Facilities, etc.
41. NUREG-0700, Human-System Interface Design Review Guidelines
The HSI system design complies with these guidelines.
42. NUREG-0711, Human Factors Engineering Program Review Model
The design process used for the development of the HSI system and the training of

personnel in the use of this system to operate the plant comply with the guidelines in this NUREG.

43. NUREG-0737, Supplement 1 Clarification of TMI Action Plan Requirements

The HSI system is used to comply with the following TMI Action Plan Requirements:

- Plant Safety Parameter Display – The HSI system provides safety parameter displays 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: -- The HSI system provides non-safety related and safety related displays for monitoring safety related instruments and non-safety related and safety related controls for safety related plant components.

44. NUREG-0800 Chapter 7 of the USNRC Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, Rev.4

The HSI system 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 provided in the Plant Licensing Documentation.

45. NUREG-0800 Chapter 18 of the USNRC Standard Review Plan for the Review of Human Factors Engineering for Nuclear Power Plants, Rev.1

The requirements of this NUREG for Human Factors Engineering Design Process are met by the HSI system. Descriptions of specific plant display screens and validation activities are described in the Plant Licensing Documentation.

46. NUREG-0899 Guidelines for the Preparation of Emergency Operating Procedures

The HSI system is used to display and execute Emergency Operating Procedures.

47. NUREG-1220 Training Review Criteria and Procedures

The training phase of the HFE Program complies with these requirements.

48. NUREG-1358 Lessons Learned From the Special Inspection Program for Emergency Operating Procedures

The procedure development phase of the HFE Program complies with these requirements.

49. NUREG-1560 Individual Plant Examination Program: Perspectives on Reactor Safety and Plant Performance

The performance monitoring phase of the HFE Program complies with these requirements.

50. NUREG-1764 Guidance for the Review of Changes to Human Actions

The performance monitoring phase of the HFE Program complies with these requirements.

3.6 IEEE Standards

51. IEEE 7-4.3.2 2003 Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations

The PSMS HSI conforms to all requirements of this standard, as augmented by R.G. 1.152, including key requirements for:

- Software quality and life cycle processes

- Independent Verification and Validation

- Communications independence

The HSI functional designs described in this topical report provide input to the software design process.

52. IEEE 338 1987 Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems

The HSI system supports compliance with this standard, as augmented by R.G. 1.22.

53. IEEE 494 1974 Method for identification of Documents Related to 1E Equipment

The documentation for the PSMS HSI 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.

54. IEEE 497 2002 Accident Monitoring Instrumentation for Nuclear Power Generating Stations

See compliance with R.G. 1.97.

55. IEEE 603 1991 Safety Systems for Nuclear Power Generating Stations (1998 version is currently not endorsed by NRC)

The HSI system conforms to this standard, as augmented by R.G. 1.153, including key requirements for:

- Quality

- Testability

- Monitoring and Information

- Bypasses

3.7 Other Industry Standards

56. ANSI/ANS 3.1 Rev.1 -1999 Selection, Qualification, and Training of Personnel for Nuclear Power Plants

See compliance with R.G. 1.8.

4.0 DESIGN DESCRIPTION

This section describes the main design features of the MHI HSI system. This HSI system has been designed in a joint project between MHI, MELCO and Japanese PWR Owner Group utilities (See Appendix A).

Figure 4.0-1 shows the design process for the MHI HSI system and the relationship between the design steps and the twelve Human Factor Engineering (HFE) elements presented in NUREG-0711, rev.2. HFE elements E01, E02, E03, E04, E05, E06, E07, E08, E10 and E11 were included in the design process with Japanese utilities, Elements E09 and E12 were not part of the design process in Japan. This topical report describes the HFE elements that were encompassed in the development program in Japan, the plan for the remaining two HFE elements (E09 and E12), and the plan for a more refined Human Reliability Analysis (HRA) methodology.

Table 4.0-1 compares the NUREG0711 HFE program elements to the elements in the HFE program implemented for Japanese PWRs. This table also identifies additional program plan activities conducted for US applications. A description of the HFE Program Plan is in the next section of this topical report.

Figure 4.0-2 shows the plan for submitting HSI/HFE documentation and making other HSI/HFE documentation available for audit for the US-APWR.

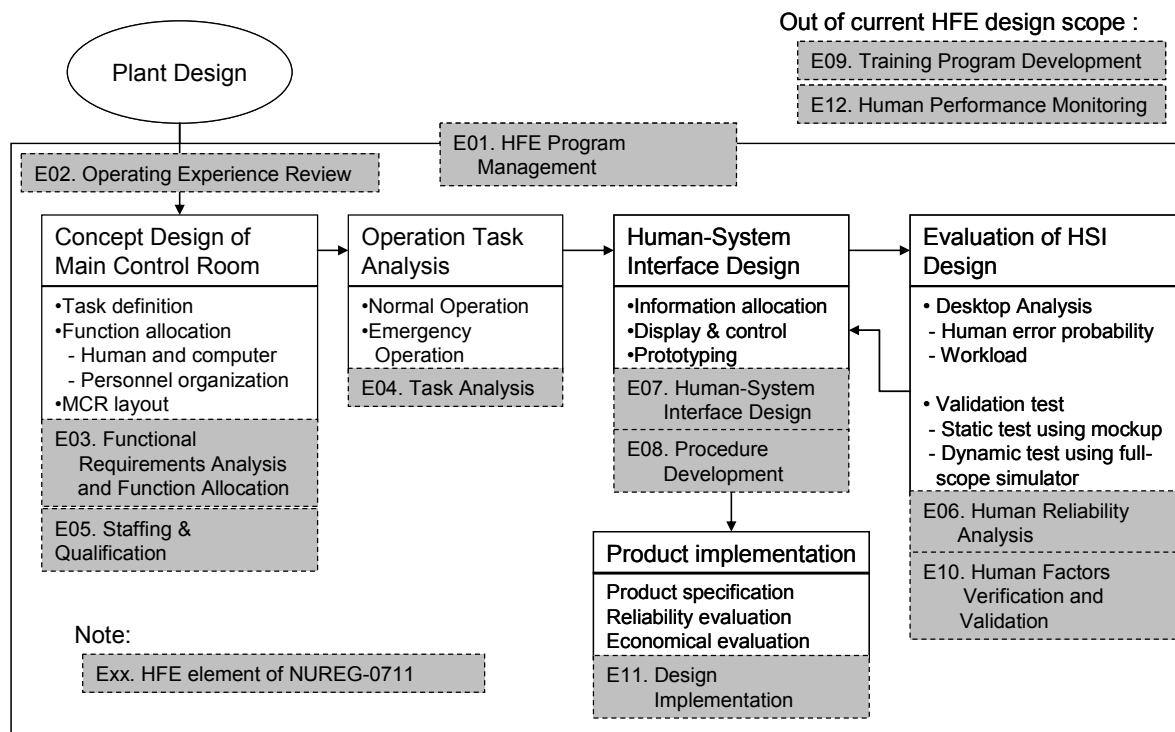


Figure 4.0-1 HFE Design Process of Past Mitsubishi PWR HSI

Table 4.0-1 Comparison of NUREG0711 HFE Program Elements to HFE Program Plan for Japanese PWRs and Additional HFE Program Plan Activities for US Applications

HFE element	Program Plan for US Applications	Experience in past development of Japanese PWR main control room
E01. HFE Program Management	MHI's design process conforms to NUREG-0711 normally. Additional documentation is required.	NUREG-0711 HFE elements, E01, E02, E03, E04, E05, E06, E07, E08, E10 and E11 were executed in the design process. E09 and E12 were out of scope (activity of power utility). (See Figure A.1 Figure A.1 HFE Design Process of Mitsubishi PWR)
E02. Operating Experience Review	Approach is same as Japanese PWR	Operation Experience is input information of the concept design phase.
E03. Functional Requirements Analysis and Function Allocation	Approach is same as Japanese PWR	Functional requirements analysis and function allocation is considered in the concept design phase.
E04. Task Analysis	Approach is same as Japanese PWR	OSD was used in a gross and narrative task analysis, and Card's human information processing model was used in detail task analysis.
E05. Staffing and Qualifications	MHI proposes operation with one SRO and one RO in the MCR for compliance with 10CFR50.54	Design goal of operation with one RO
E06. Human Reliability Analysis	Approach is same as Japanese PWR	Omission and select errors were mainly analyzed. Human error probabilities were calculated using THERP for selected scenarios.
E07. Human-System Interface Design	Approach is same as Japanese PWR	Design plan was improved through iterative design process (design, prototyping , desktop evaluation, validation test).
E08. Procedure Development	Approach is same as Japanese PWR	Operation Procedure was developed for dynamic validation test.
E09. Training Program Development	Implementation plan is added	Out of scope from HSI development
E10. Human Factors Verification and Validation	Approach is same as Japanese PWR	Two type of test was executed. One is static test using HSI mockups. The other is dynamic test using prototype HSI system and full-scope plant simulator.
E11. Design Implementation	Implementation plan is added	Out of scope from HSI development
E12. Human Performance Monitoring	Implementation plan is added	Out of scope from HSI development

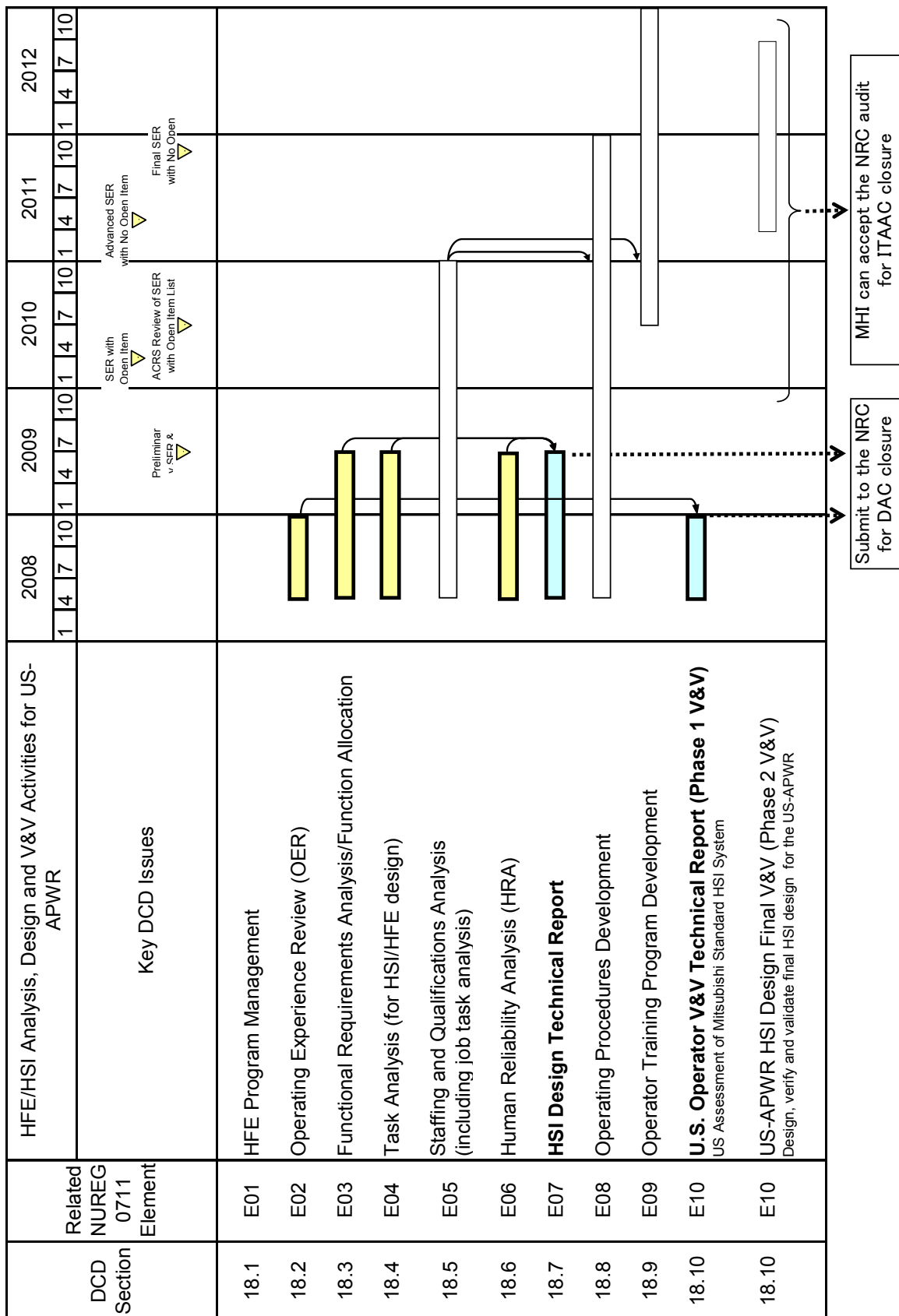


Figure 4.0-2 Submittal and Audit Plan for the US-APWR Design Certification

4.1 Design Basis

The HSI system introduces the use of soft (touch or click based) operation utilizing the computer-based HSI. (See section 4.5) Soft operations are performed by requesting an Operational visual display unit (VDU) screen on an Operational VDU and then touching or clicking an operation area of a soft switch displayed on the screen. The benefits of the soft operation are to reduce the operator's workload compared with that of the conventional HSI by providing relevant process control information in integrated displays on VDUs and utilizing a compact console that minimizes required operator movement. The HSI system also provides operation support functions that utilize the computer to consolidate large amounts of data into meaningful information displays. These advanced features of the HSI system are expected to improve overall operator performance and reduce the potential for human error.

The HSI system utilizes various visual display devices, color-coding symbol-coding, etc. It is designed for use by plant personnel having average visual ability (i.e., no weaknesses in visual power or color-blindness limitations).

The key features of the HSI system are summarized below, and explained in detail in the sections that follow

a. Integration of monitoring and operation

The main actions of plant operators consist of checking the standby condition of equipment before operation, monitoring the plant parameters (direct and relevant parameters) and identifying plant behavior during operation. In order to improve the operability of the plant, all safety and non-safety soft controls and the relevant information, such as component status and relevant parameters, are integrated onto non-safety multi-channel VDUs. The non-safety multi-channel VDUs are the primary operator interface for all plant conditions, normal and accident. To support this design basis, the Operational VDUs are classified as Important-to-Safety (similar to the Safety Parameter Display System) and they are seismically qualified. Safety VDUs provide backup HSI for failures of the non-safety multi-channel VDUs. The Safety VDUs also provide interlocks and controls to ensure that the non-safety multi-channel VDUs cannot create failure conditions that would degrade the safety functions.

The basis for this multi-channel integration is as follows:

- Safety functions are monitored by multiple non-safety and safety instrumentation (e.g., narrow range - wide range, in-cores – ex-cores)
- Multiple safety and non-safety success paths exist for all critical safety functions (e.g., Charging - Safety Injection, Main Feed – Aux Feed, Sprays - Reliefs)
- Integrated safety and non-safety monitoring and control on multi-channel VDUs provides the following benefits:
 - Continuous awareness of critical safety functions while immediate focus may be plant maneuvering and power production.
 - A single operator can execute procedures that historically involve multiple operators to coordinate multiple safety divisions and non-safety systems. This simplifies task coordination for maintaining critical safety functions.
 - Operators can execute computer based procedures with integrated information and manual controls (e.g., via hyperlinks).
 - Minimizes operator transitions between safety and non-safety VDUs, thereby reducing operator workload during critical plant situations.

These benefits reduce operator task burden and reduce the potential for human error.

b. Automatic verification of component status

When a significant plant operating event occurs such as a plant shut down or an emergency core cooling system (ECCS) actuation in an emergency, the operator's workload and level of stress increase. This stress is caused by the simultaneous operations that need to be performed such as collecting the safety-related information, confirming plant conditions, etc. In the HSI system, the status of components such as valves and breakers and the status associated with plant trip signals, ECCS signals and isolation signals are automatically checked by comparing their status with the expected status defined in the computer archives.

c. Inter-linked screen request

Individual display screens are designed for monitoring specific plant systems or functions. All the related information required for related tasks such as alarm diagnosis, control actions, procedure execution, monitoring auxiliary functions, etc can be requested on the screen. Screens for related tasks are inter-linked in terms of the functional and/or operational relationship.

d. Use of Large Display Panel for situation awareness and information sharing

The primary purpose of the Large Display Panel (LDP) is to provide Spatially Dedicated Continuously Visible (SDCV) information to operation personnel to enhance situation awareness. The LDP helps operators maintain continuous awareness of overall plant status and critical status changes, while they are engaged in operational details on a VDU display for a specific plant system or function. The secondary purpose of the LDP is to help the operations staff coordination and communication by providing a common visualization of plant information.

The following functions are provided by the LDP so that all of operators understand overall plant conditions:

- Display of key parameters and key component status for normal operation and emergency conditions. The selection basis for the information displayed on the LDP is described below.
- Grouped alarm displays and dynamic alarm prioritization to aid operator response decisions.
- Display the computer-checked results of component status verifications which support the operator's confirmation task.
- Integration of all information in a graphic display that allows easy understanding of the plant situation and quick recognition of status changes.

e. Alarm prioritization system

A dynamic prioritized alarm system is provided to avoid information overload and facilitate plant state identification. The alarm function in the Plant Control and Monitoring System (PCMS) compiles many simultaneous alarms and displays them on the Alarm VDUs and on the LDP, with color coordination categorized in three levels. Moreover, the priority of an individual alarm can be changed depending on the importance of additional alarms, so that when more critical/important alarms are activated, the overall plant status is easily recognized

using LDP and Alarm details can be confirmed and acknowledged on the Alarm VDU. Alarms are also shown in graphic displays on the Operational VDU representing the related parameter's numerical value with red color and switch information (i.e., trip, power-off, etc.).

f. Main Control Room Staff

The above-mentioned features make it possible to operate the plant by just one Reactor Operator (RO) and one Senior Reactor Operator (SRO) in the Main Control Room (MCR) during postulated plant operating modes. This Main Control Room staffing meets the regulatory requirements of 10 CFR 50.54(m)(2)(iii). The normal MCR staff is supplemented by one additional SRO and one additional RO that will be at the plant to accommodate unexpected design conditions, such as conditions where the HSI system is degraded. This overall plant staffing meets the regulatory requirements of 10 CFR 50.54(m)(2)(i). While the HSI system is designed to support the minimum MCR and plant staffing described above, the space and layout of the Main Control Room are designed to accommodate the foreseen maximum number of operating and temporary staff. Accommodations for additional staff are described below.

g. Applicable plant personnel

Plant personnel addressed by the HFE program include licensed control room operators as defined in 10 CFR Part 55 and the following categories of personnel defined by 10 CFR 50.120:

- non-licensed operators,
- shift supervisor,
- shift technical advisor,
- instrument and control technician,
- electrical maintenance personnel,
- mechanical maintenance personnel,
- radiological protection technician,
- chemistry technician,
- engineering support personnel.

In addition, any other plant personnel who perform tasks that are directly related to plant safety are addressed in the HFE program.

h. Overriding automatic systems

In general, automatic safety actuation signals are prioritized over opposite manual actuation signals. However, to allow periodic testing or maintenance, safety actuation signals can be manually inhibited by the "Lock" button. (See 4.5.3 a)

To avoid potential human error of unintentionally leaving a component in the "Lock" mode after testing or maintenance, bypass alarms for each train are continuously displayed on the LDP."

4.2 HSI System Facilities

Facilities included in the scope of the human factors engineering program are the main control room (MCR), the technical support center (TSC), the remote shutdown room, the emergency operations facility (EOF), and local control stations.

4.2.1 Main Control Room

The MCR is the place for process control and supervision in all plant situations. In addition, it provides the means for communication to others outside the plant. Finally, it is the center to initiate the maintenance of process-related equipment.

The following features are provided in the MCR:

- Within the "process control area"
 - working places for two plant operators,
- Within the "shift supervision area"
 - working place for a MCR operating crew leader,
 - working place for an additional personnel needing timely information on the process state (e.g., shift technical advisor). This can also be used as a spared work place to cope with the unavailability of one of the two work places used by the operators.
- Within the "common control area"
 - Diverse Actuation System HSI Panel (DHP) for accident mitigation and safe shutdown in case of loss of the digital I&C and HSI. This includes also the space to store and to manipulate the appropriate operating documentation and procedures;
 - LDP giving a common understanding of the plant state to the operators;
 - fire alarm board, and control board for centralized fire fighting actions in the MCR or its immediate proximity; this also includes the space to store the appropriate fire alarm sheets and procedures,
 - Maintenance Console which is used to support an additional operator in the MCR for periodic inspections and tests during plant shutdown conditions. This console is a temporary console which is disconnected from the digital data communication bus during normal plant operation. The Maintenance Console is on wheels so that it can be positioned any where in the MCR,
- communication board (internal, external),
- working place for temporary personnel,
- working area for reading paper based documentation,
- places for the printers and for the workstations giving access to plant or office applications,
- facilities for storing paper-based documentation.

The computer-based HSI working places for the additional personnel that are expected at the plant during outages and commissioning are located in the computer room or the switching and tagging room.

The facilities for the shift changes are found in the common control room.

The MCR is designed to remain functional during and after earthquakes. A fire in the MCR may initially affect one division of safety or non-safety equipment. HSI in the MCR will be disabled before the fire propagates to other divisions. When the HSI in the MCR is disabled the HSI at the Remote Shutdown Station is enabled to allow safe shutdown. An accident is not postulated concurrent with a MCR fire.

4.2.2 Remote Shutdown Room

The Remote Shutdown Room (RSR) is located in a different fire zone than the MCR. The Remote Shutdown Console (RSC), which is located in the RSR has capabilities to achieve and maintain cold shutdown.

Operators can monitor and control the plant using the VDUs on the RSC to shutdown the plant, to maintain a hot shutdown condition and also transfer to maintain a cold shutdown condition. VDUs on the RSC provide the same screens as that of the main control room, this reduces the need for additional training and minimizes the potential for human error.

Fire protection and security is adequately considered in the design of the RSR and RSC. The controls on the RSC are normally disabled. They are activated by a switching device that transfers control between the main control room and the RSR. These transfer switching devices are located in separate rooms.

The HSI display design is basically the same as that of the MCR. The RSC consists of following devices:

- Operational VDUs (They also have capability of alarm display and audible signals)
- Safety VDUs

The following physical means are provided in the RSR

- Working area for reading paper based documentation.
- Facilities for the storing paper-based documentation.

Limiting the use of the RSC for safe shutdown is entirely administratively controlled, since all HSI functions available in the MCR are also available at the RSP.

4.2.3 Technical Support Center

The onsite technical support center (TSC) provides the following functions:

- Provides plant management and technical support to plant operations personnel during emergency conditions.
- Relieves the reactor operators of peripheral monitoring and communications duties not directly related to reactor system manipulations.
- Prevents congestion in the MCR.
- Performs EOF functions for the alert emergency class, for the Site Area Emergency class and the General Emergency class until the EOF is functional.

The TSC has facilities to support the plant management and technical personnel who will be assigned there during an emergency and will be the primary onsite communications center for the plant during the emergency.

The facility consists of a plant data display system using VDUs and a LDP, data communication system, tele-communication system of telephones and facsimiles by multiple methods of transmission including private and public lines, satellite communications and adequate working area.

The TSC is located within the Auxiliary Building. The walking time from the TSC to the control room is less than 2 minutes.

The TSC working space is sized for a minimum of 25 persons, including 20 persons designated by the licensee and five NRC personnel. The minimum size of the working space provided is approximately 75 sq ft/person.

The TSC is not seismic Category I or qualified as an engineered safety feature (ESF). The well-engineered structure of the Auxiliary Building provides an adequate capability to withstand earthquakes.

The TSC ventilation system functions in a manner comparable to the control room ventilation system. The TSC ventilation system is not seismic Category I qualified, redundant, instrumented in the control room, or automatically activated to fulfill its role. A TSC ventilation system that includes high-efficiency particulate air (HEPA) and charcoal filters is provided.

The HSI display design is basically the same as that of the MCR. The TSC is equipped with the following devices:

- Operational VDUs (They also have capability of alarm display and audible signals. They are used for monitoring only and no control function is provided.)
- Large Display Panels

4.2.4 Interface with Emergency Operation Facility

The Emergency Operation Facility (EOF) is a near site or on-site support facility for the management of overall licensee emergency response (including coordination with federal, state, and local officials), coordination of radiological and environmental assessments, and determination of recommended public protective actions.. The EOF receives plant process data from the SPDS function of the PCMS which also provides data for the MCR, the TSC and the RSR. The PCMS provides an adequate fire-wall function to prevent cyber invasions from outside the plant.

4.2.5 Local Control

Manual controls are installed in local control stations (only manned on demand) for functions which:

- Require frequent component manipulation during local equipment maintenance that would excessively burden MCR operators. These components also have a manual controls in the MCR. Components which have manual controls in both the MCR and local area are controlled and managed by a tagging system.
- Require frequent process related monitoring and control actions that are not practical to automate. These manual actions would excessively burden MCR operators and these processes require no or minimal co-ordination with the MCR.
- Process related monitoring and control actions related to manual monitoring or manipulations that must be done in close proximity to the process equipment (e.g., manual batch chemical additions)

Although manual controls are not provided in the MCR for some of these functions, monitoring is provided in the MCR for all local functions.

Local controls are installed in local control stations. Local stations are equipped with either conventional HSI devices (push buttons, light indicators, etc.) or with computer and screen-based equipment. HSI device selection considers technical and economical conditions. In addition to the manual controls identified above, local controls are also credited for degraded HSI conditions in the MCR, such as MCR VDU blackout or software CCF in digital systems. These local controls operate independently of the failed HSI devices.

The local HSI is designed with consideration of the information, controls and procedures needed, and the limits of the functions implemented. This includes HSI device selection, as well as layout of conventional controls and/or computer screens, and facilities for laydown and storage of paper procedures.

4.3 Layout Design

4.3.1 Main Control Room Layout

The layout of the HSI system in the MCR is determined by the role assigned to each operator. The supervisor directs the operator in the conduct of plant operations and checks the operator's actions. Accordingly, the supervisor console is located behind the operator console. The shift technical advisor advises the supervisor on safety-relevant operations and also monitors the operator's actions. Therefore, the Shift Technical Advisor Console is located near the Supervisor Console and behind the Operator Console. The LDP provides the shared information to the operation personnel. Therefore, the LDP is located at the location where it is visible to all of the operation staff.

The distance between the Operator Console, the Supervisor Console, and the Shift Technical Advisor Console is defined considering walking passage and their ability to communicate verbally with each other over the ambient noise.

The distance between each console and the LDP and the size of the characters and symbols on the LDP are coordinated considering the visibility of the information displayed on the LDP from each console.

a. Distance between LDP and Operator Console

The LDP is located within the viewing area from each console (i.e., the Operator Console, the Supervisor Console and the Shift Technical Advisor Console). The viewing area is defined as the viewing angle with each operator seated at the console.

The LDP view from the operator console - the LDP is visible in the vertical direction and within the horizontal view of an operator sitting at the operator console.

Considering the acceptable limit of viewing angle is not more than 30 degree off the centerline of each LDP display, according to NUREG-0700 rev.2, the minimum distance is approximately 14 feet (4 meters).

b. Distance between Operational console and Supervisor Console/Shift Technical Advisor Console

In the main control room, each member of the operations crew (the reactor operators, the supervisor and the shift technical advisor) are on duty sitting down at their respective consoles. The distance between the Supervisor Console and the Operator Console is less than 17 feet. The distance is defined primarily by their communication capability in their seated positions under the ambient noise conditions.

The information exchange nature of the oral communications sets the minimum conditions that are acceptable.

NUREG-700 rev.2 was utilized to determine the maximum distance at which voice communication is usually possible.

The ambient noise level of the main control room used is based on the design target value of 55 dB.

A plot of possible distance to maintain voice communication versus the ambient noise level, taken from NUREG-0700 rev.2, is shown in Figure 4.3-2.

The maximum distance at which voice communication is possible is about 17 feet (5 meter) for an ambient noise level of 55 dB. This distance is based on the fact that the operator speaks in a raised voice when executing operational duties.

c. Distance between Each Console and Large Display Panel

The distance between each console and the LDP is set considering the vertical and horizontal viewing field of the operator, and the visibility of information displayed on the LDP.

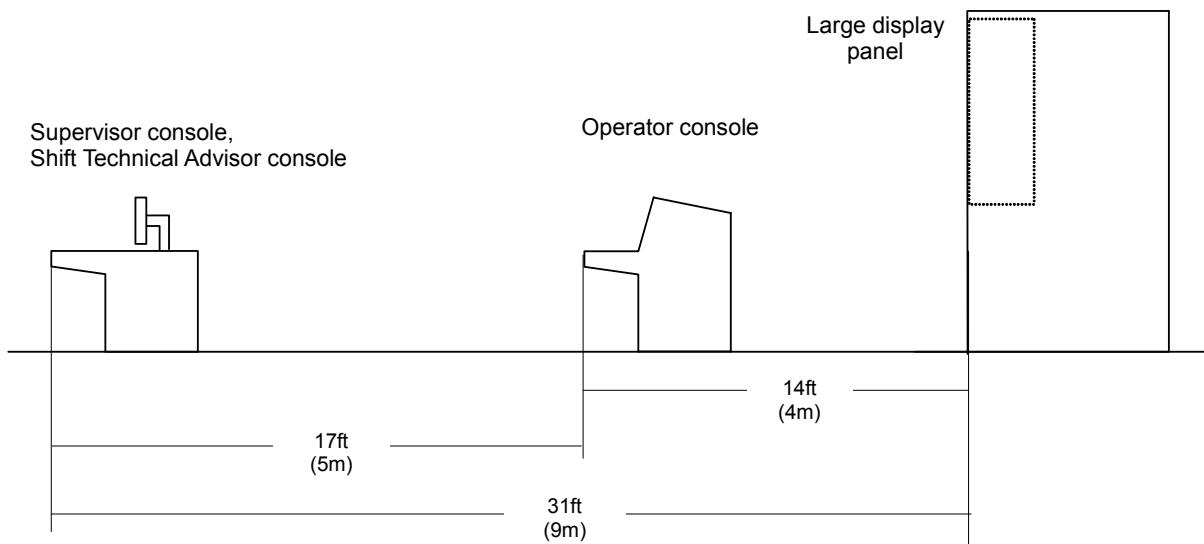


Figure 4.3-1 Distance between Each Console and Large Display Panel

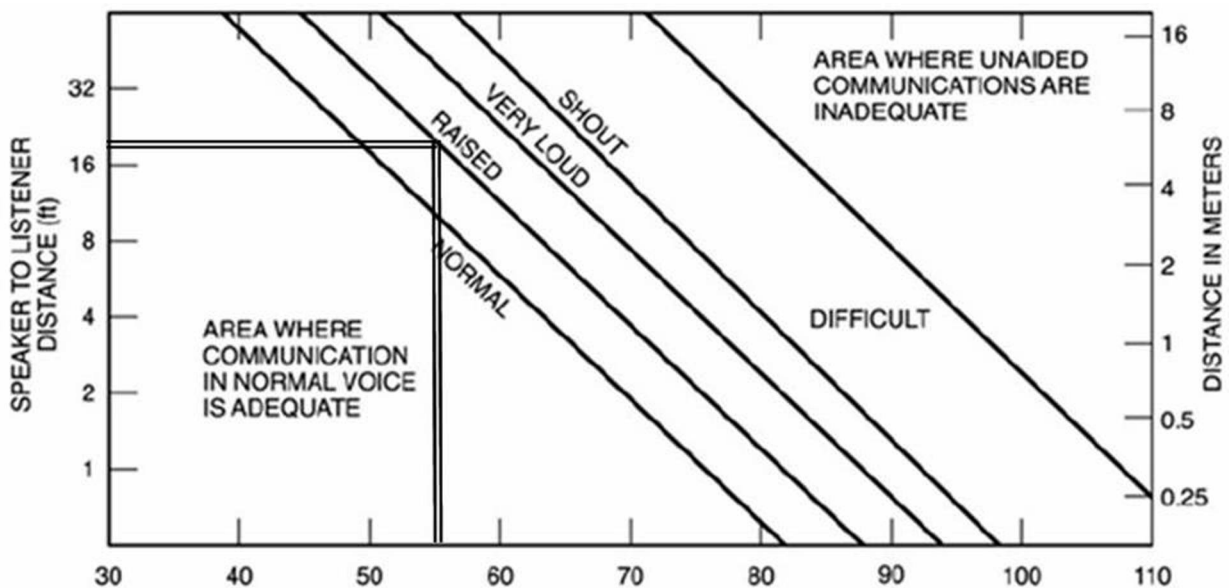


Figure 4.3-2 Voice Level as a Function of Distance and Ambient Noise Level

Figure 4.3-3 shows the typical layout of the main control room. Major HSI equipment in the main control room and other locations relevant to the control of plant operations are presented in Table 4.3-1.

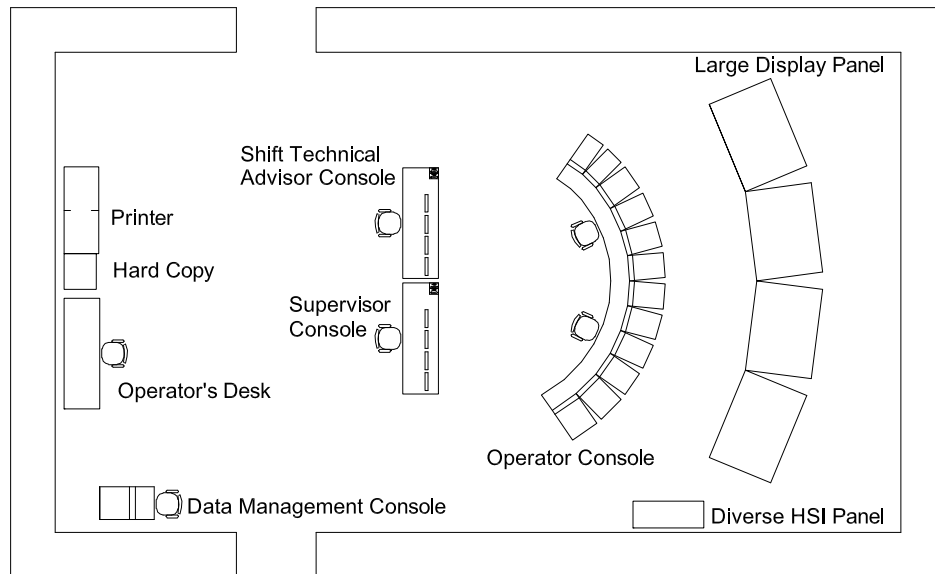


Figure 4.3-3 Typical Layout of the US-APWR Main Control Room

Table 4.3-1 Typical HSI Equipment at Various Locations

Place	Equipment	Function
MCR	Operator Console	Plant operation for any situation of the plant (incl. startup/shutdown, emergency). Can accommodate one or two operators.
	Large Display Panel	Plant status display shared by all the operators in MCR
	Diverse HSI Panel	Conventional switches and indicators for safety operation (for backup in the event of common cause failure)
	Supervisor Console	Plant monitoring by MCR supervisor (monitoring only, no operation)
	Shift Technical Advisor Console	Plant monitoring by Shift Technical Advisor (monitoring only, no operation)
	Data Management Console (DMC)	Data management and reporting from HSI system computers
	Maintenance Console	Additional console for the plant outage operation and inspections The same capability of operator console Temporarily set in use
RSR	Remote Shutdown Console	Remote shutdown operation when MCR is not available
TSC	TSC Computer	Plant management and technical support to the reactor operating personnel located in the control room during emergency conditions
EOF	EOF Computer	Management of overall licensee accident management (including coordination with Federal, State, and local officials), etc.

4.3.2 Operator Console Layout

The arrangement of the equipment at the operator console, supervisor console, shift technical advisor console and large display panel are illustrated in Figure 4.3-4, 5 and 6.

The shape, dimensions and arrangement of each console meet ergonomic design standards. Hard-wired device selection principles are as follows:

- System level operation switches to be used by operators in the event of an emergency are based on the standards and guidelines (IEEE-603-1991) related to safety systems. Means are provided in the MCR for manual initiation of protective functions at the system level:

- Reactor trip
- Actuation of ECCS
- Containment vessel (CV) isolation phase A
- Main steam flow isolation
- Main feedwater isolation
- Emergency feedwater flow isolation
- Actuation of emergency feedwater flow
- Actuation of containment vessel spray and containment vessel isolation phase B
- Main control room heating, ventilation, and air conditioning (HVAC) isolation
- Charging water flow isolation

Note: these are the examples at present state of design and the changes are defined in the Plant Licensing Documentation (e.g., DCD)

- Above functions are realized by conventional hard-wired Class 1E module switches that permit easy and prompt access by the operator.
- The bypass or inoperable state of reactor protection system (RPS) and engineered safety feature actuation system (ESFAS) and ESF system are displayed on the LDP as SDCV information.
- Means for monitoring and control of safety and non-safety systems at the system and/or component level are realized by the Operational VDUs. Safety VDUs also provide monitoring and component level control for safety functions and satisfy Class 1E requirements. Operating Procedure VDUs provide electronic versions of paper procedures with navigational hyperlinks to specific screens on Operational VDUs.
- Indicators, lamps and switches required for diverse backup as a countermeasure against software common cause failures are provided on a conventional control panel which is independent from the consoles.

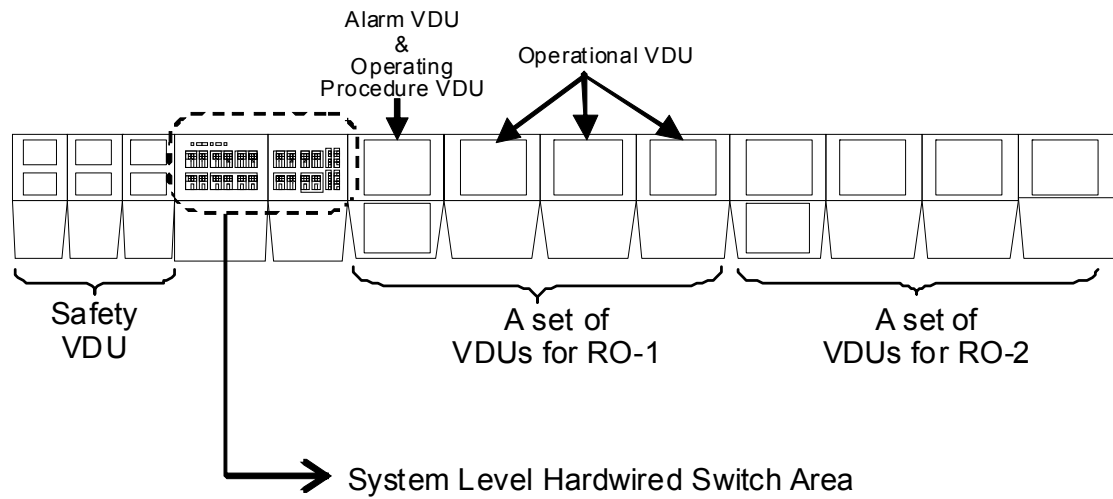


Figure 4.3-4 Equipments Arrangement of Operator Console

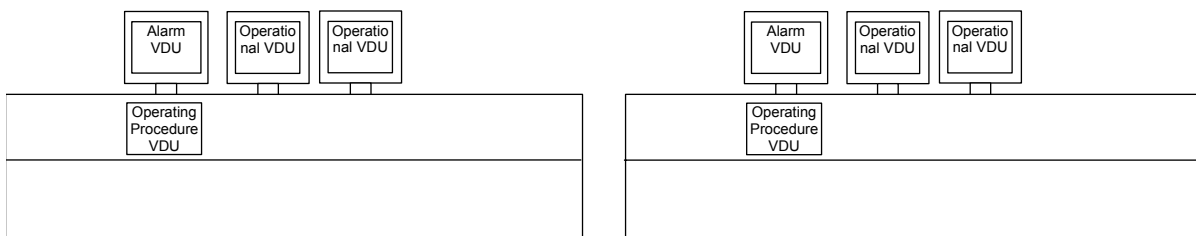


Figure 4.3-5 Equipments Arrangement of Supervisor Console and Shift Technical Advisor Console

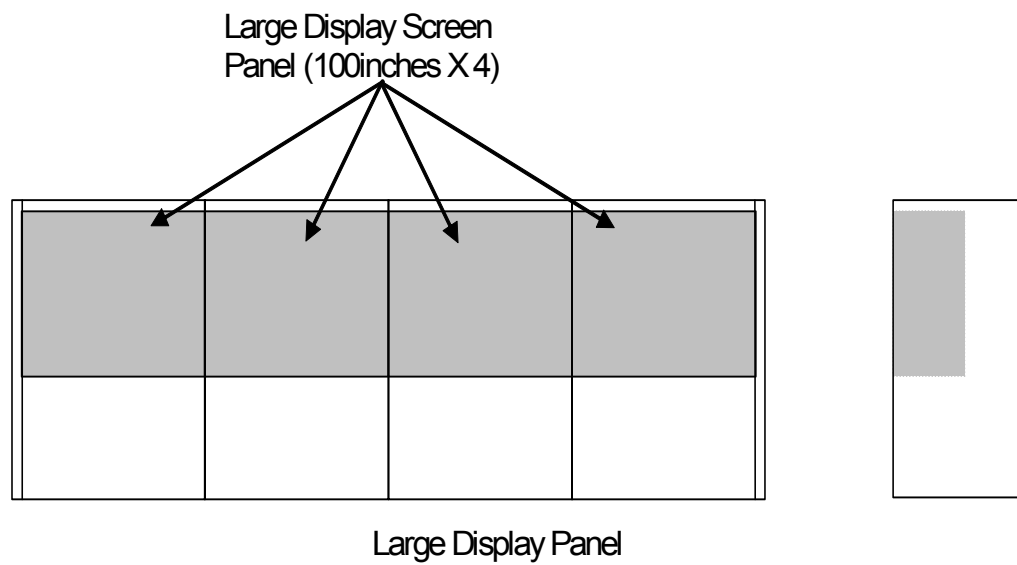


Figure 4.3-6 Screen Arrangement of Large Display Panel

4.4 Display Overview and Navigation

4.4.1 Display Overview

The following types of VDUs are installed in the operator console, the supervisor console and the technical advisor's console. The main purpose of each VDU is summarized in Table 4.4-1.

Table 4.4-1 Main Purpose of VDUs

Item	Main Purpose
Operational VDU	To execute all of the plant control and monitoring functions, including control of the safety systems.
Safety VDU	To execute the safety-related control and monitoring functions as a backup for the Operational VDU. It can control operation signals from the Operational VDU.
Alarm VDU	To acknowledge and display individual alarms using prioritization color codes. Alarm VDU also provides the alarm confirmation/non-confirmation information to the operator.
Operating procedure VDU	To provide computer-based operation procedure displays near the Operational VDU and the Alarm VDU in order to facilitate and simplify the performance of operation procedure.

The group of Operational VDU display formats also provides the safety parameter display system (SPDS) functions.

Each VDU display design and function is explained in the following sections. (See section 4.5, 4.6, 4.7 and 4.8)

4.4.2 Display Navigation System

To make access to each display easy and simple, a navigation system has been developed for each VDU.

a. Operational VDU

There are multiple paths of calling up displays in the operational VDU. Figure 4.4-1 illustrates the navigation system for calling up the displays.

The top navigation display (item (A) in the figure) is commonly used for navigating the operational VDU display information. Using the top navigation display, any operational displays can be selected within two display selection steps. This is based on the following display navigation design:

- All operational displays are grouped system by system by the number. The number is defined by the assignment capacity for the same group display request area (the bottom area in the operational VDU screen).
- The representative display (the system display is normally chosen) is selected directly from the top navigation display.

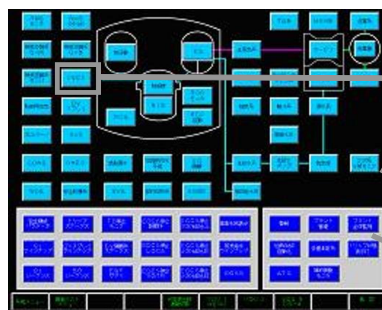
- The other operational displays are selected from the representative display using the same group display request function located on the bottom area of each operational VDU displays.

In addition, a related display which belongs to another system can be selected directly from each operational VDU screen.

Any operational displays can be also requested from a screen list menu display. (item (C) in the figure)

The related operational display can be also selected from the Alarm VDUs. (See section 4.8.3)

(A) Request from the top navigation display (B) Related screen request



(C) Request from screen list menu (3)



(D) Request from alarm VDU screen



Screen request area for the related displays which belong to the different groups.



Graphic Area

Screen request area for the same display group

Note: See table 4.4-2 for specifications of operational VDU navigation icons, (1)-(10).
See table 4.4-3 for specifications of Alarm VDU icons.

Figure 4.4-1 Screen Request Methods for Operational VDU

Table 4.4-2 Specifications of Operational VDU icons

No	Type	Color/icon Color/letter	Shape	Function
(1)	System display request area	Light blue Black	Rectangle	Top menu of system or component displays grouped by each system (e.g., CVCS,PZR)
(2)	Emergency display request area	Blue White	Rectangle	Directly screen selectable area concerning emergency related screens. (e.g., TRIP STATUS, ECCS VALVE STATUS)
(3)	Function menu area	Black Green	Rectangle	Generic display selection function (e.g., change the screen list menu, move to the previous screen)
(4)	Group list	Same as (1)(2)	Rectangle	Group names are listed here. Grouping is equal to (1)(2).
(5)	Scroll bar	Light gray	Rectangle	Scroll bar to select (4).
(6)	Screen number	Same as (1)(2)	Rectangle	Screen number of each screen. (e.g., CS-1 for CVCS screen-1)
(7)	Screen name	Light gray Black	Rectangle	Individual screen names are listed here.
(8)	Scroll bar	Light gray	Rectangle	Scroll bar to select (6)(7).
(9)	Screen request area (same group)	Light gray Black	Rectangle	Select screens included in the same group from the current screen.
(10)	Screen request area (other group)	Light blue Black	Rectangle	Select screens not included in the same group from the current screen.

b. Safety VDU

With regard to display navigation, there are two types of safety VDUs - selectable and SDCV safety VDU. The selectable safety VDU has navigation displays. (See Figure 4.4-2) The top navigation displays are divided between the operation and monitoring, respectively but they are hyper-linked by a navigation support toolbar which is located and continuously visible on the left side of each display, in each top navigation display, the hyper-link buttons are assigned system by system. The navigation system also has a hierarchical structure but enables simple and easy display access avoiding a deep hierarchy and adopting a navigation support tool.

The variable set display area requires two screens which are distributed to two SDCV safety VDUs.

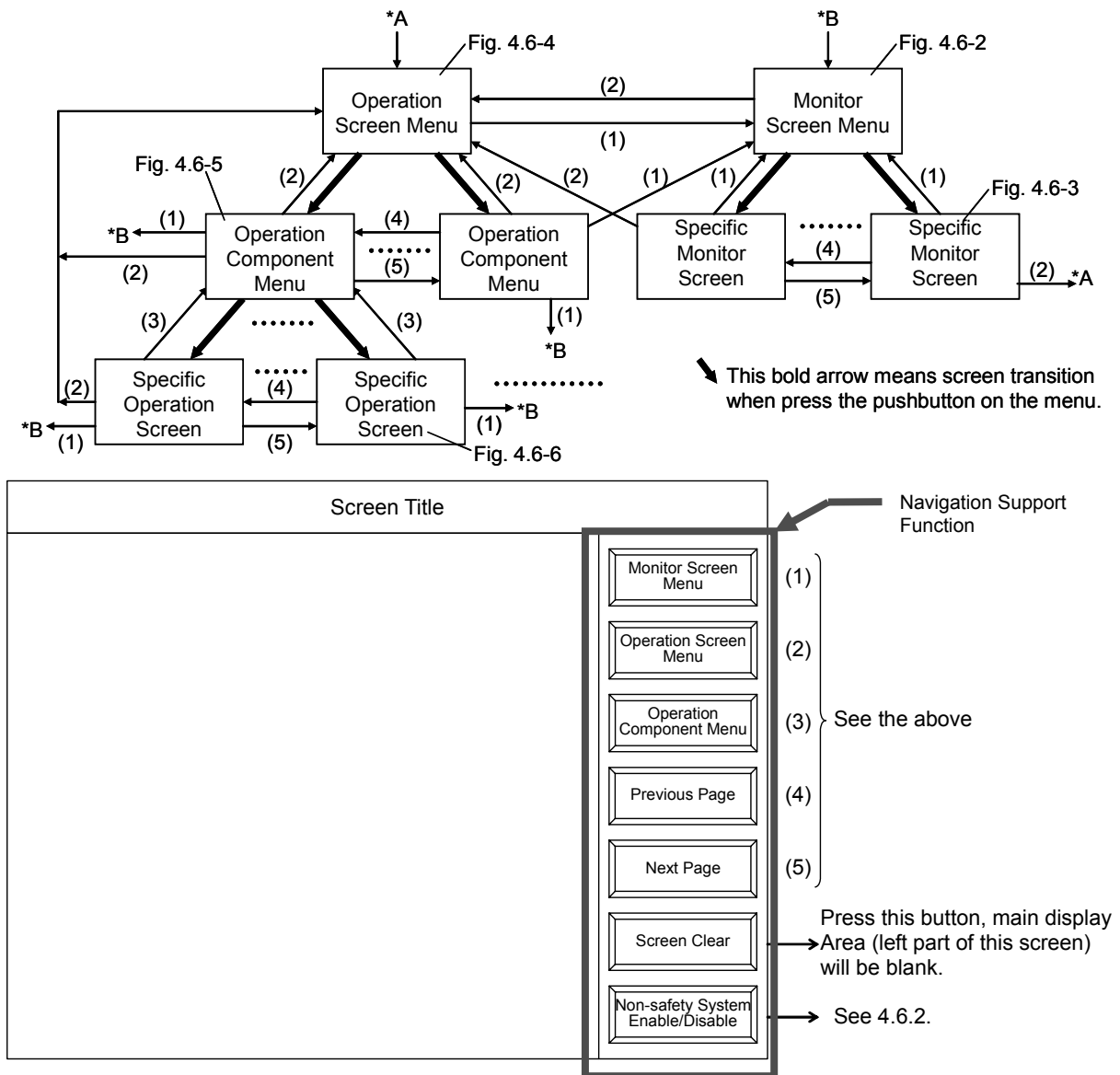
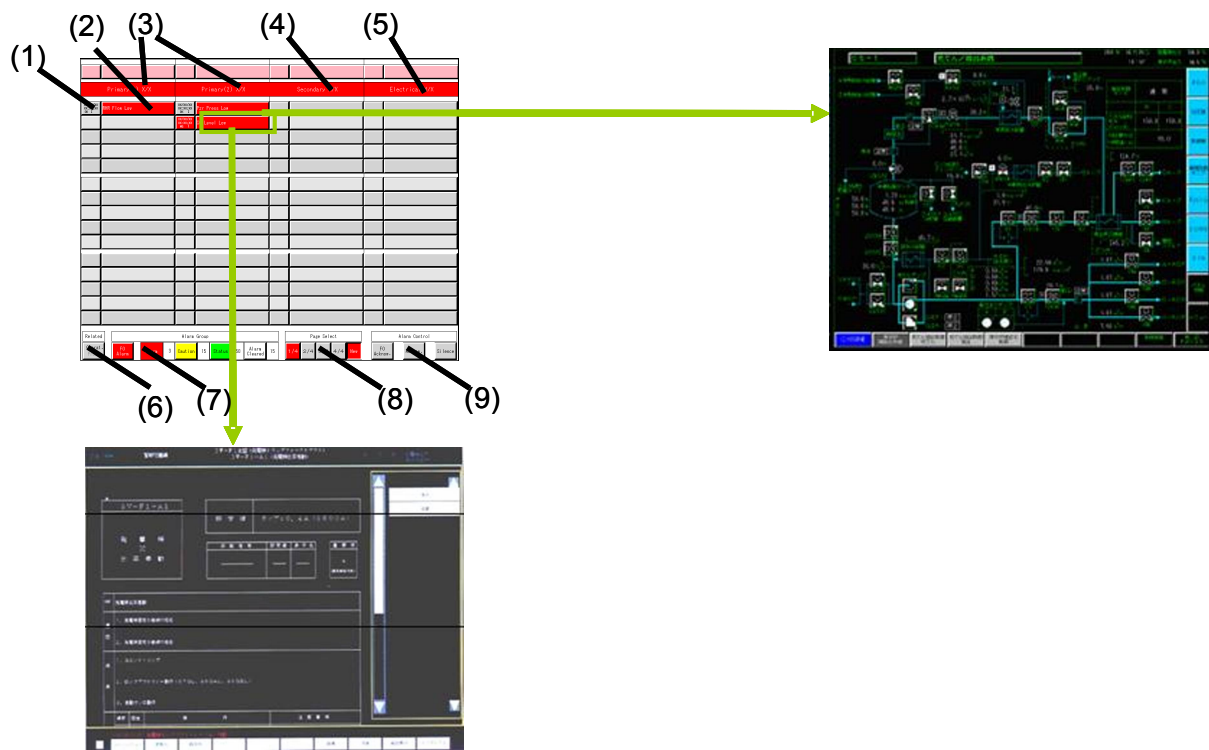


Figure 4.4-2 Screen Request Methods (Safety VDU)

c. Alarm display navigation

When an alarm message displayed on the alarm VDU screen is touched or clicked, the related display can be selected on the operational VDU near the Alarm VDU.

Or the alarm response procedure (Alarm Response Procedure (ARP); one of the plant operating procedures) can also be selected by touching or clicking the alarm message on the Alarm VDU display.



Note: See table 4.4-3 for specifications of alarm VDU navigation icons, (1)-(9). Also see Figure 4.7-1 for larger image of alarm VDU.

Figure 4.4-3 Screen Request Methods (Alarm VDU)

Table 4.4-3 Specifications of Alarm VDU icons

No.	Type	Color/icon Color/letter (Normal mode)	Color/icon Color/letter (Alarm mode)	Shape	Function
(1)	Support information	-	Light gray Black	Rectangle	Date & time when alarms occur and Static Priority are displayed
(2)	Alarm name	Light gray Black	R/Y/G W/Bk/Bk	Rectangle	Alarm name is displayed in red, yellow or green by dynamic priority system.
(3)	Primary system area	Red White	Red White	Rectangle	Primary system alarms are displayed here.
(4)	Secondary system area	Red White	Red White	Rectangle	Secondary system alarms are displayed here.
(5)	Electrical system area	Red White	Red White	Rectangle	Electrical and transmission system alarms are displayed here.
(6)	Select screen mode	Light gray Black	Light gray Black	Rectangle	Alternative mode switches or select request screen (Operational VDU display or ARP) when touched or clicked an alarm name.
(7)	Alarm group	R/Y/G/W W/Bk/Bk/Bk	R/Y/G/W W/Bk/Bk/Bk	Rectangle	Total number of alarms (red), caution (yellow) status (green) and cleared alarms (white).
(8)	Page select	Light gray Black	Red White	Rectangle	Page is selected in case that number of alarms in a page overflows.
(9)	Alarm control	Light gray Black	Light gray Black	Rectangle	First out Acknowledge area, Acknowledge area, and Silence area. Touching or clicking "Acknowledge", flicker stops and sound stops. Touching or clicking "Silence", buzzer stops.

Note: R: Red Y: Yellow G: Green W: White Bk: Black

d. Operating procedure display navigation

On the operating procedure display, related operation display names/numbers are displayed with procedures. In addition, the related operational display is selected on the Operational VDU near the operating procedure VDU by touching or clicking the display request area on the operating procedure VDU display.

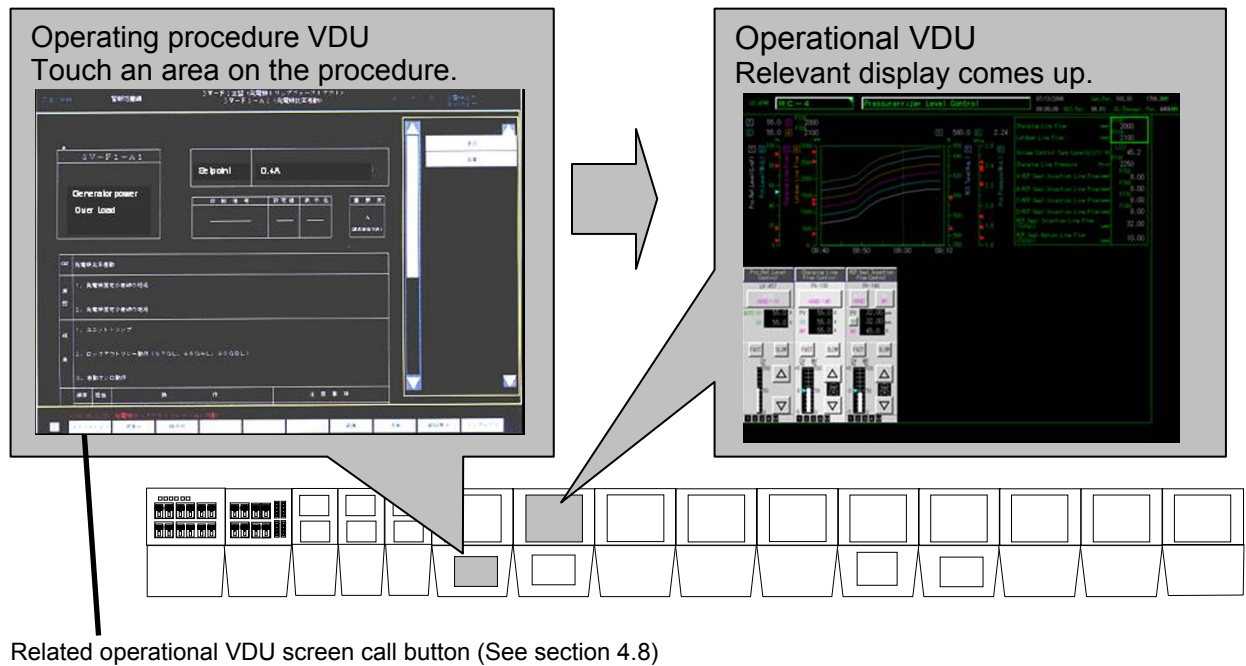


Figure 4.4-4 Screen Request Methods (Operating procedure VDU)

4.5 Operational VDU Display Design

4.5.1 Operation Devices

The Operational VDU has the following features:

- The display offers easy monitoring, taking into consideration the guidance in NUREG-0700 Rev.2, Sections 1.5.1 and 1.5.2.
- The size of the display on the Operational VDU is approximately 19 inches, which takes into account the quantity of displayed information and the size of displayed symbols and characters.
- The display is of the flat type, which makes it easy to hit the target area and minimizes glare.

4.5.2 Operation Method

This section describes the soft operation methods used in the screen-based main control board.

Soft operations are performed by requesting a system on the diagram screen and then touching or clicking an operation area of a soft switch displayed on the screen.

a. Calling Up Switches

- ON/OFF Switches;
On the Operational VDU, by touching or clicking the symbol of the device on a system flow diagram, the ON/OFF switch pops up on the screen. There is only one switch popup on the screen at any one time in order to avoid erroneous operation. The default popped up position is fixed (right-lower side) and if the related information is hidden by the popup window, the default popup position is automatically set in the other corner of the screen. The popup window can be moved by the operator in the unusual case that other information relevant to the operation may be hidden.

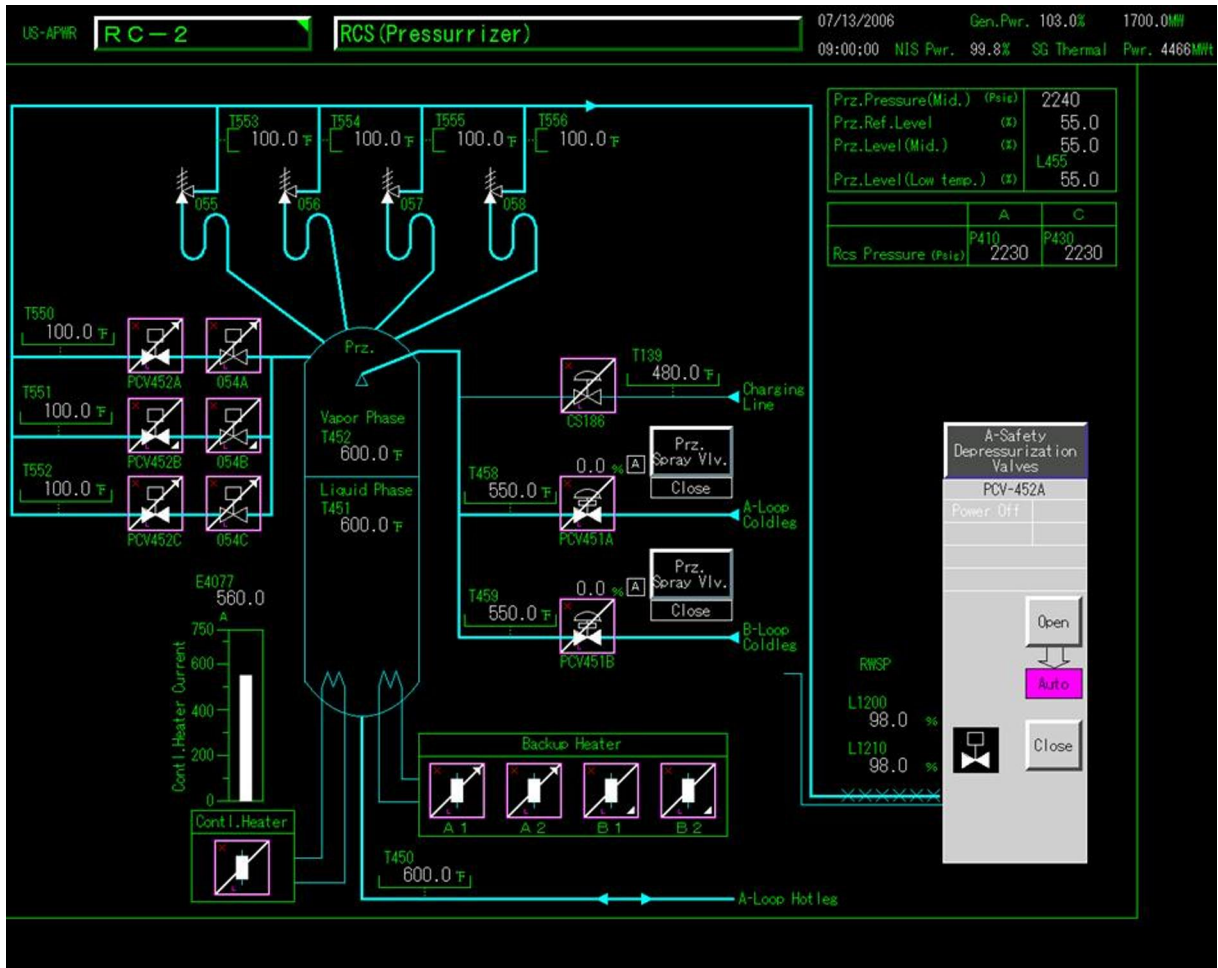


Figure 4.5-1 Example of ON/OFF Switch Popup

b. Controller and Mode Selector

In general, controllers and mode selectors are only available in fixed positions on a Controller screen that displays trend graphs and related parameters, since controlled processes require monitoring of their changing trends.

However, some controllers which are used in a manner similar to ON-OFF switches are available on the system display because they are operable without the need to see a trend. Controllers have a setpoint adjustment function and a manual demand adjustment function. These types of continuous control functions are usually difficult to utilize due to the digital system processing delay. However, in the MHI HSI system these functions are easily used based on the following methods. (See also Section 4.5-3 b.)

- **Target point indicator:** To avoid the stress, confusion and overshoot often caused by typical manual demand feedback indication delay, the HSI system accepts the demand signal, displays the target point in the manual value bar immediately (within one second) and sends the target value to the controller. A discrepancy between the demanded value and the value in the controller is easily seen by the operator. (See Figure 4.5-7)

- **Adopting a slow speed adjustment mode:** In addition to conventional adjustment mode (Normal/Fast), a slow speed mode is applied in order to modulate the setpoint correctly with the expected digital signal delay environment.
- **Adopting the soft numeric keypad for setting the setpoint:** In addition to control setpoint adjustment utilizing increasing/decreasing buttons, the setpoint can be directly input using the numeric keypad function. The HSI system then sends the target setpoint value to the controller. A discrepancy between the demanded value and the value in the controller is easily seen by the operator on controller screen. (See Figure 4.5-2 and Figure 4.5-7)
- **Auto/Manual Transfer:** A bumpless bidirectional auto/manual transfer function is installed in the controller to avoid the instability resulting from an auto/manual transition.

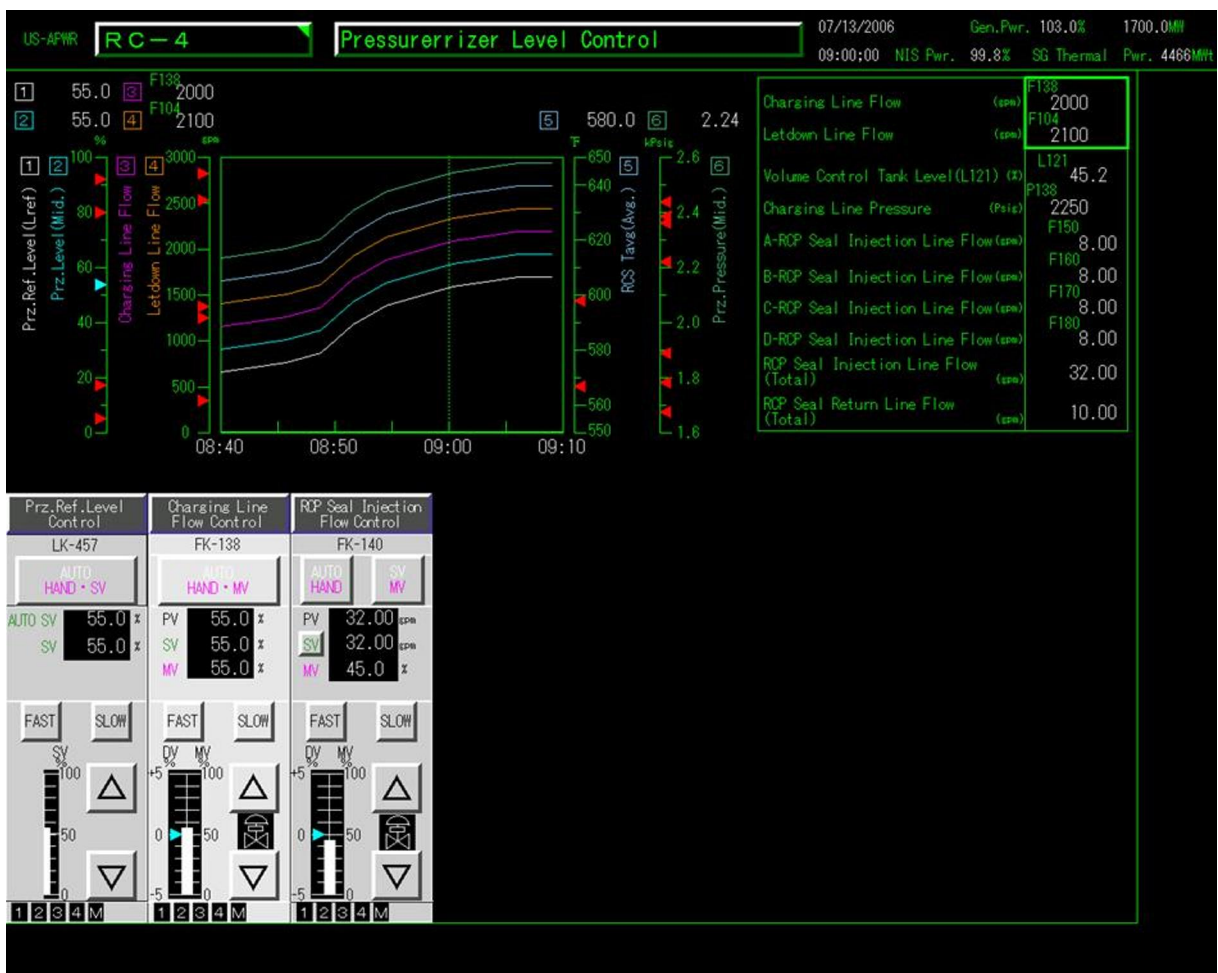


Figure 4.5-2 Example of Controller Screen

c. Displaying Screens Related to Soft Operations

•Identifying soft Operation Areas

All soft operation areas on the screen appear as convex buttons, allowing operators to distinguish operable components/valves (components/valves which respond to touch or click)

from non-operable devices. All soft operation buttons are used for the soft switches and the soft controllers. The select buttons for the soft switches and the soft controllers are located in a graphic area which is distinguished by the display select area. (See Figure 4.4-1)

•Soft Operation Feedback

Soft operation areas appear concave when continually pressed (during input), thereby providing local feedback indicating touch or click input acceptance. Controller feedback related to operation process is indicated by the color of the background on the soft operation area.

4.5.3 Switch Features

a. ON/OFF Switches Operation Related Information Display Feature

Operation related information messages which correspond to lamp information in conventional switches (e.g., control power status, operation availability status, etc.) are displayed using software switches. In addition, these messages can be viewed and acknowledged on system flow diagram screens without requiring the operator to request the control switch display. Component/valve status is also displayed on the soft switch using contact signals (result signals) from component status feedback.

A Switch software cover is an HSI interlock function which requires double action for executing the operation in order to avoid erroneous manipulation. Whenever the soft switch pops up, it is inoperable until the cover is unlocked by touching or clicking on the switch name area.

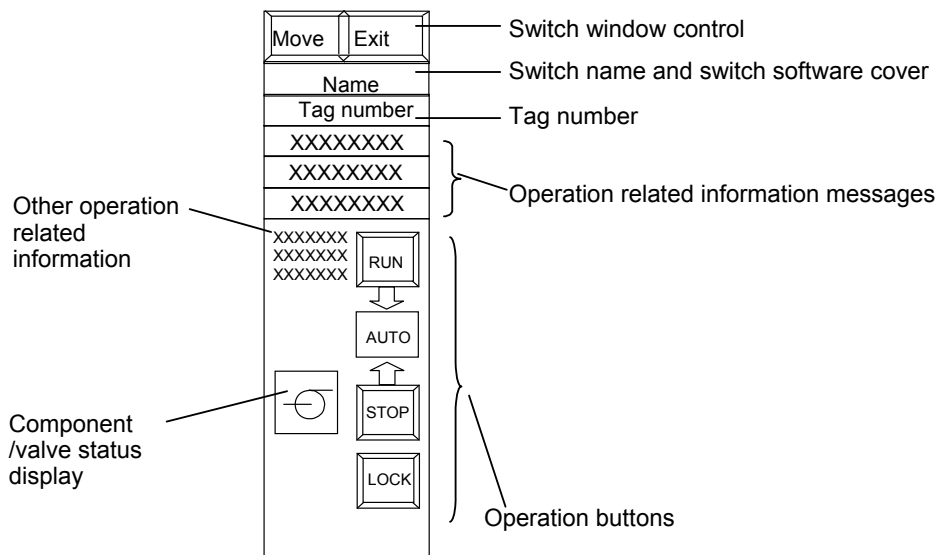


Figure 4.5-3 Example of ON/OFF Switch

Other Operation Related Information Display Features are as follows:

- On the Other Operation Related Information Display Area, the following information is displayed;

- Safety system interlock signal name: The safety system interlock signal name, such as ECCS signal, isolation signals, etc. is displayed for components that are automatically actuated by safety system signals. The display shows the signal name.
- Inching:
“Inching” appears on switches, allowing operators to distinguish inching valves from ON/OFF valves. “Inching” corresponds to valves that have throttling or bumping capability.
- Fail position : “FO”(Fail to Open), “FC”(Fail to Close)
- Lock status : “LO”(Locked Open), “LC”(Locked Closed); which means the valve status is mechanically locked (Full Open or Full Close) by a local gear chain, etc.,

Standard controls, indications and alarms for each component type (e.g. motor operated valve, solenoid valve, switchgear operated components, etc.) are defined in the Component Control and Monitoring Circuit Basic Design Guide (Reference 43).

- Soft Operation Switch Moving Feature:
The function allows operators to move the position of the popup window to the four corners of screen in case the necessary information was hidden behind a switch popup display. Touching or clicking the function, the soft switch moves to each successive corner of the screen. (See Figure 4.5-4)

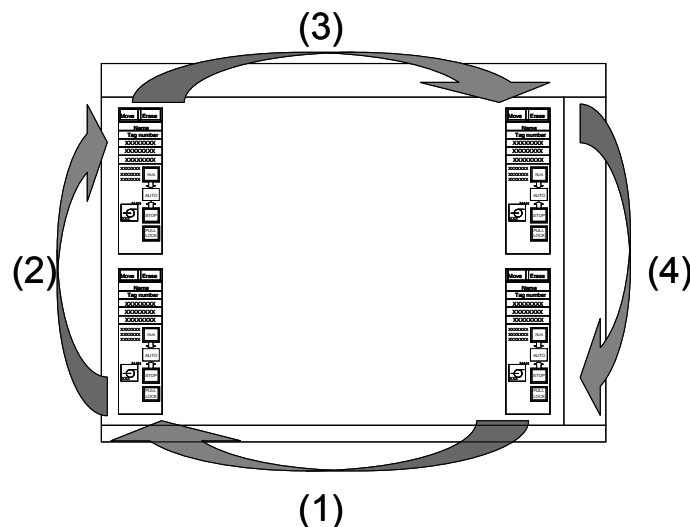


Figure 4.5-4 Soft Operation Switch Moving Feature

- Soft Operation Switch Clearing Feature;

The EXIT function enables the soft switch to be cleared off the screen. The soft switch is also cleared when another soft switch is selected on the screen.

- Tagging Feature:

For maintenance related work order management, operators are able to attach and remove tags by soft operations and the system is able to indicate the tag status by the addition of checkmarks on the applicable component/valve symbol both on the soft operation switch popup window and on the switch selection button on the Operational VDU screen. The tag type is identifiable by the color of the checkmark. Detailed tag information is displayed in a dedicated popup window. The dedicated popup window is popped up with the soft operation switch popup window touching or clicking the switch selection button.

Tagging is an administrative status function that has no effect on the operability of the component.

The tagging system provides soft electronic tags for the HSI system and physical tags for plant components. The electronic tag ID for the HSI system and the physical tag ID for plant components are identical for each component. Electronic tags are implemented within the HSI system and physical tags are attached at each component in local areas of the plant.

The tagging sequence is as follows:

- 1) Isolation and tagging data (electronic tags) and physical tags are prepared by the maintenance/operations crew.
- 2) Electronic tag data is manually uploaded to the HSI system and available to be set on tagging on the dedicated tag popup window. This status shows the icon of the component with a dotted line marked.
- 3) After setting on tagging on the tag popup window, the status change shows the icon of the component with a line.
- 4) At certain stages of maintenance, the maintenance/operations crew touches the icon and pops up the dedicated tag window for changing the tag status. Another tag status change shows a line color of the icon of the effective component. The tag status is updated appropriately for various stages of maintenance. At the local area, the physical tags are attached at components to indicate their maintenance mode.
- 5) After the maintenance is complete, the maintenance/operations crew touches the "Remove" icon on the tag popup window, and then the component icon is unmarked on the system displays. At the local area, the physical tags are removed.

Equipment Name : A-Safety Depressurization Valves
Tag No. : PCV-452A

Erase

Status	Maintenance No. Isol.Restoration No.	Isol.Tag No.	Work Group	Schedule	Charge Group	Charge	Request	Transfer	Management	Position
XXXX XXXX	XXXXXXXXXX XXXXXXXXXX	XXXX XXXX	XXXX XXXX	XXXX/XX/XX XXXX/XX/XX	XXXX XXXX	XXXX XXXX	XXXX XXXX	XXXX XXXX	XXXX XXXX	Auto

△

▽

Tag

Remove

Figure 4.5-5 Tag Popup Window

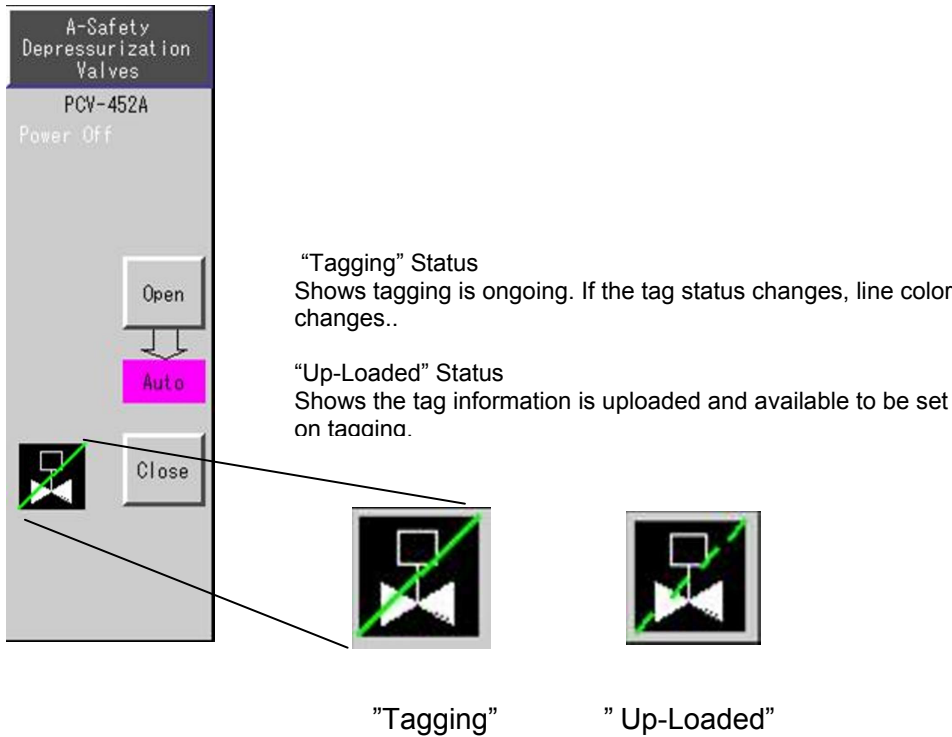


Figure 4.5-6 Example of Tag Status Display

System screens display component status, the component’s acronym name/tag name, representative operation Information messages and tagging information.

b. Manual Operation of controller Information Display Feature

Manual Operation of a controller has the following features;

- The controller is provided with an AUTO/MANUAL button, an INC/DEC button to input MV (Manipulated value) and SV (Setpoint value), a slow/normal/fast mode button and an SV value direct digital value feature.
- Target Parameter Display Feature:
This feature displays PV (Process value), SV, and MV in digital values.

- Normal/Fast/Slow Mode Selection Feature:
The Normal and Fast mode increase/decrease rates are comparable to that of conventional HSI devices.
To accommodate software operation based fine-tuning, the controller is provided with slow mode in addition to the above two modes, offering 1/10th of the increase/decrease rate of normal mode. "Fast" and "Slow" modes are selected by touching or clicking the "Fast" and "Slow" button respectively. The Normal mode is selected by selecting neither the "Fast" mode nor the "Slow" mode. The "Fast" and "Slow" modes are resumed by touching or clicking the "Fast" and "Slow" button again, respectively.
- Target point indicator Feature:
To avoid MV indication delay from the controller, the HSI system displays the operation demand immediately (within one second)

On the system display, control valve status is represented with the position limit, tag name. The representative operation Information messages are also displayed.

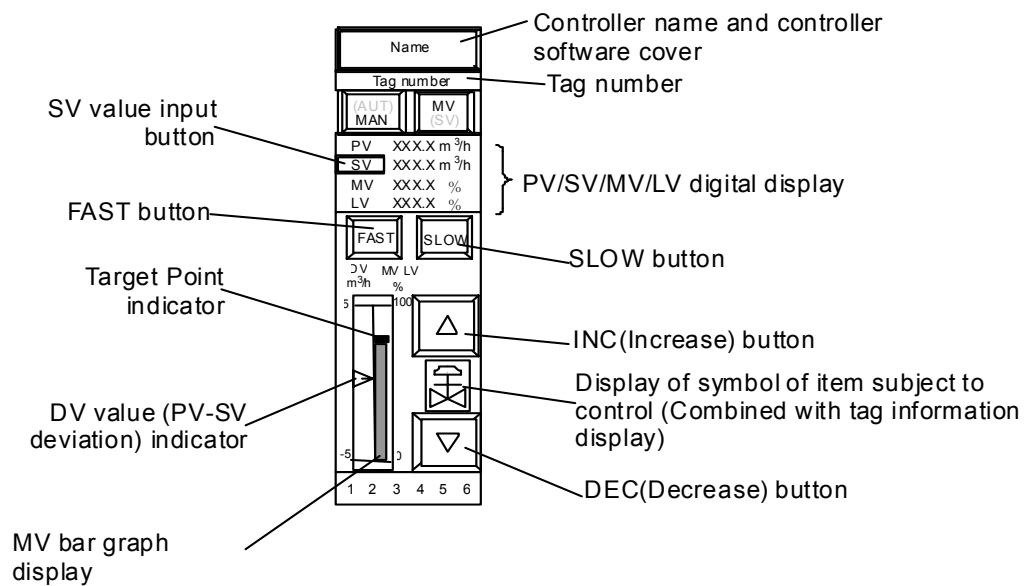


Figure 4.5-7 Example of Controller

Standard controls, indications and alarms for cascaded control functions, and controllers with additional features such as rate of change controls, are defined in the Component Control and Monitoring Circuit Basic Design Guide (Reference 43).

c. Provisions to Prevent Erroneous Operation

Provisions to prevent the erroneous operation of switches and controllers are as follows:

- Soft operation switch (including soft operation touch area) dimensions, shape, identification method, and arrangement are established based on ergonomic design standards.
- A software cover (a feature which blocks miss-touch input) is provided for all touch operation switches and controllers. The switch becomes operable when the software cover is removed by touching or clicking the name area of the switch. It becomes inoperable by touching or clicking the name area again.
- The operation method and function of conventional switches and controllers are covered and integrated on the soft switch. The feature and function of all switches and controllers are designed consistently.
- In cascaded controller (i.e., pressurizer pressure control and boron concentration control, etc.), operators can adjust the target value using the master controller which makes each subcontroller's target accommodated to the main target automatically. The accommodated target value created by the master controller is automatically set on the subcontroller at the auto mode and displayed as an auto-MV indicator value.

4.6 Safety VDU Display Design

4.6.1 Operable Devices

The Safety VDU has the following features:

- The display allows easy monitoring, taking into consideration the guidance in NUREG-0700 Rev. 2, Sections 1.5.1 and 1.5.2.
- The size of the display on the Safety VDU is approximately 10 inches.
- The display is of a flat type, which makes it easy to hit the target area and minimizes glare.

During all operating conditions (normal, emergency and degraded HSI), monitoring screens that indicate Type A and B post accident monitoring (PAM) parameters and alerted conditions which requires operator action information are continuously displayed on two trains of multidivisional SDCV Safety VDUs. The SDCV safety VDUs reduces the operator's workload to navigate between displays to monitor critical parameters, and also improves situation awareness of the total plant status.

There are two types of selectable train-based safety VDU screens:

- Train-based selectable screen

One safety VDU for each of four trains (A, B, C and D) can control and monitor all of the safety-related functions, separately for each train. The train based selectable safety VDU includes monitoring and control screens.

-Task-based selectable screen

In the task-based selectable screens, controllers are grouped so that a single screen supports a predefined set of tasks needed to execute emergency operating procedures. Multiple task-based screens are distributed to selectable safety VDUs of each train. The grouping task based controllers together reduces the navigational task burden that would be necessary during EOP execution.

4.6.2 Operational VDUs Connect/Disconnect

4.6.3 Bypass Permissive





Figure 4.6-1 Screen Transition of Request Area

4.6.4 Monitor Screen

There are four train-based selectable safety VDUs. Figure 4.6-2 shows the menu on the monitor screen which is typical of each train-based selectable safety VDU. Figure 4.6-3 shows an example of a specific monitor screen. When the number of monitored parameters in the system is less than 16, the remaining area of the screen remains blank.

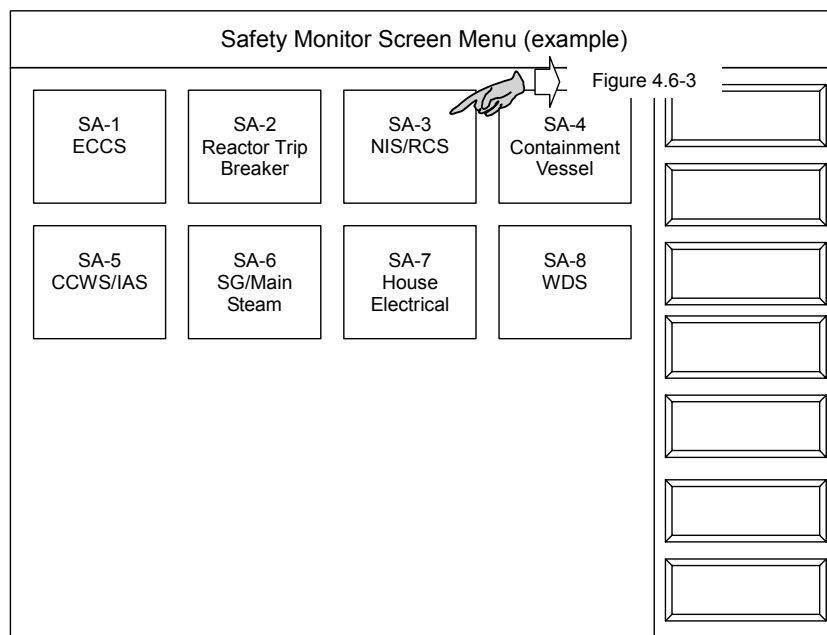


Figure 4.6-2 Monitor Screen Menu

SA-3 NIS/RCS (example of screen title)					
Source Range: Flux(l) (cps)	Parameter name				
$\times 10^*$ 10^0 10^0	Range				
Current Value					

Figure 4.6-3 Example of Specific Monitor Screen

4.6.5 Operation Screen

Figure 4.6-4 shows the menu of the safety operations screen of the train-based selectable safety VDU. Figure 4.6-5 shows the operation component menu of a specific system. When the number of operational components in the system is less than 20, the remaining area in the screen will remain blank. When the number of operational components in the system exceeds 20, the 21st component and beyond will be presented on the next page.

Figure 4.6-6 shows an example of specific operation screen. From this screen, the operator controls the target component. The feature representation of the switch shown on both the safety VDU and the non-Safety VDU (the Operational VDU) is the same.

Safety Operation Screen Menu (example)					
NIS	ICIS Gas	SS		Electrical	
RHRS	RCS-1	RCS-2	MS-1	MS-2	
CSS	CVCS-1	CVCS-2	AFW	MFW	
SFP RSFP	SIS-1	SIS-2	SGBD	CCW	
SWS	CCWS-1	CCWS-2	FIRE CTL		
IAS	H&V (C/V-1)	H&V (C/V-2)			
WDS	H&V (MCR)	H&V (other)	PROT-1	PROT-2	

Figure 4.6-4 Operation Screen Menu

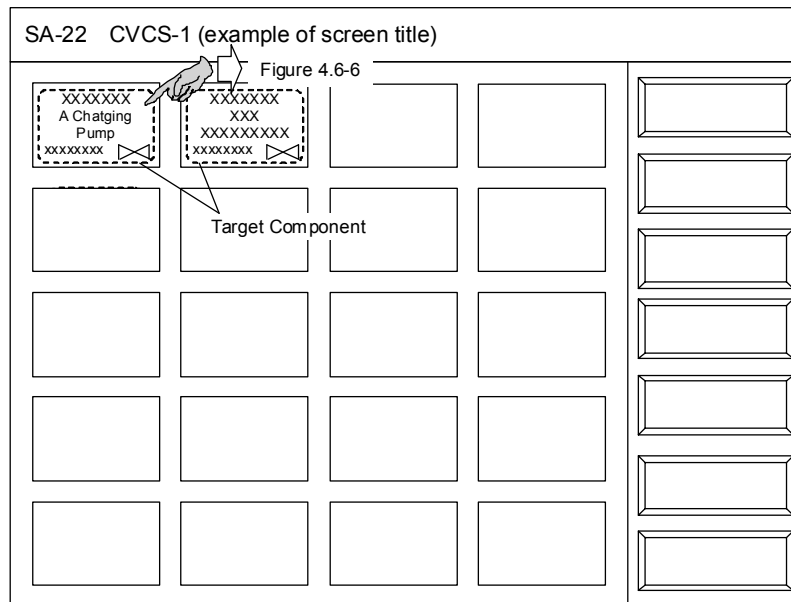


Figure 4.6-5 Operation Component Menu

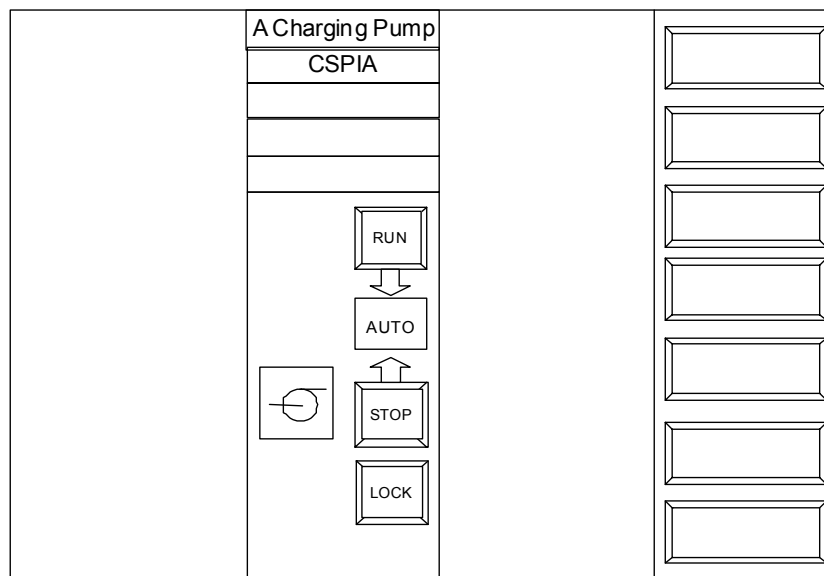


Figure 4.6-6 Example of Specific Operation Screen

4.6.6 Task-based Screen

Multiple task-based screens are distributed to selectable safety VDUs of each train. The task-based screen is designed to provide controls to conduct operation for a set of tasks. The basic hierarchy and specification of the task-based screen is the same as the operation screen. There are three levels of screen hierarchy; task screen menu (Top menu), task component menu and operation screen. In the button area of the task component menu screen, the status of each component is displayed. (See Figure 4.6-4, 4.6-5 and 4.6-6 for the screen layout)

4.6.7 Multidivisional Safety VDU Screen

Figure 4.6-7 shows the typical multidivisional safety VDU screen. The parameters for credited manual operator actions are indicated on the multidivisional safety VDUs. In addition to meeting safety display requirements for the PAM variables, these safety VDUs accommodate degraded HSI conditions (i.e., loss of all PCMS VDUs). Indications on the multidivisional safety VDUs are spatially dedicated and continuously visible (SDCV) and include alarm color coding. The multidivisional safety VDUs provide notification of the plant accident condition to the operator under all plant conditions, This information is especially useful in case of loss of the operational VDUs (non-safety VDUs in the PCMS)

Screen title				
Parameter 1	XXX.X	XXX.X	XXX.X	XXX.X
Parameter 2	XXX.X	XXX.X	■ XXX.X	XXX.X
Parameter 3	XXX.X	XXX.X	XXX.X	XXX.X
Parameter 4	XXX.X	XXX.X	XXX.X	XXX.X
Parameter 5	XXX.X	■ XXX.X	XXX.X	XXX.X
Parameter 6	XXX.X	XXX.X	XXX.X	XXX.X
Parameter 7	XXX.X	XXX.X	XXX.X	XXX.X
Parameter 8	■ XXX.X	XXX.X	XXX.X	XXX.X
Isolation Valves	Open	Close	Close	Close
SIS Pumps	Start	Start	Stop	Stop
Alarm Status 1	ON	OFF	OFF	OFF
Alarm Status 2	OFF	ON	OFF	OFF

Figure 4.6-7 Typical Multidivisional Safety VDU Screen

4.7 Alarm System

The alarm system provides all information necessary for detecting abnormal plant conditions. The alarm system ensures that the operator can easily recognize the fault conditions even when the number of fault conditions or the severity of the faults is increasing.

The main features of the alarm system are as follows:

- adequate information presentation that allows the operator to acknowledge and recognize alarm information and take appropriate corrective actions
- establishment of an alarm prioritization system that allows the operator to identify the relevant and important alarm information and not to deal with “alarm avalanche”.
- Implementation of a navigation system display that provides easy access from the alarm display to the relevant system display and the alarm response procedures.

These functions help the operator to identify and diagnose the transient condition causing the alarms and complete the necessary corrective actions.

4.7.1 Alarm Display System

a. Display Location

All alarm information is displayed on the alarm VDU, LDP and the Operational VDU.

On the alarm VDU, all alarms are categorized into four system categories (i.e., two primary systems, a turbine system and an electrical system). Alarms are recorded in each category display area in chronological order using color coding, blinking coding and audible tones.

On the LDP, all alarms are grouped in each system (i.e., reactor coolant system (RCS), residual heat removal (RHR), etc.) and these grouped alarms are located in the fixed position area of the LDP representing as the alarm tiles (system labels). (See Figure 4.9-6) The grouped alarm tiles (system labels) are also blinking and color-coded when the new alarm occurs. Primary parameter labels and component labels are also used for the individual alarm indications related with the parameters and components. These are also blinking and color coded when a new alarm related to the parameter or the component occurs.

Alarms are also shown in graphic displays on the Operational VDU representing the related parameter's numerical value with red color and switch information (i.e., trip, power-off, etc.).

There are four alarm states – new, acknowledged, cleared, reset (normal).

- New - The operator becomes aware of a new alarm by the blinking display and audible tone, and recognizes the new alarm information in the alarm VDU display.
- Acknowledged -The operator confirms (acknowledge) the new alarm by touching the new alarm display area (blinking area), which stops blinking on the Alarm VDU. Then the operator can call up the related alarm procedure display on the Operation Procedure VDU and the related operational display on the Operational VDU directly by touching or clicking the alarm message display area (See (2) in Figure 4.7-1) on the Alarm VDU in order to diagnose and take actions smoothly. Acknowledged alarms are identifiable by continuous color indications.
- Cleared - When alarm conditions return to normal the alarm is displayed as cleared. Cleared alarms are identifiable by low speed blinking and white color indications.

- Reset - Cleared alarms are manually reset by operator acknowledgement. Reset alarms are identifiable by turning to normal indication (i.e., no-indication on the Alarm display and normal color (gray color) on LDP).

b. Allocation of roles between the Alarm VDU and the Large Display Panel

The LDP provides grouped alarms in the upper area of the fixed screen. And the related individual alarms are located near the primary parameter indications in the fixed display area. This approach ensures an effective identification of the plant emergency state and the overall system status. Individual alarms are displayed on the alarm VDU display utilizing the location information on the LDP as follows:

Four division display areas on the Alarm VDU are located in accordance with the location of the system mimic information in the fixed position area in LDP. Therefore, the left two primary systems on the Alarm VDU are the primary systems outside the CV (Containment Vessel) (all primary systems except those described next) and Reactor/NSSS systems (i.e., RV, RCS, SG, MS, FWS), respectively. And to the right, the next two areas are turbine system and electrical system. (See Figure 4.7-1 and the layout of the fixed display area on LDP in Section 4.7.2) Therefore, the operator can easily make a transition from becoming aware of the new alarm occurrence on the LDP to identifying the new alarm information on the alarm VDU.

In addition, the operator acknowledges the new alarm by touching the alarm acknowledgment button which will stop blinking and ringing of the alarm VDU. The acknowledgement button only affects alarms that are visible to the operator. If there are multiple alarm pages, each page must be acknowledged separately.

To easily identify the most important alarms, multiple screens are provided to display the dynamic alarm prioritization logic. The most important alarms at that time remain in the highest prioritized alarm (Priority Level 1) display which is color-coded as red. Less important alarms at that time and cleared alarms are moved to the other lower priority alarm (Priority Level 2 or 3) screens which are color-coded as yellow and green (see section 4.7.2). The cleared alarm screen is color-coded as white.

(1)																	
(2)	Primary(1) X/X		Primary(2) X/X		Secondary X/X		Electrical X/X										
(3)	xx/xx/xx xx:xx:xx OK 1	RHR Flow Low	xx/xx/xx xx:xx:xx OK 1	Pzr Press Low													
			xx/xx/xx xx:xx:xx NO 1	SG Level Low													
(4)	Related	Alarm Group						Page Select				Alarm Control					
	Operat. Proc.	FO Alarm	Alarm	3	Caution	15	Status	50	Alarm Cleared	15	1/4	2/4	3/4	4/4	New	FO Acknow.	Acknow.

- (1) First-out Alarms display area
Each first-out alarm of "ECCS Actuation", "Reactor Trip", "Turbine Trip" and "Generator Trip" is displayed.
- (2) Alarm title area
"Primary (1)"; Primary systems outside the CV (all primary systems except "Primary (2)")
"Primary (2)"; Reactor/NSSS systems (i.e., RV, RCS, SG, MS, FWS)
"Secondary"; Turbine system
"Electrical"; electrical and transmission system
- (3) Alarm message display area
All individual alarm messages are displayed in the four system categories with its occurrence date/ time and static prioritization levels.
- (4) Alarm acknowledgement/reset and screen request buttons area
Related; Alternative switch for related display selection between Operational display and Operation procedure display
Alarm Group; Alternative switches for prioritization alarm display selection, "First out alarm", "Alarm (Priority 1 alarm display)", "Caution (Priority 2 alarm display)", "Status (Priority 3 alarm display)" and "Alarm Cleared (Cleared alarm display)"
Page Select; Alternative switches for multiple alarm page selection which displays 15 messages x 4 categories alarms in one page.
Alarm Control; Alarm acknowledge buttons for First out alarm and other alarms which can make all alarm displayed on the current page acknowledged by each alarm page and each prioritization alarm page.
Alarm sound stop button which can make the alarm sound stopped to reduce operator's stress. Blinking still remains so that unacknowledged alarms are identifiable.

Figure 4.7-1 Alarm VDU Screen Specifications

4.7.2 Alarm Prioritization

a. Prioritization Based on Specific Importance (Static Prioritization)

Many alarms are statically prioritized by importance based on plant impact including release of radioactive materials and the demand for operator action. The static priorities have six levels. Table 4.7-1 shows the static prioritization category. The prioritization levels are displayed on an alarm message area on the Alarm VDU.

b. Prioritization Based on Dynamic Prioritization (Dynamic Prioritization)

The priority of other alarms is dynamically determined by alarm processing logic which focuses on the relationship between each issued alarm based on physical relationships such as the plant process and equipment status. Based on that dynamic determination, each alarm is prioritized at the given moment to its importance. The dynamic priorities have three levels. The prioritizations for all alarms are as follows:

- Priority Level 1 (alarm information; Need actions)
- Priority Level 2 (caution status information ; Need acknowledgment but no need for actions)
- Priority Level 3 (status information ; No need for actions nor acknowledgement)

The dynamic prioritization rules are simple, consistent and do not depend on the plant specific mode. In the dynamic prioritization, there are three rules:

- Higher prioritization rule: For multiple-setpoint alarms, lower importance alarms are regarded as status information when higher priority alarms are activated. For example, Figure 4.7-2 shows the tank level alarm which has multiple setpoints.(i.e., Low and Low-Low) In this case, the Low alarm is displayed as Priority 1 (alarm information) until the tank level achieves to the Low-Low alarm setpoint. When the level achieves the Low-Low alarm setpoint, the Low-Low alarm is displayed as Priority 1 and the Low alarm is changed to Priority 3 (status information).
- Cause-consequence rule (Component level): For those alarms which have a relationship between "result" and "cause", the "result" alarm is regarded as status information when the "cause" alarm is activated. For example, Figure 4.7-2 shows the illustration of the fluid system. Normally the outlet pressure low alarm is Priority 1. However, whenever the pump is tripped the outlet pressure low alarm will also occur. Therefore, the low pressure alarm ("result" alarm) is regarded as Priority 3 (status information) when the pump is stopped by the interlock alarm (i.e., "cause" alarm) which is displayed as Priority 1 (alarm information).
- Mode rule: This is the Cause-consequence rule at the system level. For example, Figure 4.7-2 shows the charging pump trip alarms. Normally charging pump trip alarms are Priority 1. However, charging pump trips are regarded as Priority 3 (status information) when the pumps are stopped by an SI signal (i.e., "cause" alarm), which is displayed as Priority 1 (alarm information).

If a Priority Level 3 alarm is used for an interlock and the status of the component relevant to the interlock is not monitored by the alarm system, it must be regarded as a Priority Level 2 alarm. For example, "Pressurizer level deviation high from setpoint" alarm is initially Priority 1. It would normally turns to Priority 3 when the "Pressurizer level high alarm" occurs. However,

since the level deviation alarm controls the backup heater it is downgraded only to Priority 2. This prompts the operator to confirm the actuation of the backup heater.

Table 4.7-1 Static Alarm Priority

Priority	Primary System		Ventilation System		Turbine & Electrical Systems	
	Type	Contents	Type	Interim	Type	Interim
I	ECCS Actuation	Alarms related with ECCS, C/V isolation signals	Safety System Activate	Ventilation isolation alarm of MCR	-	-
II	Reactor Trip	First out Alarms	-	-	Turbine Generator Trip	First out Alarms / Blackout
III	Caution for ECCS Actuation	1 Malfunction alarms of ECCS actuation 2 Manual actuation alarms after ECCS actuation	Same as the Primary system	Same as the Primary system	Same as the Primary system	Electric power supply about ECCS
IV	Caution for Reactor Trip	1 Causing alarms of reactor trip 2 Manual actuation alarms about protective 3 Primary component's alarms	-	-	Turbine Generator Trip Caution	1 Causing alarms of Turbine and Generator 2 Emergency manual actuation alarms 3 Primary component's alarms
V	Cautions for	Alarms concerning caution system monitoring (including partial trip)				
VI	Operation Management	1 Local operating alarms 2 Alarms concerning plant maintenance 3 Alarms concerning testing				

(High) ← → (Low)

On the Alarm VDU, alarms are distinguished and displayed on each prioritization alarm page. For Priority 1 and 2 alarms, the operator needs to acknowledge new alarms so that when alarms move to Priority 1 and 2 pages, these alarms are blinking and audible on the new page. On the other hand, Priority 3 alarms are not acknowledged because they do not need operator's actions and confirmation. Avoiding new alarm acknowledgment and recognition on the blind pages, the prioritization page select button (i.e., Alarm group area in (4) on Figure 4.7-1) is blinking until all alarms are recognized on each Prioritization alarm page. Alarm prioritization is also identifiable on the LDP representing the Priority color code which is the same as on the Alarm display. Regarding the group alarms, the higher priority color code in the same group is represented. (See section 4.9.3 e.)

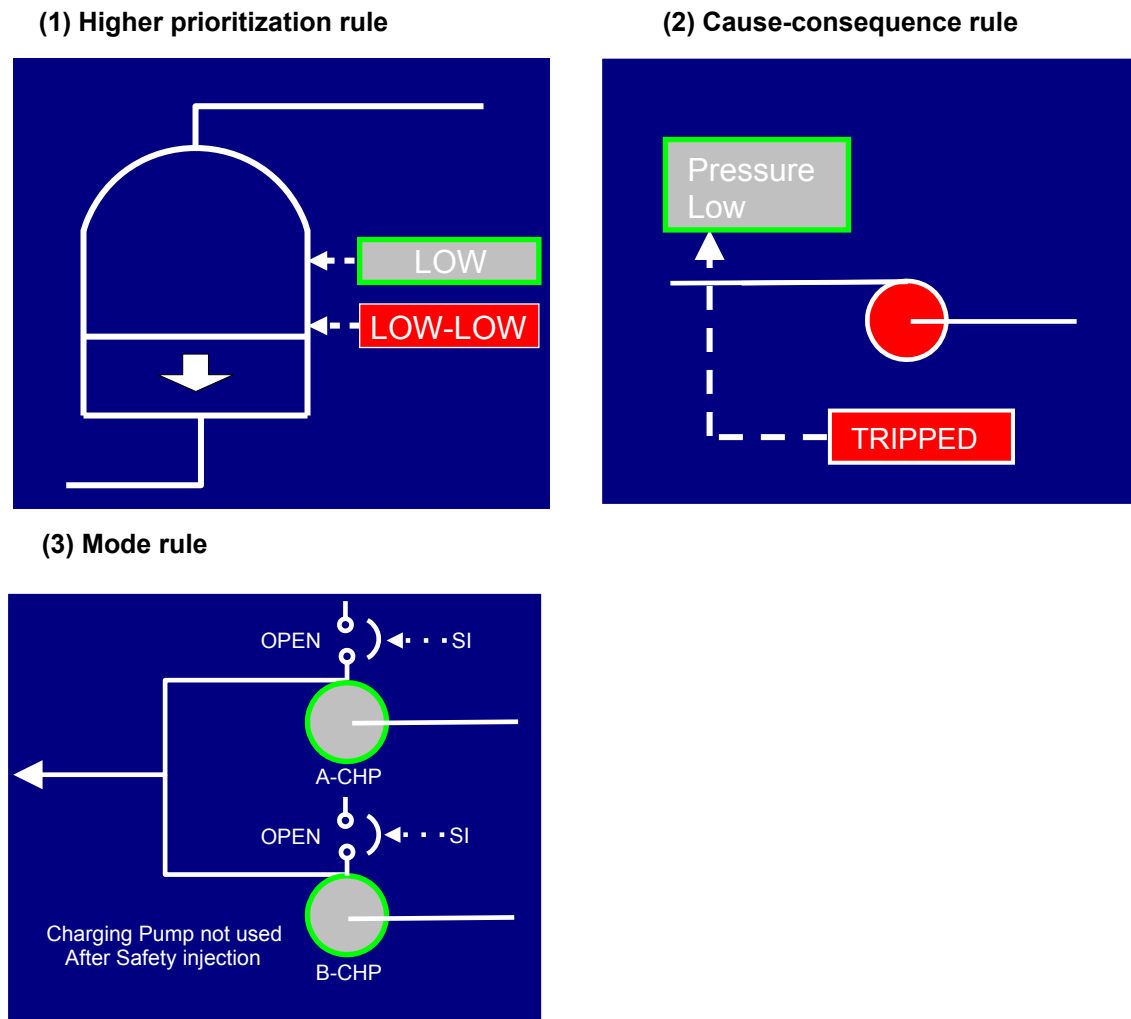


Figure 4.7-2 Dynamic Alarm Prioritization

4.7.3 Coding by Alarm Sound

Alarms are coded by sounds to enable operator identification. Bypass and permissive indicators are also acknowledged by sound and blinking. They are also identifiable from the alarm sounds. The sounds are coded based on their frequencies and repeating cycles. There are no sounds for cleared alarms.

4.7.4 First-out Alarms Displaying

A first out alarm is the first condition to cause a major change in plant state (i.e., reactor trip, turbine trip, generator trip, and ECCS Actuation). First out alarm groups are designated for each separate condition (i.e., reactor trip, turbine trip, generator trip, and ECCS Actuation). The first out alarms for each group is displayed on the Alarm VDU and on the LDP. All alarms after the first out alarm are displayed in time series on a dedicated first-out screen on the alarm VDU.

The first-out alarm is detected by the PSMS processor, turbine protection or hard-wired equipment (Generator trip) with a high time resolution (less than 100 milliseconds).

4.7.5 Acknowledging and Resetting Alarms & Stopping Alarm Sound

‘Acknowledging’ means that the operator identifies and confirms the individual new alarm concretely and ‘Resetting’ means that the operator deletes the cleared alarms. Alarms are acknowledged and reset using alarm acknowledgement and reset buttons provided on the alarm dedicated screen (displayed on the Alarm VDU).

In addition to the acknowledging and resetting, there is an alarm sound stopping function. This function simply stops the sound associated with existing new alarms. Blinking still remains so that unacknowledged alarms are identifiable. The alarm sound is stopped using an alarm sound stop button provided on the Alarm VDU screen and an operator console hardware button. It stops all sounds associated with existing new alarms at the moment. Therefore, sounds are generated for any new alarms that occur after the alarm sound is stopped. If neither the sound stop button nor hardware button are used, then alarm sound stops automatically.

4.7.6 Avoiding Nuisance Alarms

A “Black Board” alarm concept is applied so as to improve operability. Alarm logics distinguish normal conditions that are not alarmed (e.g., low flow when the pump is demanded to be off,) and abnormal conditions which are alarmed (e.g., low flow when the pump is demanded to be on) judging from equipment status and process measurement status.

4.7.7 Link to Related Display

Touching or clicking the alarm message area, the related operational display is selected on the Operational VDU next to the Alarm VDU or the related alarm response procedure is selected on the Operating Procedure VDU in front of the Alarm VDU.

The selection is made by alternative switch located on the Alarm VDU. (See Figure 4.7-1)

4.8 Computer-Based Operating Procedure

Computer-Based Procedures (CBP) are provided on the Operating Procedures VDU. The essential interaction principles are as follows:

- The procedure is structured in accordance and compliant with the textual images, so that it is easy to handle and has the flexibility to incorporate textual modifications. The textual document is also available as a backup of the CBP.
- By requesting operations on the Alarm VDU, alarm response procedures (ARPs) are directly selected on the Operating Procedure VDU which is located in front of the Alarm VDU. (See Figure 4.4-3 and Table 4.4-2)
- In case of emergency, such as plant trip, the operators can request the emergency procedure for reactor trip or ECCS by touching the first-out alarm on the Alarm VDU. Specific accident procedures (e.g., LOCA, SGTR) are requested from the CBP menu screen after the operator identifies the plant status.
- By selecting hyper-links on the Operating Procedures VDU, the related operational VDU display is automatically displayed on the Operational VDU. (See Figure 4.4-4).
- The related soft switch or controller is not requested directly on the Operating Procedures VDU to avoid operator's omission of relevant information (line-up, inlet difference pressure, etc.) confirmation. For example, when the operator is to execute a procedure that requires a valve to be opened, the operator takes the following steps:
 - 1) Select the hyper link on the CBP for the Operational VDU page
 - 2) Select the component to be controlled
 - 3) Select the component switch software cover
 - 4) Select the control action (open/close)
- When the operator completes the current task on the CBP, the operator selects the hyper link concerning the next task on the CBP in order to call up the related operational VDU page without closing the current windows or pages.

A Commercial off the shelf (COTS) platform and a generic format (PDF, MS Word, HTML, etc.) are used for the operation procedure system. This approach enables lower cost for utilities' alterations to operating procedures. The development process is as follows:

- 1) The procedure is manually created or revised using the COTS platform. The procedure includes fields with unique tag identification for links to appropriate Operational VDU screens and links to other procedures.
- 2) The procedure is manually reviewed and approved through appropriate plant administrative quality assurance (QA) procedures.
- 3) The approved procedure is compiled using automated CBP tools to integrate into the digital HSI system. The CBP tools are developed using a design process that includes Verification and Validation, and Configuration Management. This process is equivalent to the design process used for the PCMS.
- 4) A series of manual checks are performed to ensure the CBP tool has compiled with the procedure correctly. Since the automated CBP tool has been previously verified, these

manual checks include samples of procedure steps and hyperlinks. Complete manual verification is not required.

- 5) The new CBP software, which includes the newly compiled procedure, is maintained under Configuration Management.
- 6) Backup paper procedures in case of the degraded HSI conditions to be described in Section 4.11 will be easily accessed from storage facilities in the MCR and RSR.

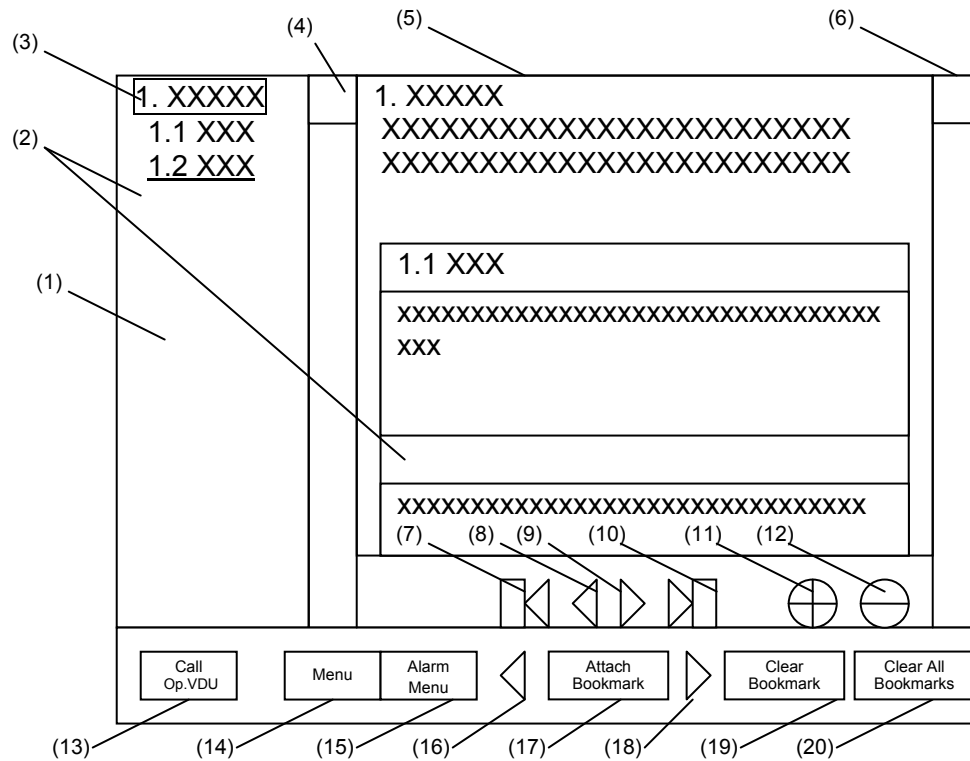
The design of the computer-based procedures complies with the criteria of DI&C ISG-05 (ML072540140), as follows:

General Review Criteria:

1. The computer-based procedure system is designed as an integral part of the US Basic HSIS for the Main Control Room.
2. The CBP system ensures the procedure user (e.g., operators) is always in control of the procedure system, since bookmarks can be entered only by the user and only the user can initiate page or procedure selection. Other aspects of criteria 2 are not applicable to the US Basic HSIS, because there is no control or information automation in the CBP system.
3. The configuration controls within the design and the procedure modification process ensure the computer-based procedure system always presents the most recently approved and issued version of a procedure.
4. V&V activities ensure that the computer-based procedure system always displays the selected procedure. Failure to display a procedure is easily recognized and prompts the operator to utilize backup HSI.
5. The computer-based procedure system allows the operator to easily move from one procedure to another at any time through the use of multiple procedure VDUs and multiple procedure windows within each VDU.

Backup Procedures Review Criteria:

6. Back-up paper procedures are maintained for continued operation under degraded HSI conditions (i.e. loss of non-safety VDUs), and accident mitigation and/or safe shutdown under degraded HSI conditions (i.e. loss of non-safety VDUs or CCF affecting all VDUs), and accident management . .
7. Backup paper procedures are easily accessible in the MCR. Paper procedures are used under all conditions at the RSR, TSC and EOF; these procedures are easily accessible in these locations.
8. The computer-based procedures and backup paper procedures are generated from the same original COTS computer files. All are under the same configuration controls.
9. The ability of operators to quickly, easily and effectively access to backup procedures is confirmed through formal V&V activities, which include tests of the fully integrated HSI using dynamic high fidelity full scope simulation.
10. With the exception of bookmarks and navigational controls (e.g. hyperlinks), computer-based procedures look identical to backup paper procedures, such that the operator can use them equally effectively.
11. Computer-based procedures and backup paper procedures are generated from the same source file to ensure that the contents are the same.



Note: See table 4.8-1 for specifications of CBP icons, (1)-(20)

Figure 4.8-1 Computer-based Operating Procedure

Table 4.8-1 Specifications of Operating Procedure VDU icons

No.	Type	Color/icon Color/letter	Shape	Function
(1)	Index window	White Black	Rectangle	Index of the selected procedure. Link to top of each chapter or section at (5) by touching or clicking chapter or section title.
(2)	Bookmark	White Blue	Underline	By touching or clicking certain chapter/section title or paragraph, then touching or clicking (17), a bookmark is attached. The letters change to blue and underlined.
(3)	Selected procedure in procedure steps	-	Rectangle Frame	Selected procedure (chapter, section or page) in the procedure steps displayed on (5).
(4)	Scroll bar	Light Gray	Rectangle	Scroll window (1).
(5)	Procedure Window	White Black	Rectangle	Display procedure page, including text, figure table, etc.
(6)	Scroll bar	Light Gray	Rectangle	Scroll window (6).
(7)	Page control	Light Gray Blue	Triangle	Go to previous chapter.(Also available by touching or clicking previous chapter on (1))
(8)	Page control	Light Gray Blue	Triangle	Go to previous page.
(9)	Page control	Light Gray Blue	Triangle	Go to next page.
(10)	Page control	Light Gray Blue	Triangle	Go to next chapter. (Also available by touching or clicking next chapter on (1))
(11)	Page control	White Blue	Circle	Zoom in.
(12)	Page control	White Blue	Rectangle	Zoom out.
(13)	Call operational VDU	Dark Grey White	Rectangle	Call up the related screen on the Operational VDU. Repeat to touch or click, to call other screens, grouped as the "related screen" to the page, current displayed on CBP.
(14)	Menu	Dark Grey White	Rectangle	Select a procedure from procedure list. (e.g., Reactor Operation, Turbine Operation, Accident Operation)

Table 4.8-1 Specifications of Operating Procedure VDU icons (continued)

No.	Type	Color/icon Color/letter	Shape	Function
(15)	Alarm menu	Dark Grey White	Rectangle	Same as select "Alarm Response Procedure" (ARP) at (14), prepared to approach quickly. Procedures for "First out alarms" (plant trip, ECCS activation) are included in the ARP.
(16)	Bookmark control	Dark Grey White	Rectangle	Go to previous bookmark.
(17)	Bookmark control	Dark Grey White	Rectangle	Attach a bookmark. (See (2))
(18)	Bookmark control	Dark Grey White	Rectangle	Go to next bookmark.
(19)	Bookmark control	Dark Grey White	Rectangle	Clear the bookmark.
(20)	Bookmark control	Dark Grey White	Rectangle	Clear all bookmarks.

Note: Generic control functions, such as "Open the window", "Close the window", "Save", "Load" are supported by the commercial off the shelf platforms and not included in the Figure 4.8-1 and table 4.8-1.

4.9 Large Display Panel

4.9.1 Purpose of Large Display Panel Installation

The purposes of the LDP are the following:

- To provide continuously visible information to the plant operator in order to ensure that the operator has all relevant plant information.
- To make plant information simultaneously available to all plant operating staff on duty and to support operator team activities

4.9.2 Large Display Panel Screen Display Features

The large display panel for the US-APWR has four 100-inch diagonal screens. The sizes and locations of these screens may vary for operating plants based on physical limitations of the MCR. For example, if 100-inch screens cannot be accommodated, smaller screens can be duplicated in multiple MCR locations to ensure readability by all operators. The actual sizes and locations for operating plants will be described in the Plant Licensing Documentation.

4.9.2.1 Fixed Display Area

The fixed display area displays the same information at all times. The following section explains how that information supports plant operation during various plant conditions.

- During Normal Operation
The fixed display area displays the main plant parameters required for monitoring the plant status during normal operation, enabling quick error detection. It also displays the main plant parameters required for monitoring the plant status during power fluctuation and parameters that may cause a plant trip. The fixed display area simplifies verification of performance of main plant systems during normal operation.
- In the Event of a Plant Trip
In the event of a plant trip, the fixed display area displays information required for verification of trip status information related to the reactor, turbine and generator immediately following a plant trip, thereby simplifying the trip status verification process.
- In the Event of an ESFAS Actuation:
In the event of an ESFAS actuation, the fixed display area displays the engineered safety features components status and process values indicating system performance, thereby simplifying verification of the safety injection operation status (See section 4.10).
- During Accident Response (Status Identification)
At the time of an accident, the fixed display area displays the main plant parameters required for plant status identification (Type A and B parameters of R.G.1.97), thereby simplifying status identification when an accident occurs.
- In the Event of an Alarm
In the event of an alarm, the fixed display area displays grouped alarms, thereby simplifying detection.
- Safety system bypass or inoperable state indication (BISI) is continuously visible on the fixed display area based on the principles of design and industry guidelines (IEEE-603-1991, R.G. 1.46, IEEE-497, etc.).

Table 4.9-1 shows the typical parameters mentioned above and Figure 4.9-1 shows the typical layout for the LDP.

For key parameters indicating the status of critical power production functions and critical safety functions, the LDP presents numerical values and trend arrows. The trend arrow distinguishes direction of the trend (up or down) and the rate of change (slow or fast). The trend arrows enhance situation awareness by allowing operators to quickly detect changing process conditions without needing to read changing numerical values.

4.9.2.2 Variable Display Area

The variable display area shows detailed plant information and trend displays on the operational VDU display, thereby supplementing the information provided in the fixed display area and facilitating retrieval of plant information. The contents of the variable display area can be selected from the operator console and from the supervisor console, thereby helping the operating staff's common awareness and communication. The variable display area can also automatically display pre-selected screens. Manual and automatic screen selections are described below.

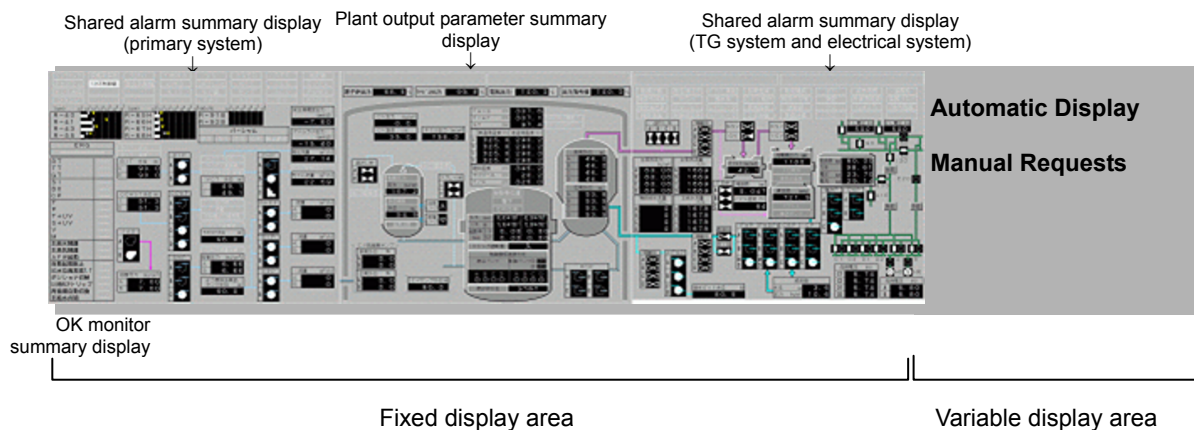


Figure 4.9-1 Large Display Panel Specifications (Overall)

a. Automatic Display

The variable LDP screen can be automatically selected based on the following trigger signals:

- First Out Alarm – The screen that is automatically selected is relevant to the First Out alarm condition. This screen helps the operator diagnose the condition that lead to the plant disturbance.
- Permissive signal activated/deactivated – The screen that is automatically selected is relevant to the specific Permissive/Bypass function.

The automatic display function can be blocked by the operator.

b. Manual Request

The ability to manually select displays for the variable display area on the LDP requires that the operational VDU be available, since it features a request menu button on each screen. The function of the menu button is as follows:

1) Transmission menu

The transmission menu button is set as a function key on each operational VDU screen. When the transmission menu button of the screen currently displayed on the operational VDU is pushed, the current screen is displayed on the variable display portion of the LDP. Even if the display screen of the operational VDU changes after the transmission menu button is pushed, the display screen in the LDP variable display is not changed.

2) Connection menu

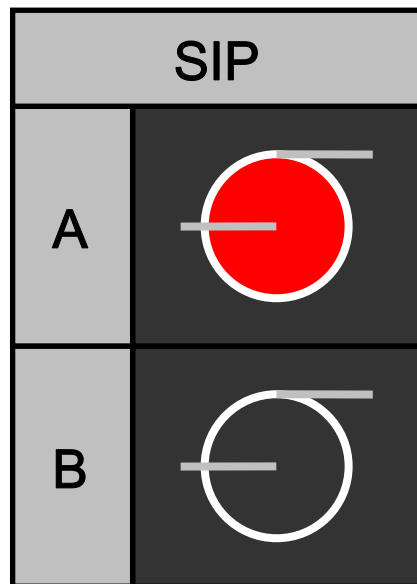
The connection menu button is set as a function key on an operational VDU screen. By turning on the connection menu button, the variable LDP screen is automatically requested to be the same as the operational VDU screen requesting it. When different screens are selected on the operational VDU, these same screens are displayed on the LDP.

There is no priority between the manual selection commands from operational VDUs used by the RO, SS or STA. Therefore the last requested screen is displayed. In addition, if the automatic display function is not blocked, when an automatic display trigger signal comes, the variable portion of the LDP changes to an automatic display screen.

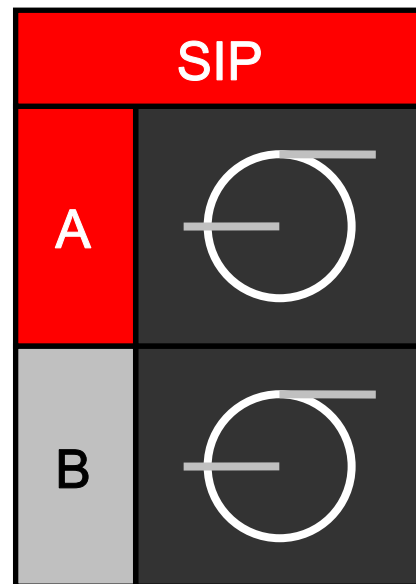
4.9.3 Alarm Display on the Large Display Panel

a. Flow Sheet Image

The LDP uses equipment symbols to display alarms when conditions arise that affect the particular equipment. For example, a pump trip alarm is displayed by having the pump icon flicker.



A-SIP trip
(A-SIP icon turns red)



A-SIP AOP bearing oil pressure low-low
(“A” and “SIP” frames turn red)

Figure 4.9-2 LDP Component Alarm Status Display

b. Abbreviation of Alarm Name

Although an alarm is displayed by using the symbol and parameter name label of the equipment and the alarm name, if the equipment's name is contained in an alarm name and the recognition of the affected equipment is not difficult, the equipment name is omitted. The design intent is for the alarm display on the LDP not to become complicated or unclear by excessive display of the alarm identification information.

c. Message Slot System

For alarms related to the same parameter (e.g., high, high-high, low, low-low) the alarm display on the LDP includes dynamic display areas instead of separate window tiles as is typical on conventional control boards. The dynamic display area shows the highest priority alarm condition.

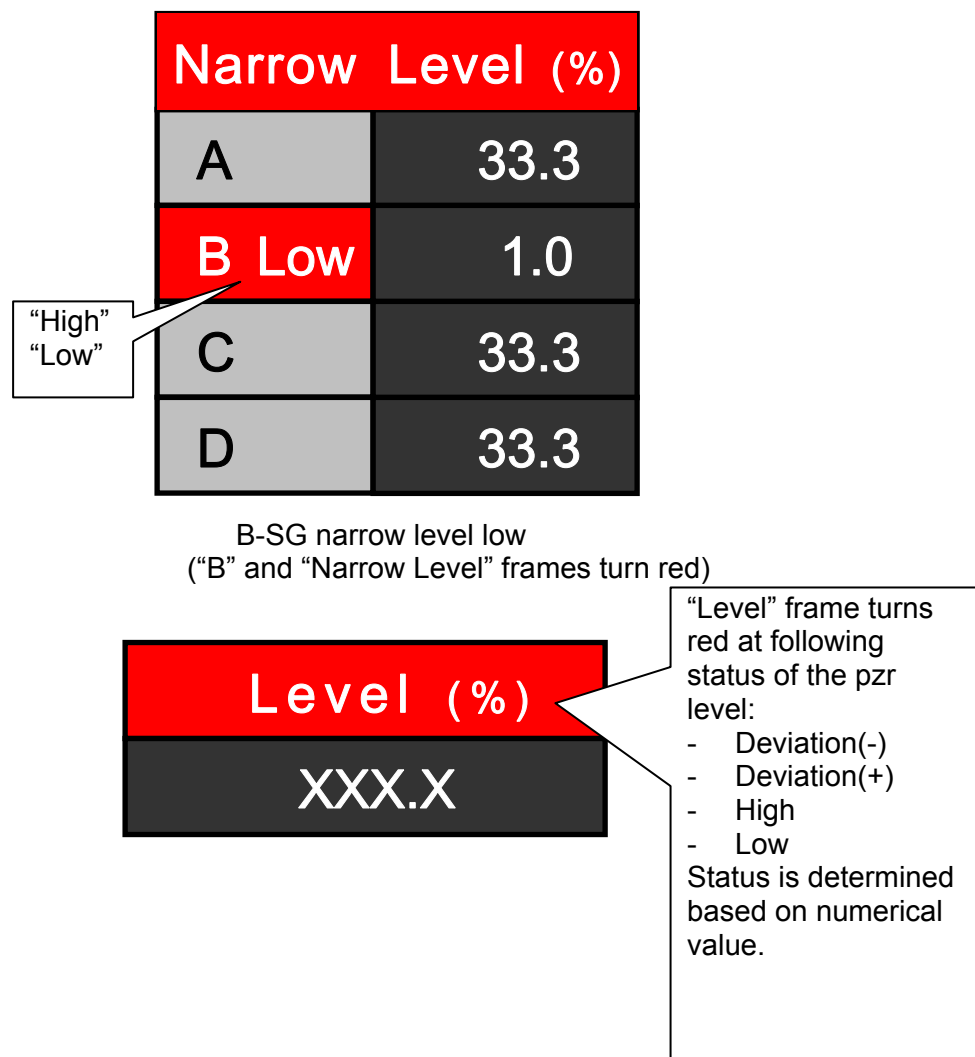


Figure 4.9-3 LDP Process Parameter Alarm Status Display (1/2)

Narrow Level (%)	
A	XX.X
B (+)	XX.X
C (L)	XX.X
D	XX.X

"Narrow Level" frame turns red at following status of each SG level:

- High-High
- High
- Deviation(-) (Level>Set point)
- Deviation(+) (Level<Set point)
- Low

Identification letter displays the status.

B-SG level deviation (+)(Level<Set point) together with C-SG level low

Figure 4.9-4 LDP Process Parameter Alarm Status Display (2/2)

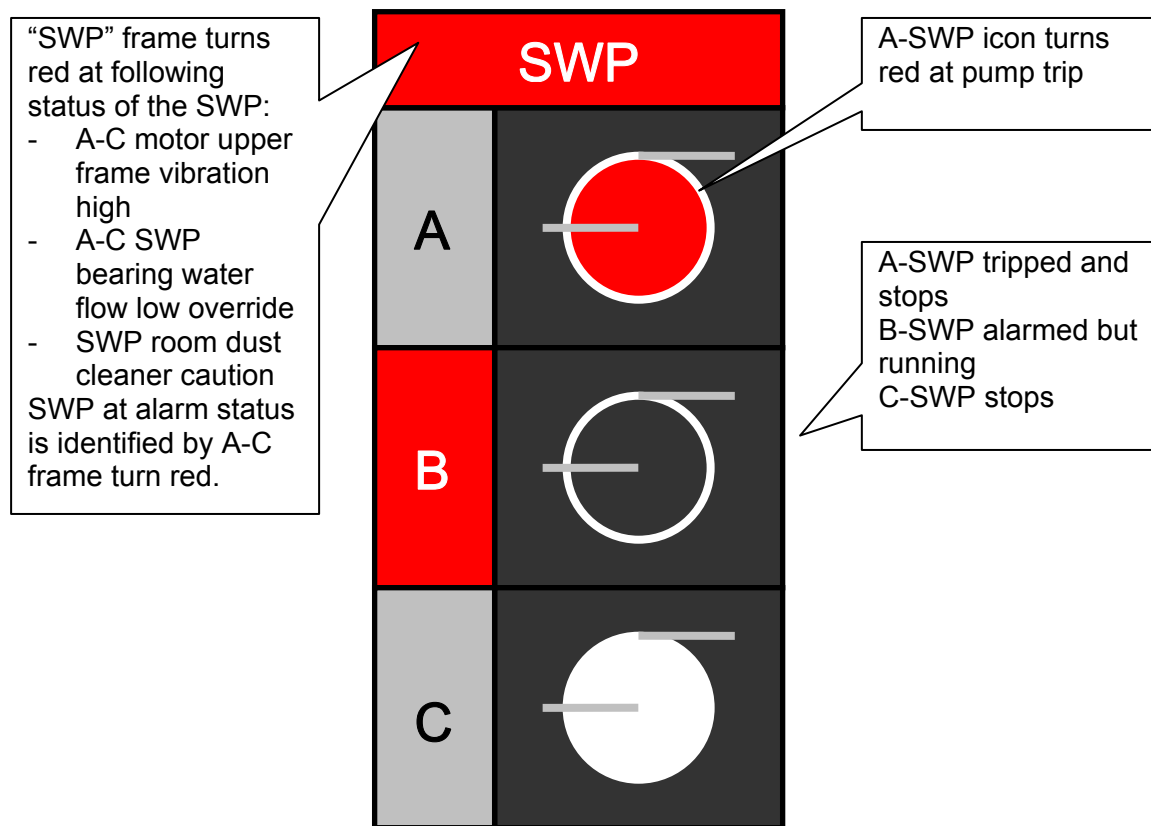
d. First-out Alarm

In order that a first out alarm may show directly the initiation of a nuclear reactor trip signal, an ECCS signal, etc., alarm sharing is not performed because performing such sharing could cause identification and corresponding operation to be difficult. However, the LDP fixes for every first out the display of the first hit alarm. Checks are also made on the alarm VDU screen after second hits. Each first out alarm for "ECCS Actuation"/Reactor Trip"/Turbine Trip"/Generator Trip" is arranged in the topmost part of the Large Display Panel screen. Each first out alarm indicates as a message in the message display area for each first out alarms (message slot) rather than in window tile form like a conventional control board.

e. Shared Alarms

Certain alarms are basically shared for every parameter state. However, the alarm of a multi-level alarm displays the state and provides a display location which is commonly used for every parameter. ("Water Level Low" ->"Water Level High" if a state changes, the message will change)

The shared alarm represents the highest priority color code of the individual dynamic prioritization alarms involved in each shared alarm display frame. Whenever a new alarm occurs, the shared alarm display area blinks with sound and may change the priority color if a new alarm is higher dynamic priority alarm. If all individual alarms in the shared display frame are cleared, then the display color turns white with low blinking. If all individual alarms in the shared display frame are reset by touching or clicking the reset button on the Alarm display, then the shared display area turns normal background color.



A-Service Water Pump trip together with B motor upper frame vibration high

Figure 4.9-5 LDP Shared Alarm Status Display

f. SDCV Alarms and OK Monitor

The following alarms are displayed on the fixed section of the LDP (i.e., the display format is SDCV):

- alarms relevant to PAM parameters (Pressurizer Level Low, CV Pressure High, etc.)
- alarms demanding urgent responses (SG Level Low/High, etc.)
- alarms used for identification of major events (Radiation monitoring system (RMS) monitor High, Alarms related LBB, etc.)
- alarms important for overall supervision of plant status (Pressurizer Press Low, etc.)
- alarms from automatically checking actuation results for demands from the RPS and ESFAS. This is referred to as the “OK Monitor”. (See section 4.10.2)
- alarms from automatically checking the operability of ESF plant components. This is referred to as the “Bypassed or Inoperable Status Monitor” (See section 4.10.4)
- alarms from automatically checking the critical safety function status tree logic. This is referred to as the “Critical Safety Function Monitor” (See section 4.10.3)
- alarms resulting from one-out-of-N channels actuating in the RPS or ESFAS. This is referred to as the “Partial Trip Monitor” (See section 4.10.5).

The automatic checking results of the actuations for events are also displayed as SDCV features as “OK Monitor”. (See section 4.10.2)

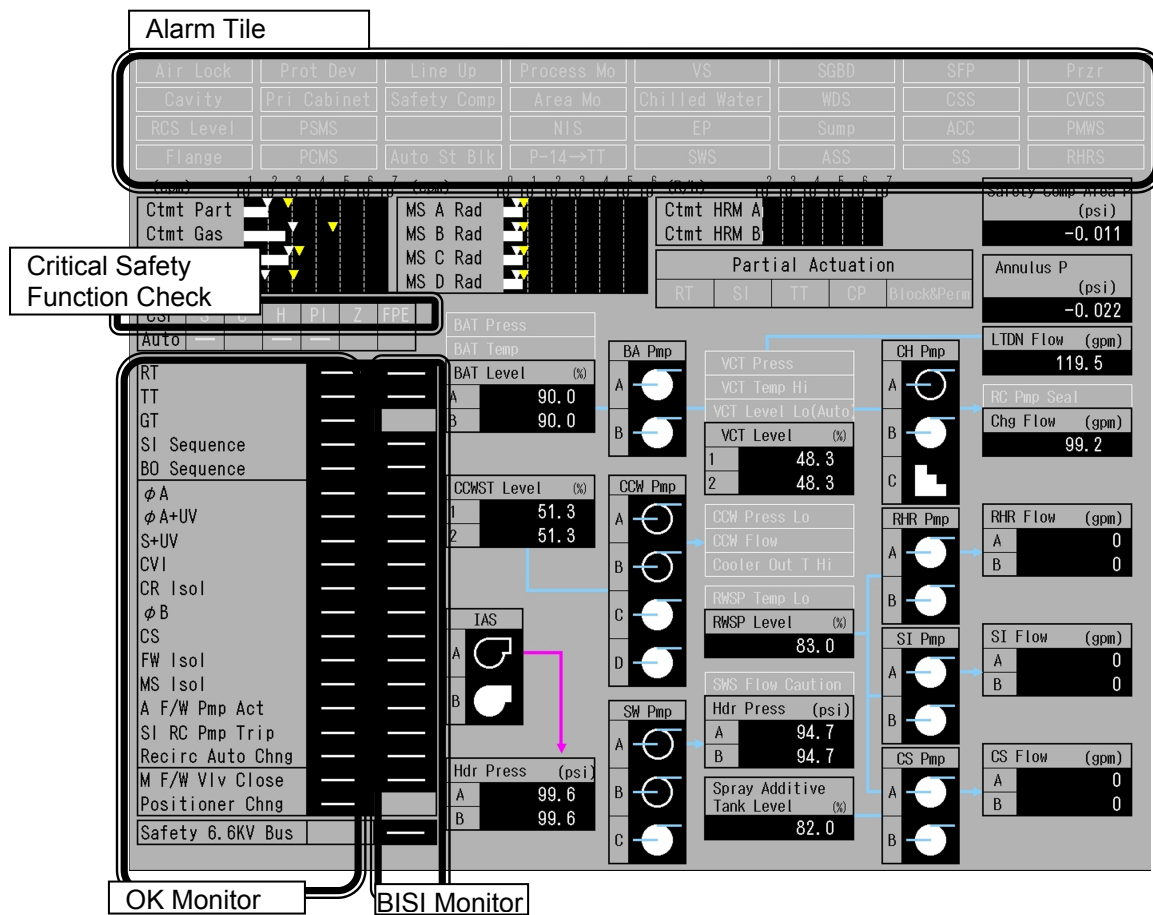
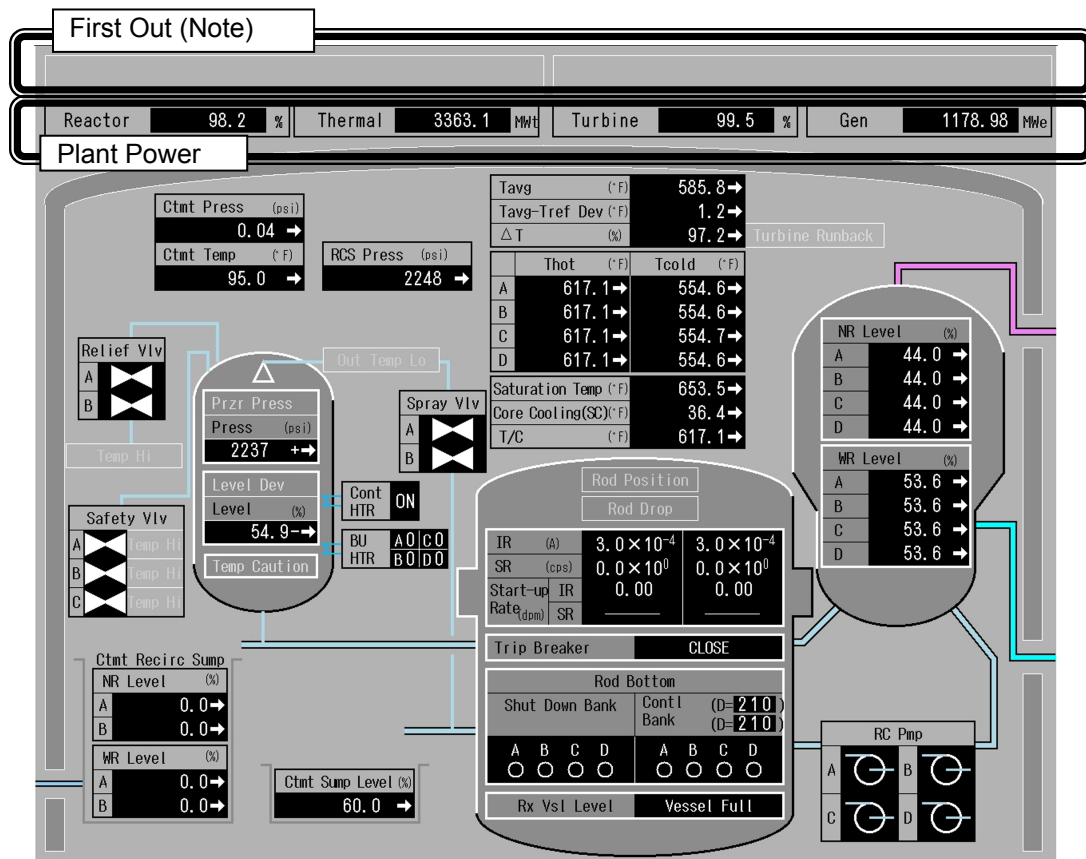


Figure 4.9-6 Large Display Panel Specifications (Left Wing)



Note:

PSMS tag the "First Out" when reactor (generator, turbine) trip or ECCS signal transmits for the first time. Although other trip or ECCS signals follow it and transmit at the same cycle of data bus, HSI systems read the tag and display the "First Out".

Figure 4.9-7 Large Display Panel Specifications (Center Wing)

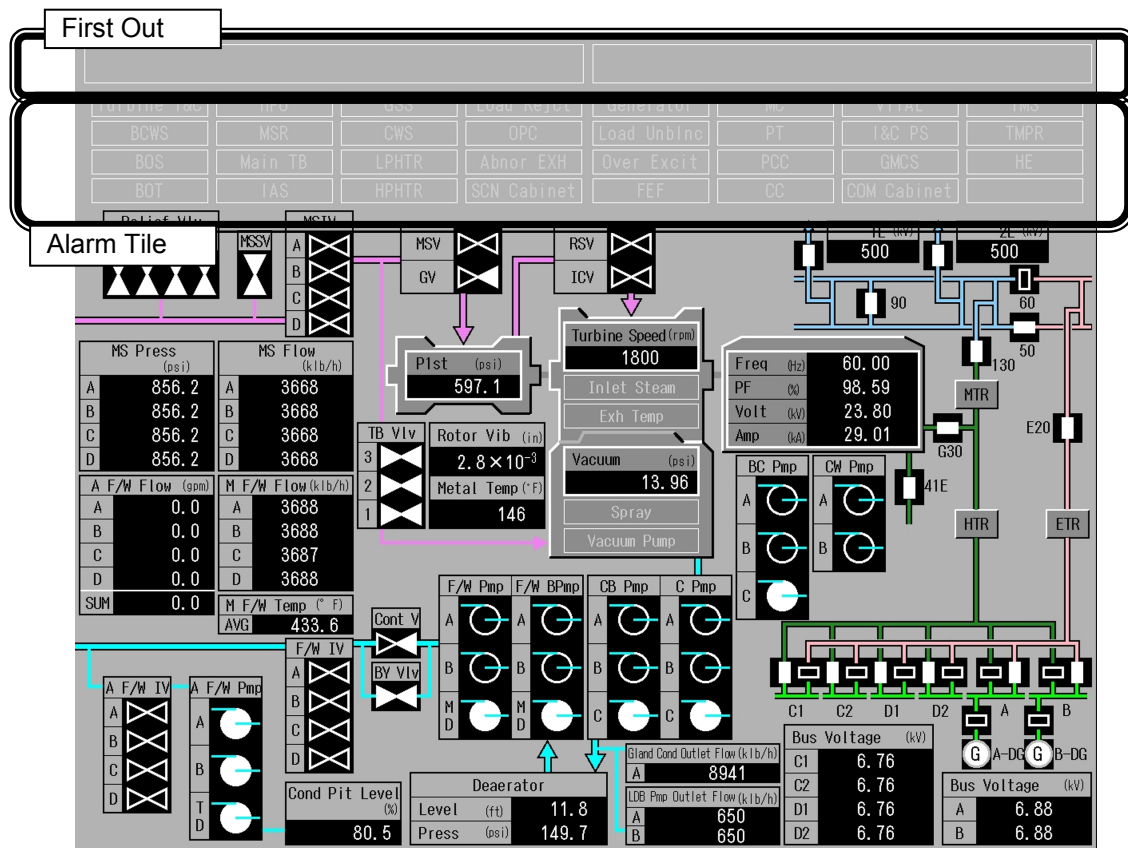


Figure 4.9-8 Large Display Panel Specifications (Right Wing)

Table 4.9-1 Parameters on LDP

	Plant Power	Cause of Reactor Trip	Plant Trip	ESFAS Actuation	PAM	SDCV Alarm	OK Monitor
Reactor Thermal Power	X						
Turbine Power	X						
Generator Power	X						
Nuclear Instrumentation System (NIS) Power	X	X			X		
Pressurizer Pressure	X	X			X	X	
Pressurizer Water Level	X	X			X	X	
Pressurizer Reference Water Level	X						
RCS Average Temperature	X	X					
RCS Reference Temperature	X	X					
RCS Delta-Temperature	X	X					
RCS Hot Leg Temperature (Wide Range)					X		
RCS Cold Leg Temperature (Wide Range)					X		
RCS Subcooling (Loop)					X		
RCS Subcooling (T/C)					X		
Core Outlet Temperature					X		
RCS Pressure					X	X	
Power Range Neutron Flux	X	X					
Intermediate Range Neutron Flux	X	X	X	X	X		
Source Range Neutron Flux	X	X	X	X	X	X	
Intermediate Range Neutron Flux Change Rate		X	X	X			
Source Range Neutron Flux Change Rate		X	X	X			
SG Water Level (Narrow Range)	X	X			X	X	
SG Water Level (Wide Range)					X		
SG Reference Water Level	X	X					
Main Steam Pressure	X	X			X	X	

Table 4.9-1 Parameters on LDP (continued)

	Plant Power	Cause of Reactor Trip	Plant Trip	ESFAS	Actuation	PAM	SDCV Alarm	OK Monitor
Main Steam Flow	X	X						
Main Feed Water Flow	X	X					X	
Main Steam Tie Line Pressure	X	X						
Main Feed Water Head Pressure	X	X						
Turbine First Stage Pressure	X	X						
Charging Water Flow	X	X						
Letdown Water Flow	X	X						
Boric Acid Tank Water Level						X		
CCW Surge Tank Water Level						X		
Service Water Supply Line Pressure						X		
Containment Pressure						X	X	
Containment Temperature						X		
CV Annulus Pressure						X		
Safety System Component Room Pressure						X		
R/V Water Level						X		
Safety Injection Water Flow						X		
RHR Flow						X		
EFW Flow						X		
CV Spray Cooler Outlet Flow						X		
SFP Water Level						X		
RWSP Water Level								
EFW Pit Water Level						X	X	
CV Sump Water Level						X	X	

Table 4.9-1 Parameters on LDP (continued)

	Plant Power	Cause of Reactor Trip	Plant Trip	ESFAS Actuation	PAM	SDCV Alarm	OK Monitor
CV High Range Radiation Monitor					X		
CV Dust Radiation Monitor					X	X	
CV Gas Radiation Monitor					X	X	
Condenser Ejection Gas Radiation Level					X	X	
SG Blow Down Radiation Monitor					X	X	
Main Steam Radiation Monitor					X	X	
N-16 Main Steam Radiation Level					X	X	
Exhaust Duct Gas Radiation Level					X	X	
Control Room Emergency HVAC System Status					X		
Emergency Power Generator				X			
Reactor Trip Breaker Status		X	X	X	X		X
Control Rod Position	X	X	X		X	X	X
Pressurizer Relief Valve	X	X			X		
Pressurizer Relief Valve Shutdown Valve	X	X			X		
Pressurizer Spray Valve	X	X					
Pressurizer Back Up Heater	X	X			X		
Pressurizer Control Heater	X	X			X		
MFW Control Valve	X	X		X			X
MFW Bypass Control Valve	X	X		X			X
SG Makeup Water Line Valve		X					X
MFW Isolation Valve	X	X		X			X
EFW Isolation Valve				X			X
Turbine Bypass Valve	X	X					
Main Steam Relief Valve	X	X			X		

Table 4.9-1 Parameters on LDP (continued)

	Plant Power	Cause of Reactor Trip	Plant Trip	ESFAS Actuation	PAM	SDCV Alarm	OK Monitor
Main Steam Relief Valve Isolation Valve	X	X			X		
Main Steam Isolation Valve	X	X		X			X
Reactor Coolant Pump	X	X					
Charging Pump	X	X					
Component Cooling Water Pump		X		X			X
Service Water Pump		X		X			X
Safety Injection Pump				X			X
CV Spray/RHR Pump				X			X
Emergency Feedwater Pump				X			X
IA Compressor				X			X
CV Recirculation Fan				X			X
Bearing Cooling Water Pump		X					
Main Stop Valve	X	X	X				
Governor Valve	X	X	X				
Reheat Stop Valve	X	X	X				
Interceptor Valve	X	X	X				
Turbine Rotation Rate	X	X					
Deaerator Pressure	X	X					
Deaerator Tank Water Level	X	X					
Condenser Vacuum	X	X					
Condensate Pump	X	X					
Condensate Booster Pump	X	X					
Circulating Water Pump	X	X					
Power Factor	X	X					

Table 4.9-1 Parameters on LDP (continued)

	Plant Power	Cause of Reactor Trip	Plant Trip	ESFAS Actuation	PAM	SDCV Alarm	OK Monitor
Generator Frequency	X	X					
Generator Voltage	X	X					
Generator Current	X	X					
Turbine Shaft Vibration	X	X					
Feed Water Pump	X	X					
Feed Water Booster Pump	X	X					
Transmission Voltage	X	X		X			
Safety M/C Bus Voltage	X	X		X	X		
Non-Safety M/C Bus Voltage	X	X		X			
Main Trans Circuit Breaker	X	X	X	X			
Generator Load Break Switch	X	X	X				X
Generator Field Circuit Breaker	X	X	X				X
Emergency Trans Circuit Breaker	X			X			X
Emergency Power Generator Circuit Breaker	X	X		X			X
House Trans Power Receive Circuit Breaker		X					X
Safety M/C Bus Power Receive Circuit Breaker	X			X			
Non-Safety M/C Bus Power Receive Circuit Breaker	X			X			
Switching Station Circuit Breaker		X					
Emergency Trans Power Receive Circuit Breaker		X					X
Transmission System Circuit Breaker	X	X		X			X
Safety DC Current C/C Bus Voltage					X		
Reactor Trip Status			X				X
Turbine Trip Status			X				X
Generator Trip Status			X				X

Table 4.9-1 Parameters on LDP (continued)

	Plant Power	Cause of Reactor Trip	Plant Trip	ESFAS Actuation	PAM	SDCV Alarm	OK Monitor
ECCS Status (ECCS Line-Up Valves)				X			X
ECCS Sequence Components				X			X
Black Out Sequence Components				X			X
CV Spray Sequence Components				X			X
Main Control Room Isolation Sequence Components				X			X
CV Isolation Phase A (T Signal) Actuating Valves				X			X
CV Spray Signal Actuating Valves				X			X
CV Isolation Phase B (P Signal) Actuating Valves				X			X
CV Isolation Phase A (T Signal) & Emergency Bus Under Voltage Signal Actuating Valves				X			X
Safety Injection Signal & Emergency Bus Under Voltage Signal Actuating Valves				X			X
CV Ventilation Isolation Signal Actuating Valves				X			X
Main Control Room Ventilation Isolation Signal Actuating Valves				X			X
Automatic Activation Block				X			
Main Steam Bypass Start Up Valve				X			X
EFWP Outlet Flow Control Valve			X				X
EFWP Drive Steam Inlet Valve			X				X
SG Sampling Line CV Outside Isolation Valve				X			X
SG Blow Down CV Outside Isolation Valve				X			X
SG Blow Down Stop Valve				X			X

4.10 Automatic Checking of Actuators

4.10.1 Integration of Monitoring and Operation

Typical actions of plant operators include checking the standby condition of equipment before operation, monitoring operating parameters (direct and relevant parameters) and identifying the plant behavior during operation. In order to improve the operability of the HSI system, all of the manipulation information on each switch (i.e., control power status, operation availability status, etc.) is displayed on an Operational VDU display with the component/valve status. Standard status indications and alarms for each component type (e.g., motor operated valve, solenoid valve, etc.) are defined in the Component Control Basic Design Guide (Reference 43).

4.10.2 Automatic Checking of Actuators for Events

When a significant event like a plant trip occurs, or if an ECCS actuation occurs in case of an emergency, the operator's required actions and the attendant stress increase because the operator must simultaneously carry out many tasks, e.g., the operator must collect the safety-related system information and confirm plant conditions, etc.. In the HSI System, the status of components, valves and breakers, as well as the plant trip signals, ECCS signals and isolation signals are automatically checked and compared against the design conditions stored in the computer. The check results are displayed on the fixed area of the LDP and the Operational VDU as "OK monitor".

The following typical signals are verified:

- Reactor Trip
- Turbine Trip
- Generator Trip
- ECCS Actuation
- Containment vessel isolation phase A (T signal)
- Main steam flow isolation
- Main feedwater isolation
- Emergency feedwater flow isolation
- Actuation of emergency feedwater flow
- Actuation of containment vessel spray
- Containment vessel isolation phase B (P signal)
- Containment vessel HVAC isolation (V signal)
- Main control room HVAC isolation (M signal)
- Charging water flow isolation

Figure 4.10-1 shows how the OK monitor results are displayed on the LDP and operational VDUs. Color coding is used to distinctly display one or multiple trains "Not OK", thereby allowing operators to recognize when a function is not meeting minimum actuation line-up requirements

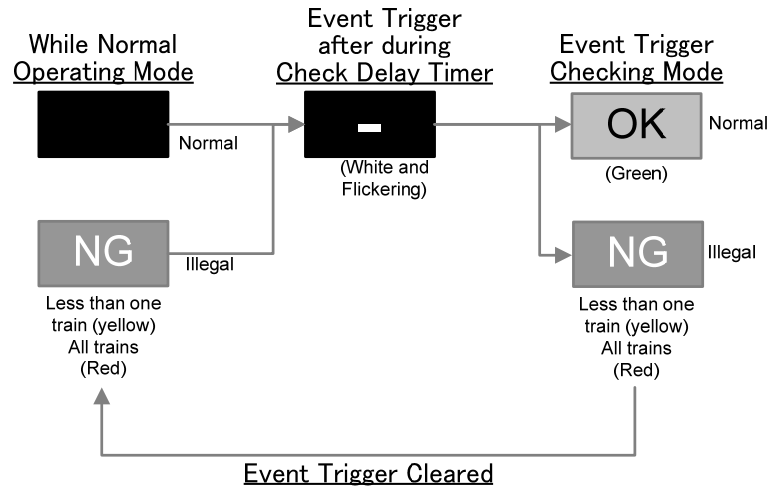


Figure 4.10-1 OK Monitor Display Format

4.10.3 Automatic Verification of Critical Safety Functions

When an event of accidents happens, the Unit Management Computer (UMC) continuously checks the plant conditions and confirms the integrity of the following (typical) Critical Safety Functions (CSF):

- Reactivity Control
- RCS Inventory
- Core Cooling
- Secondary Heat Sink
- RCS Integrity
- Containment Integrity

Note that Radioactivity Control from Supplement 1 to NUREG-0737 is maintained by maintaining all other critical safety functions, including containment integrity. Monitoring and controlling the six critical safety functions, defined above, is consistent with the Emergency Operation Procedures (EOP) of US operating plants and with the EOPs of the US-APWR. All EOPs, including those of the US-APWR, are described in plant licensing documents.

If any of the critical functions are threatened, based on the logic defined in the EOP, a corresponding color coded alarm is displayed on the fixed area of the LDP (see Figure 4.9-6). CSF alarms prompt operators to execute state-oriented accident management procedures.

4.10.4 Bypassed and Inoperable Status Indication (BISI)

The Bypassed or Inoperable Status Indication (BISI) function automatically checks the operability and position status of plant components and displays the results at the system level on the fixed area of the LDP near the OK monitor. Color coding is used to distinctly display one or multiple trains in the bypassed or inoperable condition, thereby allowing operators to recognize when a function is not meeting minimum operability requirements.

4.11 Response to HSI Equipment Failures

The following standard and degraded operating configurations are considered in the HSIS design:

- Standard configuration (no loss of HSI functions)
- Degraded HSI systems by single failure
- Loss of all non-safety HSI
- Loss of all digital non-safety and safety HSI (Common cause failure (CCF))
- Loss of MCR

For each of the operating mode, the means to monitor and control the plant is as follows:

4.11.1 Standard Configuration

The operation of the plant is performed from the MCR whatever the plant status is, provided that the technical and operating criteria for the HSI are met. In this mode, the secondary control means are not allowed to send orders to the process.

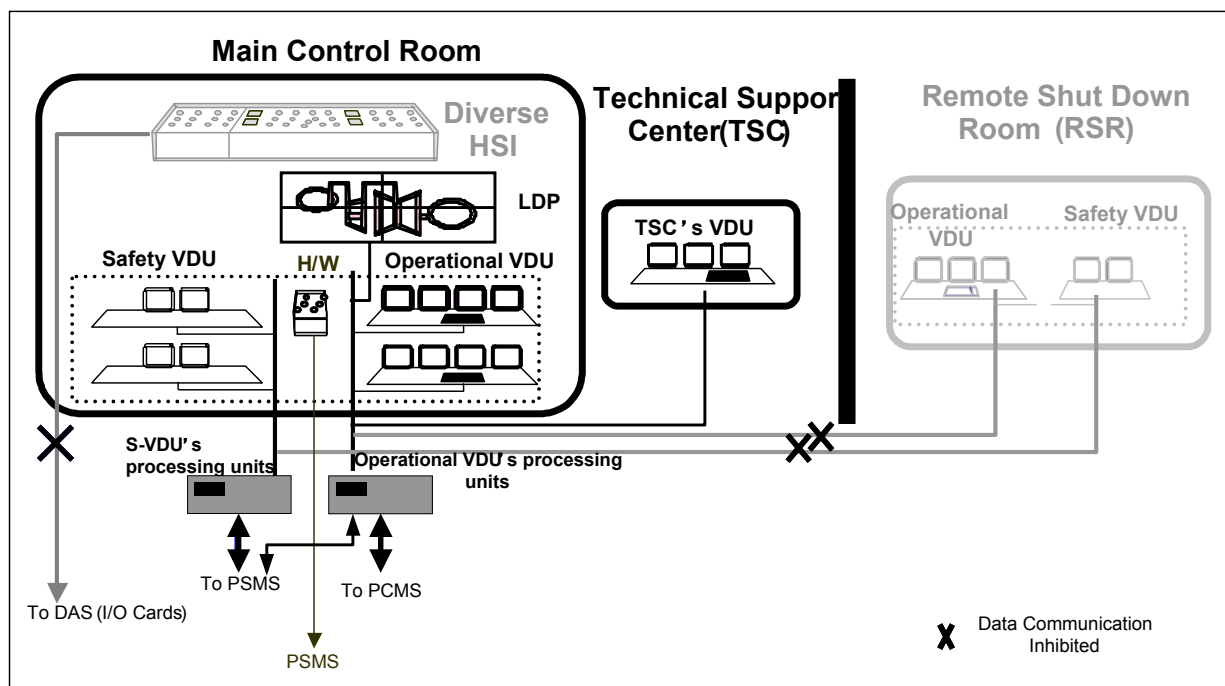


Figure 4.11-1 Standard Configurations for the Plant Operation

4.11.2 Degraded HSI Systems by a Single Failure

Figure 4.11-2 shows the overall architecture of the I&C System. In this architecture the HSIS data communication buses and computers have a duplicated configuration:

- Unit Management Computer (UMC)
 - Plant performance calculation (Reactor thermal power, etc.)
 - Logic calculation for monitoring (OK monitor, etc.)
- Process Recording Computer (PRC)
 - Plant operation logging instead of recorders of conventional plants
 - Plant trip sequence record
 - Long term recording of specific analogue parameters in case of an accident
 - Fast recording of specific analogue parameters in case of a transient or accident
- Alarm logic Computer
 - Dynamic prioritization of alarms
 - Alarm control (acknowledge, Reset, etc.)
 - Alarm logging with time
- Large Display Computer
- TSC Computer
- EOF Computer

Therefore, a single failure of the bus or computers induces no influence on plant operation tasks. However, a single failure of VDUs, VDU processors or the LDP is considered.

As for a failure of LDP, the most likely failure of the LDP is that of the back lamp. The LDP has a spare lamp in it and easily exchanged by manual. In addition, it is also available to change the variable area to display a failed fixed area display and the SDCV function of the LDP is maintained.

The set of VDUs for a single operator is as follows:

- | | |
|---------------------------|---|
| - Operational VDU | 3 |
| - Alarm VDU | 1 |
| - Operating Procedure VDU | 1 |

The appropriateness of the above described quantity of VDUs is confirmed by task analysis and by static and dynamic V&V by operators. Since there are two complete sets of 5 VDUs at the Operator Console, for use by one or two ROs, the operability is also validated in case of failure of one of the above VDUs.

As for the failure of the console for SS or STA, the SS console and STA console has the same function and capability. The SRO can shift to the non-failed console.

The appropriateness of the operator staffing of one Reactor Operator (RO) and one Senior Reactor Operator (SRO) under these degraded HSI conditions is confirmed by task analysis and by static and dynamic V&V by operators.

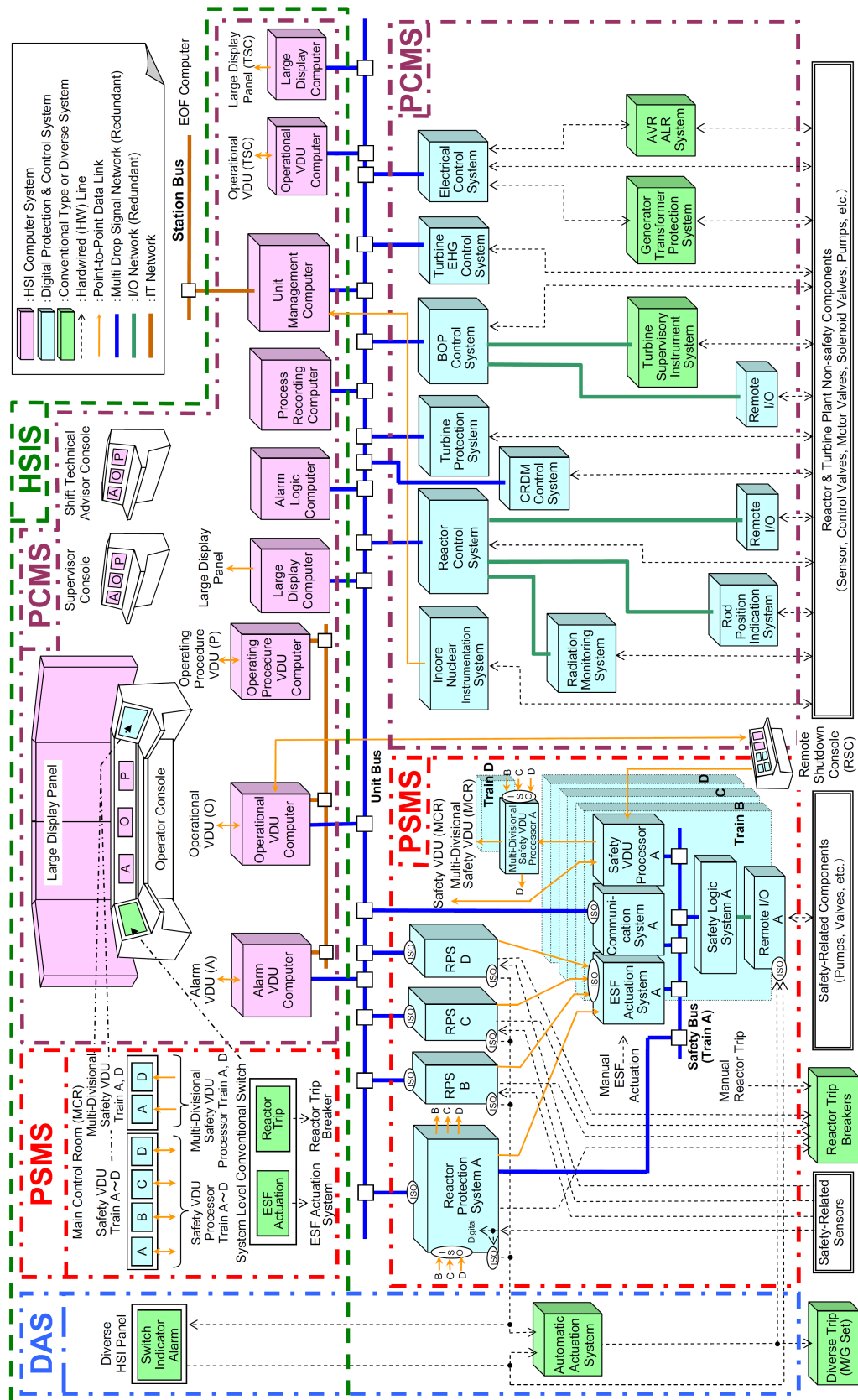


Figure 4.11-2 Overall I&C System of the US-APWR

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

4.11.3 Loss of All Non-safety HSI

The loss of the HSI is defined by a set of criteria (e.g., how many workplaces are needed to operate the plant and how many screens per workplace are needed). These criteria are defined during the detail design. However, for the worst case design basis, loss of the LDP and all non-safety VDUs is postulated.

The self diagnosis of non-safety HSI system is expected to inform operator of the failures on LDP alarms and the Data Management Console (DMC) buzzer and messages. But since failure of all non-safety HSI is assumed, final credit for plant operability is supported by only the safety VDUs.

The criteria based on the operational needs are mainly defined by determining the minimum information and controls required to execute paper-based Emergency Operating Procedures (EOP). Even in this case the minimum staffing of one RO and one SRO is considered. The safety VDUs provides means to monitor safety parameters and controls of all of the safety components.

The Limiting Condition for Operation (LCO) for loss of all non-safety HSI is defined in the Technical Specifications of the Plant Licensing Documentation. The following conditions are typical:

Condition 1: Maintain present conditions and monitor and maintain critical safety functions by safety VDU and repair failures within approximately 12 hours.

This condition is preferred because it avoids a forced shutdown plant transient under degraded HSI conditions. However, the ability to maintain this condition is largely based on the operability of the plant's non-safety control systems. If the failure only affects the non-safety HSI, it is likely the plant control systems will remain operable and will continue to control the plant in automatic modes. If the failure also affects the non-safety control systems, it is likely that a forced shutdown will be required.

Condition 2: If condition 1 is not satisfied, the plant is shutdown, and maintained in a hot stand-by state by safety VDUs (using only safety plant systems) and repair failures within 72 hours.

Condition 3: If condition 2 is not satisfied, the plant is moved to and maintained in a cold shutdown condition by safety VDUs (using only safety plant systems).

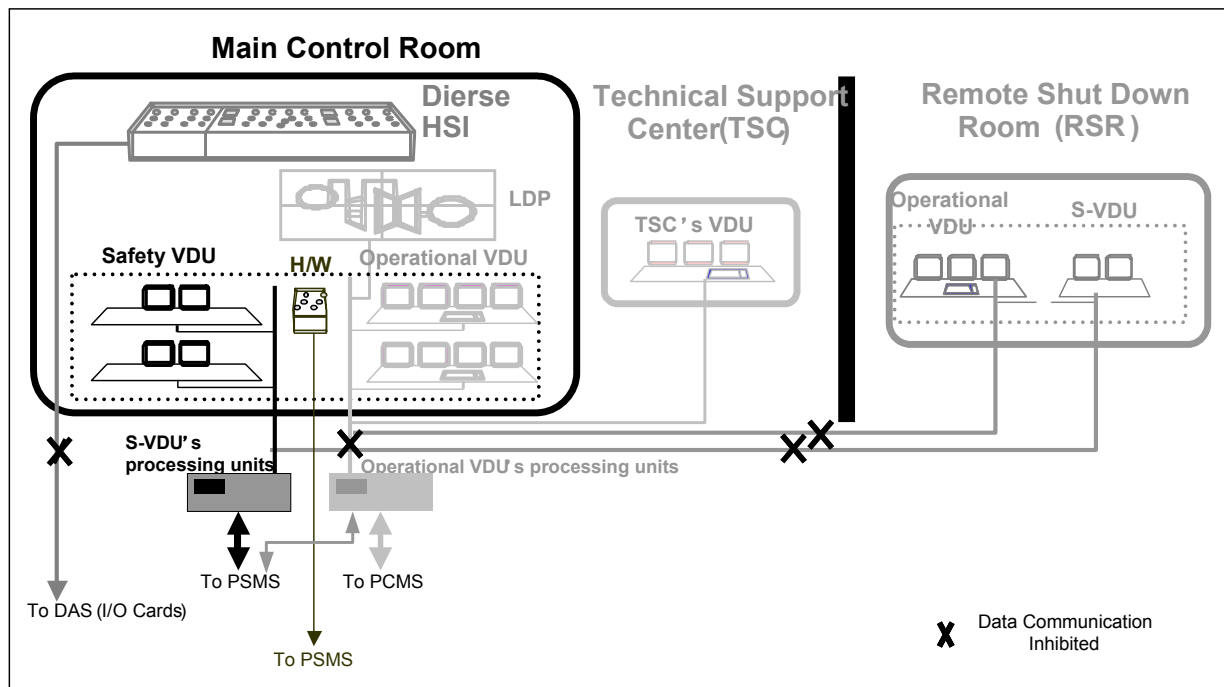


Figure 4.11-3 Configurations in Case of Operational VDU Loss

The appropriateness of the operator staffing of one Reactor Operator (RO) and one Senior Reactor Operator (SRO) under these degraded HSI conditions is confirmed by task analysis and by static and dynamic V&V by operators. Additional operators that are available at the plant are utilized as needed.

4.11.4 Loss of All Digital Non-safety and Safety HSI (CCF)

If all digitalized I&C including HSI related processors is lost, the operation of the plant is transferred to the DAS HSI Panel (DHP). The MCR and the RSS are not allowed to send orders to the process. The switch of control mean is governed by a procedure.

The enabling of the DHP is governed by a procedure. The I&C systems design ensures priority is given to signals that maintain the safety functions. The operator uses procedures and the DHP to maintain the following safety functions, as a minimum:

- Reactivity Control
- RCS Inventory
- Core Cooling
- Secondary Heat Sink
- RCS Integrity
- Containment Integrity

The control and monitoring means for the DHP are provided as hard wired switches and indicators. It ensures the diversity to the other digital HSI systems.

The configuration and system architecture are described in the Defense in Depth and Diversity (D3) topical report.

The Limiting Condition for Operation (LCO) for loss of all digital non-safety and safety HSI is defined in the Technical Specifications of the Plant Licensing Documentation. The following conditions are typical:

The plant is shutdown, and maintained in a hot stand-by state by the DHP (using all available, but primarily plant safety systems) and failures are repaired. The DHP does not provide the capability to transition to cold shutdown.

The D3 Coping Analysis also demonstrates the ability to cope with Anticipated Operational Occurrences and Postulated Accidents under this CCF condition. The operator actions credited in this coping analysis are executed from the DHP. These actions are encompassed and evaluated through the HFE design process described in Section 5.

The appropriateness of the operator staffing of one Reactor Operator (RO) and one Senior Reactor Operator (SRO) under these degraded HSI conditions is confirmed by task analysis and by static and dynamic V&V by operators. Additional operators that are available at the plant are utilized as needed.

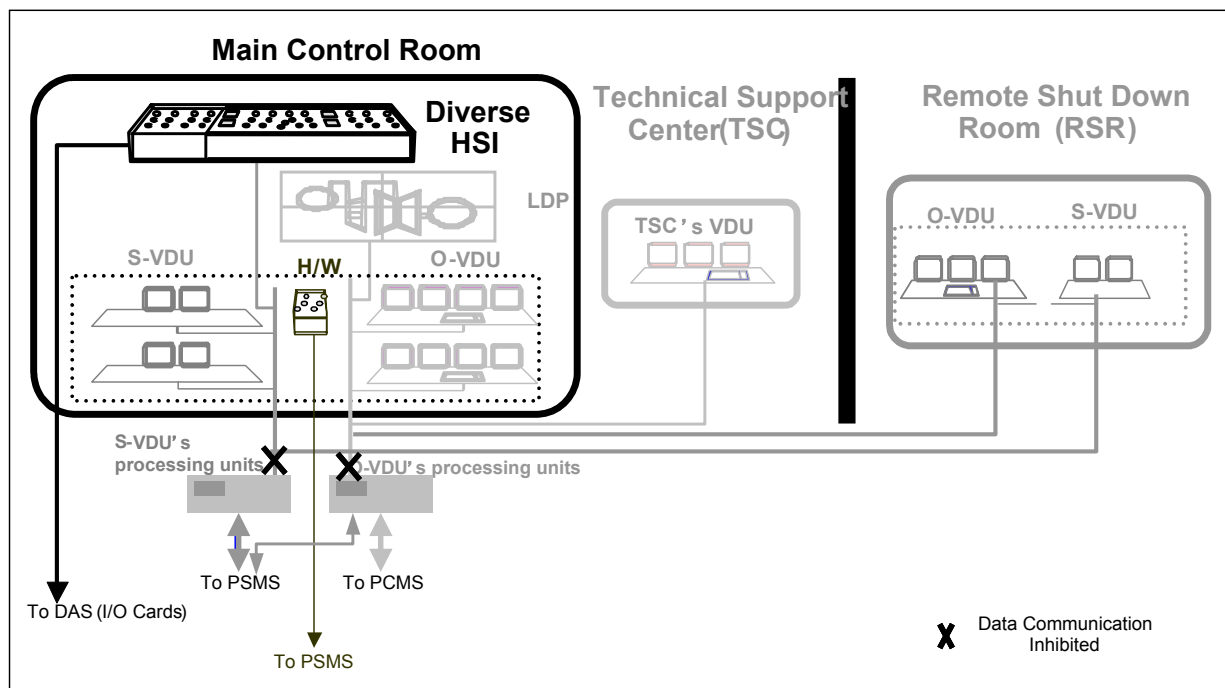


Figure 4.11-4 Configurations in Case of CCF

4.11.5 Loss of MCR

In this configuration, the main control room must be evacuated for undefined reasons or due to fire. Initially any degradation to HSI equipment is limited to only one safety or non-safety division due to separation and independence of divisions in the MCR. However, ultimately it is assumed that the fire damages all MCR HSI equipment. Therefore the operation of the plant is transferred to the remote shutdown room (RSR) where the plant is brought and maintained to a safe shutdown condition.

Before leaving the MCR, the shift team performs preliminary actions like tripping the reactor. However, if time permits reactor trip is not executed until the RSR is manned. This avoids

creating a plant transient that cannot be monitored. Once operators arrive in the RSR, the MCR control means are isolated from the process so that they are not allowed to send orders (but the RSR is). This transfer is governed by an operating procedure. Since all MCR HSI functionality is available at the RSR (i.e., all safety and non-safety divisions) there is no need for evaluation of display, alarm or control availability.

The appropriateness of the minimum operator staffing of one RO and one SRO is confirmed by analytic validation of the task analysis and the static and integrated V&V by operators.

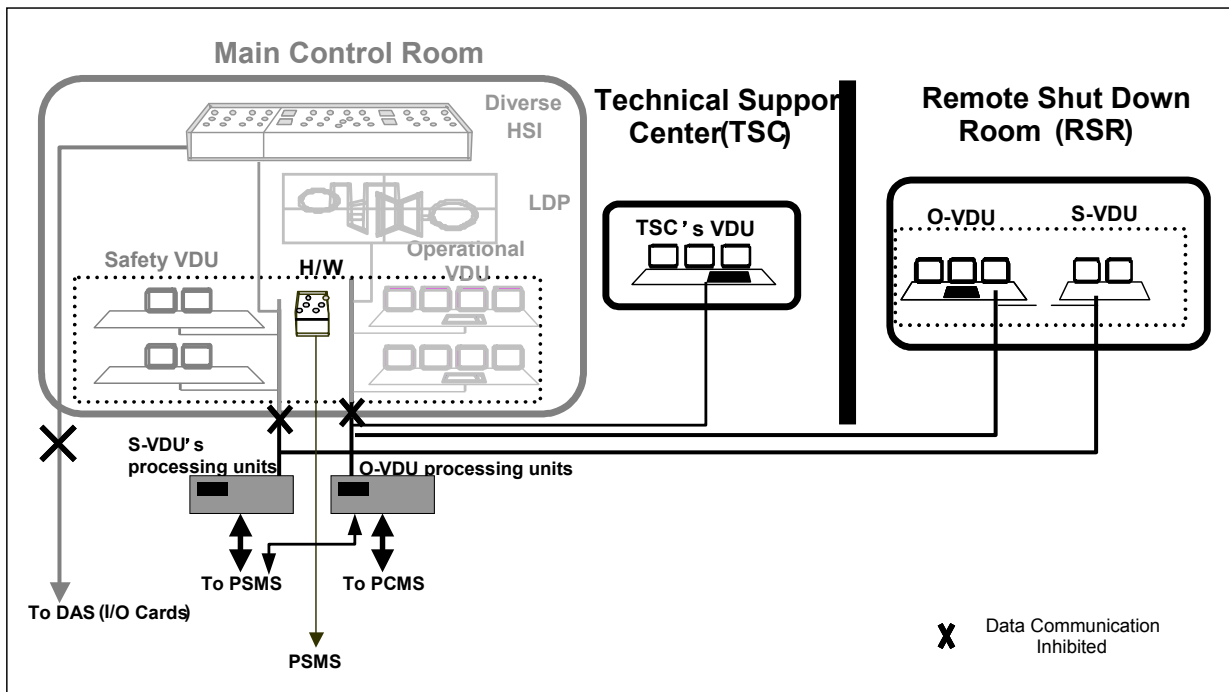


Figure 4.11-5 Configurations in Case of MCR Loss

4.12 Key Technical Issues

This section summarizes the key HSI related technical issues.

a. Multi-channel operator stations

For all plant conditions, including DBA and safe shutdown, the primary operator interface is provided by

- Non-safety Multi-channel LDP
 - SDCV information and alarms significant to safety and power production
- Non-safety Multi-channel VDUs
 - Selectable interface for all other information, alarms and controls
- Conventional Class 1E switches
 - SDCV controls for system level actuation of safety functions

Safety VDUs provide back-up Class 1E information and control for all safety functions. And also provides SDCV monitoring function for Post Accident Monitoring parameters.

Non-safety multi-channel HSI allows the operator interface to match the integration of safety and non-safety functions that exist in plant systems and to utilize those systems in an integrated manner to maintain plant functions. The non-safety multi-channel HSI is developed under the HFE Program and with a software development process that ensures suitable quality for use during all normal and abnormal plant conditions.

b. HSI to accommodate reduced operator staffing

Integrated safety and non-safety functions on the Multi-channel LDP and VDUs provide the following benefits:

- Continuous awareness of critical safety functions while immediate focus may be plant maneuvering and power production.
- A single operator can execute procedures that involve multiple safety divisions and non-safety systems, simplifying task coordination for maintaining a single safety function.
- Operators can execute computer based procedures with integrated information and controls and/or hyperlinks.

It minimizes operator transitions between safety and non-safety VDUs, thereby reducing operator workload during critical plant situations.

The benefits reduce operator task burden, reduce potential for human error, and facilitate reduced MCR operator staffing.

The minimum staffing of one SRO and one RO in the MCR and one additional SRO and RO at the plant, meets the staffing requirements of 10CFR50.54. This minimum staffing is validated for normal operation and all degraded HSI conditions.

c. Operation under Degraded Conditions

The HSIS accommodates the following degraded HSI conditions:

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

The HFE Program validates operation under these degraded conditions with the minimum plant staff.

d. Minimum inventory of HSI

The fixed area of LDP presents SDCV information to the operating staff. The parameters and alarms on the LDP are described in Section 4.9, including SDCV indications for BISI of RPS, ESFAS and plant safety systems.

Means are provided in the MCR for manual initiation of protective functions at the system level. These functions are realized by conventional hard-wired Class 1E switches that enable easy and prompt access by the operator. Means for manual control of safety systems at the component level are realized by the safety VDUs described in section 4.6.

The minimum SDCV inventory and the minimum inventory for degraded HSI conditions are established to monitor and control the six critical safety functions:

- Reactivity Control
- RCS Inventory
- Core Cooling
- Secondary Heat Sink
- RCS Integrity
- Containment Integrity

This applies to all normal and emergency plant modes. The specific functions and tasks and the key required HSI resources, including alarms, controls, displays and procedures, are extracted from Normal Operating Procedures, Emergency Operating Procedure (EOP) and Plant probabilistic risk assessment (PRA), which are described in plant licensing documents. The minimum inventory is based on monitoring key performance parameters for each critical function and controlling the preferred non-safety and safety success paths. The design of the minimum inventory HSI is developed and evaluated through the HFE design process described in Section 5.

This is because Class 1E HSI is provided for all Class 1E instrumentation and plant components via Safety VDUs. The design of the minimum inventory HSI (SDCV and Class 1E) is developed and evaluated through the HFE design process described in Section 5.

e. Computer based procedures

In addition to the display Navigation system for HSI, the computer based operating procedure VDU is provided. It enables operators to perform certain and reliable operations.

The computer based procedures (CBP) are developed under the HFE Program and with a software development process that ensures suitable quality for use during all normal and abnormal plant conditions. The change process defined for CBP maintains the original quality while reducing the maintenance burden to a manageable level.

5.0 HFE DESIGN PROCESS

The US Basic HSIS will be applied in its entirety to the US-APWR and to operating plants. Therefore, the HFE design process described in this section is applicable in its entirety to the US-APWR and to operating plants.

This section describes the generic HFE design process. Any portions of the HFE design process that are not complete for a specific plant and therefore may require future commitments, such as Design Acceptance Criteria or licensing conditions for operating plants, are described in Plant Licensing Documentation.

The HFE program plan described in this section is a general version of an HFE program plan which can be applied for new plants as well as plant modifications. The plant licensing documentation for each project provides an individual HFE program plan which can accommodate each project integrating some citation of the general portion of a HFE program plan in the topical report and specific information considering each project condition. Chapter 18 of the US-APWR DCD exemplifies a plant specific program plan, which fulfills the requirement for “plant licensing documentation”. This plan is followed by an Overall HFE Implementation Procedure and specific Implementation Procedures for each program element, all written uniquely for each project. A similar set of plan and procedure documents will be written for each plant modification project.

5.1 Human Factors Engineering Program management

The overall goal of the HFE program management is to ensure the HSI system reflects the latest human factor principles and satisfies all of the required regulatory requirements. In addition, the goal is to define the means by which HFE activities are executed. (Reference 11)

5.1.1 Human Factors Engineering Program

5.1.1.1 Human Factors Engineering Program Goals

The general objectives of the HFE Program are stated in “human centered” terms, which, as the HFE Program develop, are defined and used as a basis for HFE test and evaluation activities. The Human Factors Engineering Program goals include the following:

- Personal tasks are accomplished within the required time and in accordance with specified performance criteria
- The HSIs, procedures, staffing/qualifications, training and management and organizational support result in a high degree of operating crew awareness of plant conditions.
- The plant design and allocation of functions maintain operational vigilance and provide acceptable workload levels to minimize periods of operator underload and overload.
- The operator interfaces minimize operator error and provide for error detection and recovery capability.

The generic HFE program goals of the program are as follows;

- i) Ensures HFE program is implemented in conjunction with plant design process. Appendix C, HSI/HFE topical report show the HFE program will be completed in conjunction with plant design process which will be completed by the plant construction and operation milestone.
- ii) Ensures that the integrated HSI and support functions/ implementation program, i.e., operating procedures, staffing/qualifications, training show high degree of operating crew situation awareness.
Operating crew situation awareness will be verified and validated in V&V process and Human Engineering Discrepancy (HED) which addresses situation awareness issue, will be addressed and resolutions are fed back to HSI design and/or supporting functions/programs in order to improve them. Then this iteration process will continue until the situation awareness level reaches more than the current situation awareness level of operating HSI using Likert measurement methodology.
- iii) The plant design and allocation of functions always provide operation vigilance and acceptable workload levels.
Functional requirement analysis and Functional allocation address operator's significant monitoring parameters and controls and task analysis ensures the minimum staffing can conduct operations within acceptable workload levels. Acceptability is determined by ensuring tasks can be accomplished within time and performance criteria, and by comparing workload levels to that of conventional plants.
- iv) The HSI and supporting functions/programs minimize operator error and provide for error detection and recovery capability.
Human Reliability Analysis addresses critical human actions for establishing plant safety and how they are considered through HSI design and supporting functions/programs.

5.1.1.2 Assumptions and Constraints

An assumption or constraint is an input to the HFE program. The design assumptions and constraints are following:

- Program must conform to regulations and rules related to safety and human factors design.
- Program must meet the requirements of utility operators. For this purpose, functional requirements analysis and function allocation are processed by the method described in Section 5.4., verification of the function allocation is conducted by the task analysis method described in Section 5.4, and validation of the HSI design is ultimately evaluated by the verification and validation method described in Section 5.10.
- Human system interface requirements must be consistent with the control and instrumentation capabilities of the plant process systems (i.e. the process systems of the US-APWR or the process systems of operating plants for upgrades).
- State-of-the-art human factors practices and computer technologies must be utilized. However, hardware restrictions are taken into account in the human system interface design.
- MHI uses Safety VDUs for safety related HSI. To meet the software quality requirements, the software for these devices must be kept very simple. As a result, these devices have primitive graphics and navigational capabilities.

- To meet the D3 (Defense-In Depth and Diversity) requirements, MHI uses conventional HSI components, such as analog indicators, status lights, alarm tiles and switches. These devices do not have the same dynamic capabilities as digital VDU HSI devices.

The detail design HFE implementation plan is described in Section 5.11.

5.1.1.3 Applicable Facilities

The description of the applicable facilities is implemented in Section 4.2.

5.1.1.4 Applicable HSIs, Procedures and Training

The applicable HSIs, procedures, and training for the HFE Program encompass all operations, accident management, maintenance, test, inspection and surveillance interfaces (including procedures) for safety significant equipment.

5.1.1.5 Applicable Plant Personnel included in HFE Program

The description of the Plant Personnel in HFE Program is implemented in Section 4.1.

5.1.2 Human Factors Engineering Design Team and Organization

5.1.2.1 Organization

The organizational structure to control the Human Factors Engineering is shown in Fig. 5.1-1.

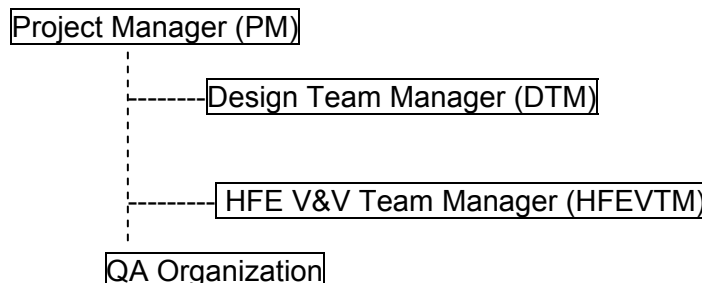


Figure 5.1-1 Organization of HFE Design Team

5.1.2.2 Roles and Responsibilities

The roles and responsibilities for the key sections of the organization are described in this section.

1) Project Manager (PM)

The PM assures that process of design, V&V and quality assurance is appropriately implemented in accordance with the HFE Implementation Plan.

2) Design Team Manager (DTM)

The Design Team conducts all design activities for hardware and software. The DTM is responsible for developing and maintaining the HFE design process schedule. The DTM is

the central point of contact for management of the HFE design and implementation process. The DTM assures that the design team correctly performs the design based on the technical requirements and the development process in accordance with the HFE Implementation Plan. The DTM is also responsible for

- Development of HFE plans and procedures, conducting HFE activities for all elements except Verification and Validation (V&V), and review of V&V results.
- Initiation, recommendation, and provision of solutions for problems identified in the implementation of the HFE activities
- Verification of the effectiveness of the solutions provided to problems
- Assurance that HFE activities comply with HFE plans and procedures
- Phasing of activities*
- Methods for identification, closure, and documentation of human factors issues
- HSI design and HFE documentation configuration controls

Note: * The Design Team Manager's responsibility of "phasing of activities" includes planning the schedule for all HFE activities and milestones, including the high level scheduling of V&V activities and milestones. However, the detailed scheduling of V&V activities and milestones is the responsibility of the V&V Team manager.

The HFE Design Team holds the following technical skills.

- Human Factors Engineering
- Systems Engineering
- Nuclear Engineering
- Instrumentation and Control (I&C) Engineering
- Architect Engineering
- Plant Operations
- Computer System Engineering
- Plant Procedure Development
- Personnel Training
- Systems Safety Engineering
- Maintainability/Inspectability Engineering
- Reliability/Availability Engineering

The HFE Design Team is directly responsible for developing plans, procedures and schedules, and carrying out the HFE activities for the operating experience review, the functional requirements and function allocation analysis, and the task analysis. The HFE Design Team reviews the plans, procedures and schedules, and provides oversight for the staffing and qualifications analysis, the human reliability analysis, procedure development, V&V, the training program development, the design implementation, and human performance monitoring. The HFE design team conducts all design activities for HSIs. The HFE design team consists of a multi-disciplinary technical staff. The team is under the leadership of an individual experienced in the management of the design and operation of complex control technologies. The specific individuals and qualifications of those individuals, who are responsible for each HFE program element are documented within the implementation procedure for that HFE program element.

3) HFE V&V Team Manager (HFEVTM)

The V&V team conducts the HFE Verifications and Validations in accordance with the HFE V&V Implementation Plan.

The V&V Team Manager is responsible for all activities of the V&V Team, development of HFE plans and procedures for V&V and review of HFE plans, procedures and results for all elements except V&V. HFEVTM has sufficient resources (budget, staff, etc.) and authorities to ensure V&V activities are not adversely affected by commercial and schedule pressures.

The V&V team holds following technical skills:

- plant operation and operator training
- Human System Interface design
- Human factor engineering

The V&V Team has technical competence equivalent to the Design team. The V&V Team shall ensure all items in the HFE Issues Tracking System have been completed at the appropriate phase of the design process.

4) QA Organization

The QA organization conducts the quality assurance in accordance with the Quality Assurance Plan which includes conformance of the suppliers' overall QA program.

The QA Organization shall conduct periodic audits of the design and V&V processes, which include disposition of items in the HFE Issues Tracking System.

For each new plant or operating plant upgrade project, the following will be included in the project Quality Assurance Manual:

“New or revised documents that describe or impact human actions regarding operations, maintenance or test activities of safety significance shall be reviewed by the HFE Team. Comments from the HFE Team should be mutually resolved prior to issuance of the document. Where this is not possible, the comments shall be tracked for resolution in the HFE Issues Tracking System. Comments that cannot be resolved shall be elevated through the management chain for resolution.”

The Design Team and V&V Team are trained in the constraints of the overall I&C design. Each project includes an Overall HFE Implementation Procedure and specific Implementation Procedures for each program element. These procedures detail the responsibilities of the HFE Design Team and V&V Team, including how those teams carry out their responsibilities for each program element.

As a minimum, the HFE team for each program element will include one or more experts with skills in HF engineering, plant operations, program management and database management. In addition, the following additional experts will be included for each specific program element:

- OER – I&C
- FRA/FA – plant systems
- TA –plant systems
- Staffing and Qualifications – plant maintenance
- HRA – PRA
- HSI Design – I&C, plant systems
- Procedures – procedure
- Training – training
- V&V – training and procedure
- Design Implementation – I&C
- Human Performance Monitoring – training

5.1.3 Human Factors Engineering Processes and Procedures

a. General Process Procedures

The process through which the HFE Design team executes its responsibilities is depicted in Figure 5.1-2. . In this figure, the “Design Section” refers to another organization (not the HFE team) responsible for generating a document that contains requirements or descriptions of safety significant human-machine interfaces. The “Review Committee” refers to the aggregate of all reviewers for that document; an HFE team member is one of the reviewers. “Review record sheets” and “Record Review Log” are used to formally document and track the reviewers’ comments. Comments that result in unresolved HFE issues are extracted and tracked in HFE Issues Tracking system. These issues are closed only after the resolution is reflected in the appropriate HSI documentation (e.g., HSI design, procedures, training).

- The HFE Design team manager is responsible for assigning HFE activities to individual team members, governing the internal management of the team, and making management decisions regarding HFE.
- HSI design is made and prepared by the HFE design team and the answers to the comments on the design are approved by the HFE Design team manager.
- Equipment design changes are conducted using the Review record sheet in accordance with the process flow shown in Figure 5.1-2.
- Design team review of HFE products is conducted in accordance with the process flow shown in Figure 5.1-2.

An HFE Design Team representative will be assigned to review every plant document that contains requirements or descriptions of safety significant human-machine interfaces. This includes documentation for local controls, maintenance activities, periodic testing activities, etc. HEDs identified by the HFE Design Team reviewer will be entered in the HFE Issues Tracking System database and tracked to closure.

b. Process Management Tools

The HFE Design team uses “Review Record Sheet” to implement the HFE review process. An example of the HFE review form attached to the Review Record Sheet is shown in Table 5.1-1.

c. Integration of HFE and Other Plant Design Activities

The inputs from other plant design activities to the HFE Program and the outputs from the HFE Program to other plant design areas are extracted and summarized in discrepancy reports before the open review committee meeting. These results are reviewed in the review committee meetings. The review committee meetings are held concurrently with the design process described in Figure 5.1-3.

d. HFE Program Milestones

HFE Program Milestones are shown in Figure 5.1-3. A relative schedule of HFE tasks showing relationships between HFE elements and activities, products, and reviews is also shown in

Figure 4.0-2. The Phased Implementation Plan for the complete HFE program is described in Appendix C.

e. HFE Documentation

Deviations from the evaluation criteria derived from functional requirements and/or other input documents are documented and rated for severity in terms of their potential effect on performance of the HSI system.

f. Subcontractor HFE Efforts

The HFE Team confirms that HFE requirements are included in each subcontract. The subcontractor's compliance with HFE requirements are periodically verified by review of the subcontractor's HSI design and manufacturing guidelines by the HFE Team. The V&V Team is responsible for this verification review. Verification will be conducted to the same standards as designs created by the Design Team. For example if the supplier is required to conform to the US Basic HSIS Style Guide, which the V&V Team has already verified against NUREG-0700, the V&V Team will verify the supplier's products against the Style Guide. Otherwise, the V&V Team will verify the supplier's products against NUREG-0700. In all cases, the HSI inventory provided by the supplier will be verified against the operating / maintenance / test procedures and/or the task analysis. Verification procedures are plant specific documents. These procedures define the standards and input documents to which the supplier's design will be verified. These verification activities occur during the design stage.

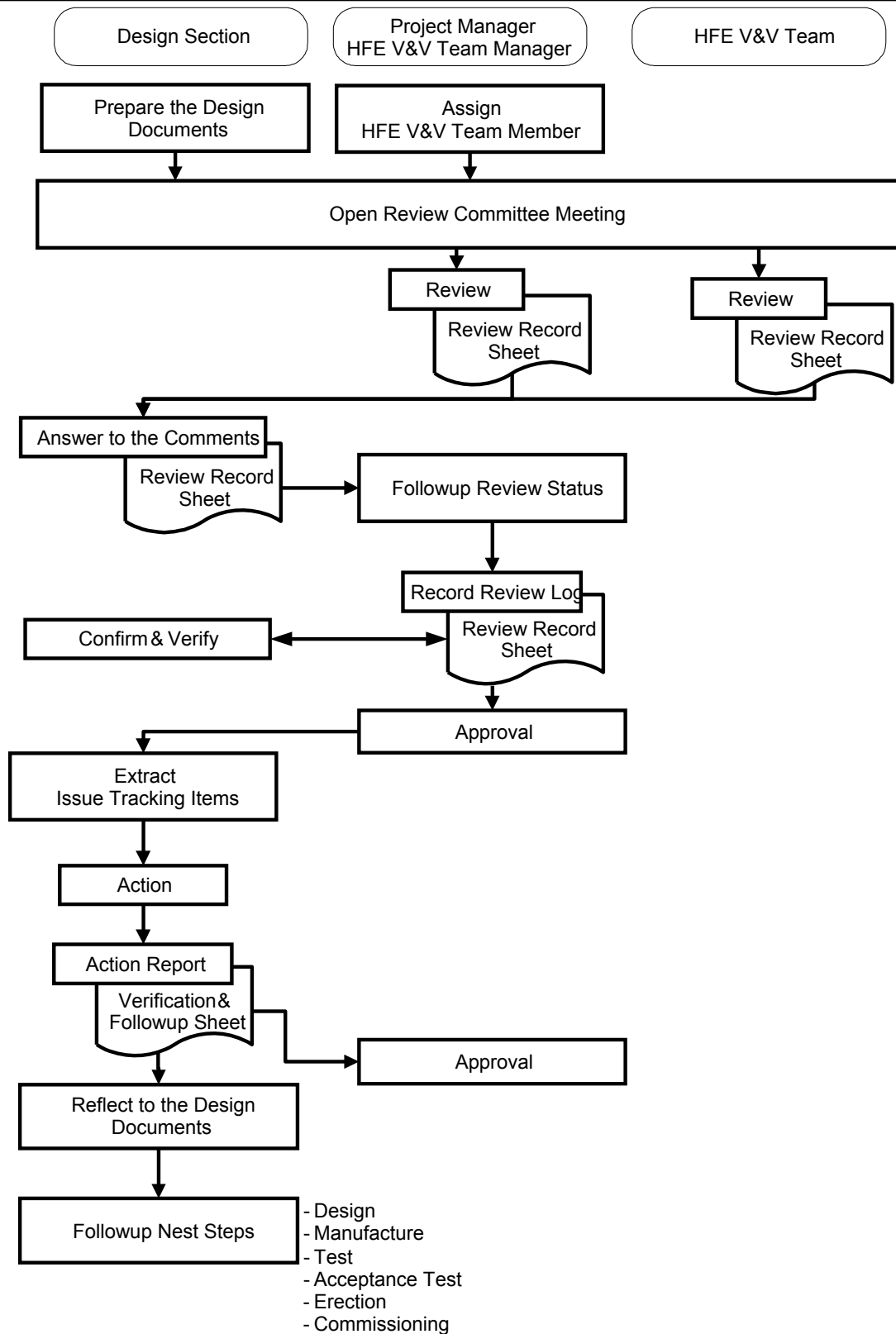


Figure 5.1-2 General Process Procedure of HFE Design

Table 5.1-1 Example of Comment Sheet in Review Process

Document					
Date					
Review Items	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/ Editorial)	COMMENTS	Answer to the comments

5.1.4 Human Factors Engineering Issues Tracking

The HFE Issues Tracking System is the same as tracking system used for the rest of the design effort of the US-APWR. It is available to address human factors issues that are either (a) known to the industry or (b) identified throughout the HFE design, development, and evaluation process.

- HFE Design Team members are responsible for issue logging, tracking and resolution, and resolution acceptance.
- There is no significance threshold for issue entry into the tracking system. Each issue or concern entered into the system is evaluated for its significance to human performance. The basis for the disposition of all entries is included in the database.
- Each action taken to eliminate or minimize the issue or concern is thoroughly documented. The final resolution of the issue is documented in detail, as is the design team's acceptance of the resolution.

5.1.5 Human Factors Engineering Technical Program and Milestones

The HSI design implementation activities include the development of static and dynamic models for evaluating the overall plant response as well as the performance of individual control systems, including operator actions. Verification activities, using static graphic displays are conducted prior to validation activities, using dynamic displays driven by high fidelity plant models. The dynamic models are used to:

- Analyze steady state and transient behavior,
- Confirm the design of the advanced alarm system concepts,
- Confirm the adequacy of control schemes,
- Confirm the allocation of control functions to a system or an operator,
- Develop and validate plant operating procedures, and
- Incorporate as effectively as possible, into the plant design the utilization of full scope or limited use simulators.

Using part-task simulation an initial set of plant systems is identified through modeling, including the development of the graphical user interfaces (GUI). The part-task simulator is used in the preliminary US-APWR design and expanded to include US-APWR's unique design features. As the US-APWR design progresses, the part-task simulator proceeds through a series of iterative evaluations resulting in the development of a complete control room full scope simulator. A Full scope simulator is used for integrated validation testing. In addition, the simulator facility is the focal point for operator evaluations and feedback checkpoints throughout the HSIS design process.

The general development of the following eleven key implementation plans, analysis, and evaluations is identified and described in Figure 5.1-3.

- Operating experience review
- Functional requirements analysis and function allocation
- Task analysis

- Staffing and qualifications
- Human reliability analysis
- HSI design
- Procedure design
- Training design
- Human factors verification and validation
- Design implementation
- Human performance monitoring

The HSI design implementation activities include the development of static graphic displays, and dynamic graphic displays driven by high fidelity plant model simulators. Static graphic displays are used for the following verification activities:

- i) Conformance to NUREG-0700 design criteria
- ii) Confirmation of HSI inventory with operating procedures
- iii) Confirmation of usability with task analysis. Dynamic graphic displays driven by high fidelity plant model simulators are used to validate the completely integrated HSI design. Verification activities, using static graphic displays are conducted prior to dynamic validation activities with high fidelity plant simulator models.

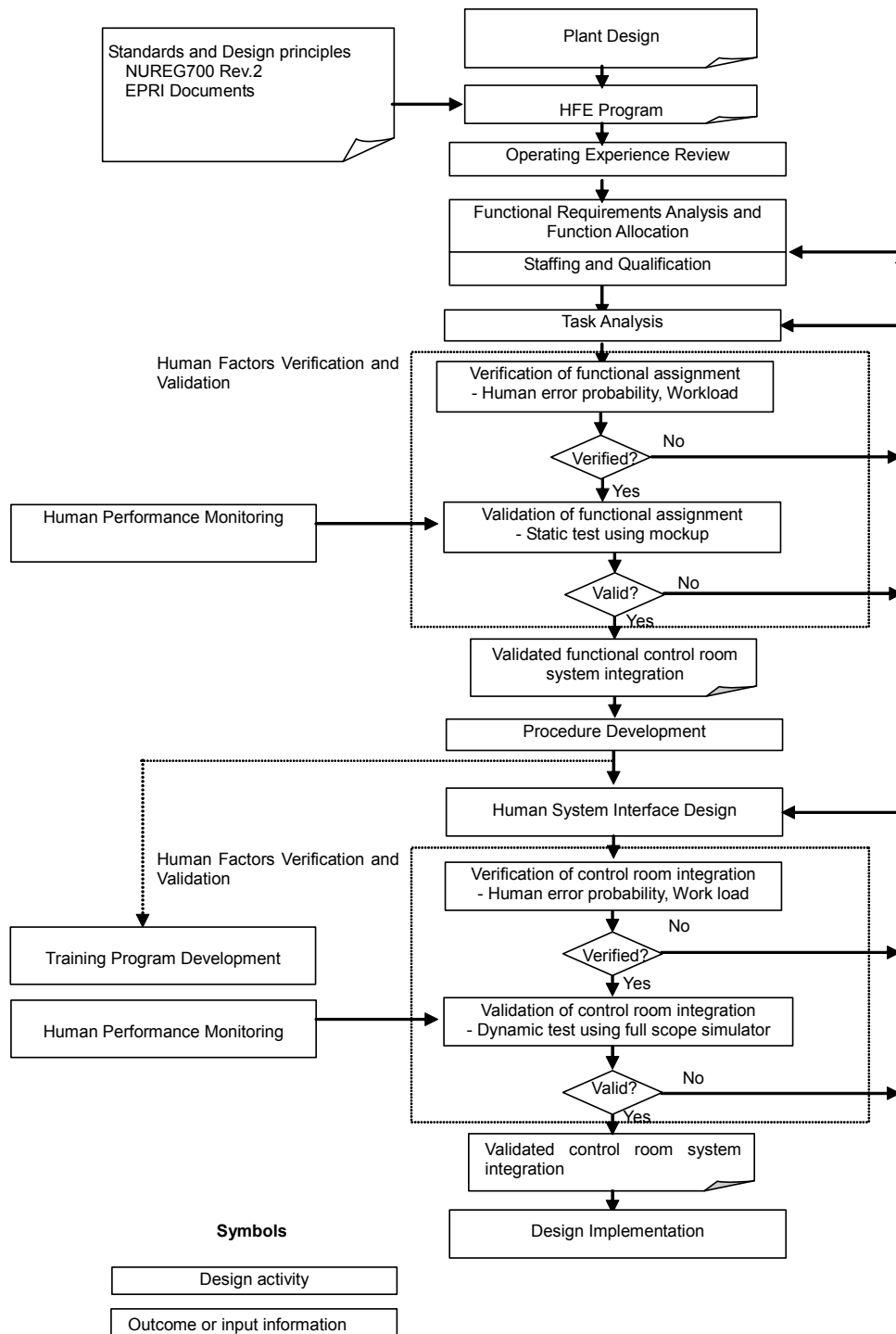


Figure 5.1-3 Overall Design Process

5.2 Operating Experience Review (OER)

The main purpose of the operating experience review is to identify HFE-related safety issues that arose in previous designs. HFE-related issues are extracted from the past commissioning and operating experience and are addressed in the new design.

OER information sources include NUREGs (Reference 5.2,etc.), Nuclear industries reports (e.g., INPO, LER) and Utilities operator's interviews.

The OER implements the following process:

- Extracting and screening HFE-related issues to identify those relevant to the MHI HSI system. Brief explanations are provided for issues considered not relevant.
- Relevant issues are evaluated. Explanations are provided for issues that are already accommodated in the HSI design. It is noted that the HSI design is still evolving at this point, so the evaluation considers the design only as it is defined in documentation at the time of the OER (i.e., anticipated design features that are not currently documented are assumed not to exist at the time of this evaluation). Issues not accommodated in the current HSI design documentation are added to the HFE Issues Tracking System for further resolution.
- Conducting the HFE issues resolution process.

MHI has examined and addressed the issues and causes of the events in the past commissioning and/or the present operating plants, both domestic and overseas, and improved the in-service plant facilities and the construction plant designs if necessary in order to avoid the issue again.

When the HSI system is applied to an operating plant, the Corrective Actions Program for that plant will be reviewed to identify any plant specific human performance issues that have not already been accommodated in the US Basic HSIS or that may be applicable to the specific HSI Inventory for that plant.

Each application of MHI's HSI system will build upon previous applications. For example, the first US-APWR will build upon the application of the HSI system to Japanese plants. The first application of the HSI system to an operating plant, will build upon the application to the US-APWR. Therefore the scope of OER and the specific plan for that OER is described in plant specific licensing documentation.

Table 5.2-1 shows the example of the OER analysis.

Table 5.2-1 Example of OER Analysis

Control Number	Prepared	Source Number	Plant	Issue Date	System	Comments	Subject	Abstract	Situation	Contributing Factors	Corrective Actions	Status	Analysis of Countermeasures for the Domestic plants
2006-12-0204	-	NRC Information Notice 2006-18	FORSMÅ (KÄLSÄVER / SWEDEN)	2006/07/25	Electric system	Emergency battery	The loss of two of the four trains of safety power and AC and DC power due to a common mode failure	The event occurred in the 400 kV switchyard to support maintenance. During the maintenance, a short circuit in the switchyard led to the loss of two of the four trains of safety power and AC and DC power due to a common mode failure. The events is significant in that it could have caused the common mode failure in all four trains and therefore, could have resulted in the loss of all four trains of safety-related AC and DC power. The Swedish Nuclear Power Inspectorate categorized the event under the International Nuclear Event Scale (INES) as a level 2 event.	The event began when an arc and a two phase short circuit occurred when a breaker was opened in the 400 kV switchyard to support maintenance. The electrical transient dropped the voltage to about 30 percent of nominal voltage and the unit was disconnected from the grid. The reactor was shutdown and the unit was disconnected from the grid. The main generator. This sudden overvoltage caused two of the four electrical inverters to fail and consequently disabled two emergency diesel generators (EDGs) from powering the corresponding buses as expected. The reactor successfully scrammed and all control rods inserted. The control room staff were challenged by the absence of control room indications associated with the two trains of power supply that were lost. The event was further complicated by the actuation of the containment spray and emergency cooling systems. After restoring power, the operators were able to secure the containment spray and emergency cooling systems.	Based on the INPO reports which was attached blow	Based on the INPO reports which was attached blow	N2	In domestic plant, the same event does not occur as the following reasons: a. Switch gear shall not be opened during the maintenance by interlock logic. b. The safety inverter shall not be tripped caused by the overvoltage. c. Generator shall be tripped by Turbine trip instead of low frequency signal. d. Safety voltage line shall be automatically supplied by a backup power source.
2006-12-0216													

5.3 Functional Requirements Analysis and Function Allocation

Functional requirements analysis is the identification of functions that must be performed to satisfy plant safety objectives. Functional allocation is the analysis of the requirements for plant control and the assignment of control functions to personnel (e.g., manual control) and system elements (e.g., automatic control and passive, self-controlling phenomena).

- Combinations of personnel and system elements (e.g., shared control and automatic systems with manual backup)

Since this is an evolutionary plant, the functions and allocations are based primarily on historical practices, except as may be necessary to accommodate:

- Issues identified in the OER
- Reduced operator staffing
- New functions for the US-APWR that were not in previous plants
- Functions that are changed significantly by the use of digital technology

Therefore the focus of this HFE effort is to identify any changes from historical practices (i.e., a detailed evaluation of unchanged practices is not conducted).

“Historical practices” refer to practices in Japanese PWRs which are essentially the same as practices in operating Westinghouse PWRs in the US. The FRA/FA will identify any differences in historical practices that are pertinent to the analysis

The key function allocation changes of the US-APWR are as follows;

- An automatic isolation of emergency feed water flow to the broken SG.
- Elimination of recirculation of ECCS

Other detailed allocation changes are described in the Plant Licensing Documents. The report for this element identifies all function allocation changes from the reference plant, including the reason for those changes and technical justification regarding human performance in accordance with the methodology and criteria described in Sections 5.3.1 and 5.3.2.

The function analysis and allocation report will document the function allocation for major plant functions, with the primary focus on functions of safety significance. Where the function allocation is different than historical practices the change is justified based on change drivers, the function allocation hierarchy described in Section 5.3.1, and the function allocation principles described in Section 5.3.2. Function allocation changes from historical practices are emphasized in all aspects of the HFE program, including V&V.

5.3.1 Functional Requirements Analysis

Functional requirements analysis is the identification of functions that must be performed to satisfy plant safety objectives. A functional requirements analysis is conducted to;

- Determine the objectives, performance requirements, and constraints of the design,
- Define the high-level functions that have to be accomplished to meet the objectives and desired performance
- Define the relationships between high-level functions and plant systems(e.g., plant configurations or success paths) responsible for performing the functions

-
- Provide a framework understanding the role of controllers (whether personnel or system) for controlling the plant.
-

Figure 5.3-1 shows the hierarchical structure of the plant's functions that is performed to satisfy conventional plant safety objectives. The top hierarchical level (Critical Safety Function level) shows essential functions for the plant safety. The lower level (Event level) shows the specific emergency and accident events that are caused to affect each plant safety function. The component level shows the components that cause to affect each accident event and safety function. (References 24 and 30)

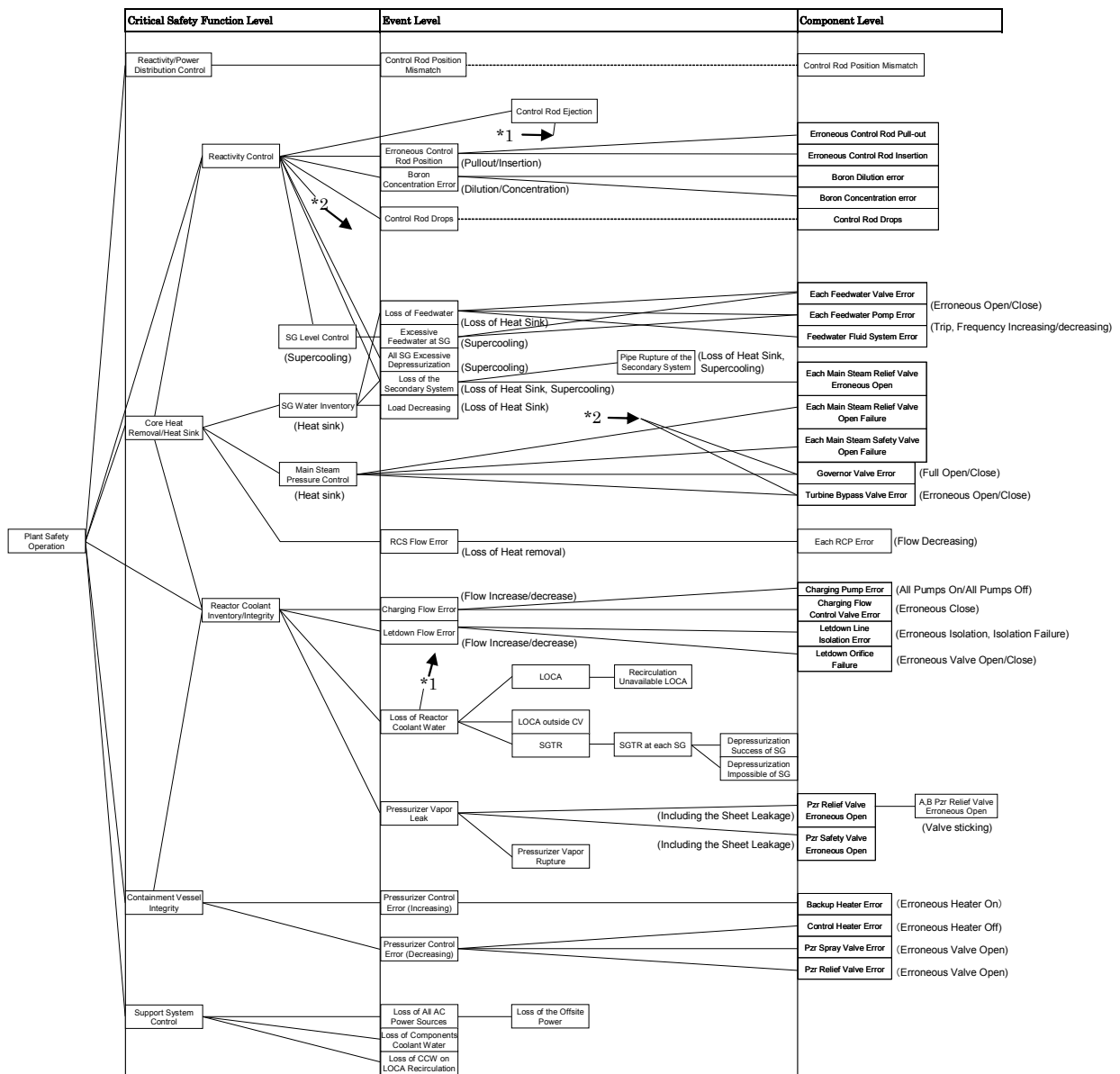


Figure 5.3-1 Hierarchical Structure of Safety Plant Functions

5.3.2 Function Allocation

The operator is ultimately responsible for the safe operation of the plant. Therefore automation is a tool applied to aid the operator, not replace the operator. Automation is applied only when it results in clear and distinct operational or efficiency advantages, and there is no adverse effect on human performance to support plant safety or availability. (Reference 24, 14 and 15)

The following two main automation rules apply:

- automated sequences have to help the operator to eliminate certain operating tasks provided that:
 - those tasks are not necessary in order for the shift operating team to maintain its knowledge of the plant situation or to build itself a comprehensive representation of that situation;
 - technological and economical objectives of sequence automation are met.
- automation of sequences has to foster co-operation between the shift operating team and the I&C designers. It is therefore necessary to inform the shift operating team of the reason, meaning, achievement, and progress of the actions performed by the I&C system.

Those rules aim at enabling the operator to stay in control of the automation installation in order to address:

- those situations that the automated sequences cannot handle completely or in an optimal way
- the malfunction or errors in automated sequences, which is handled by enabling a detection of faults and by limiting the risk of error following a manual recovery.

Therefore, the shift team needs to keep its knowledge on the system behavior up-to-date and needs current HSI functions (dialogues, information displaying, and controls) and documentation.

Automation is implemented according to predefined general criteria which dictate that significant improvement be identified in plant safety, availability and economics.

5.3.2.1 General Rules

The following tasks, contributing to the previous objectives, are automated regardless of the status of the plant:

- tasks requiring a quick or highly reliable reaction:
 - action credited for beyond design basis events prior to 10 minutes are generally automated. This criterion is based on the Defense-in-depth and diversity (D3) coping analysis. The thermal hydraulic portion of the D3 analysis determines the time available for operator action. The HFE portion of this analysis ensures that manual action within this time can be reasonably expected without human performance errors. In general, experience has shown that actions required after 10 minutes can be justified based on the HFE portion of this analysis. However, any manual actions that cannot be justified by the HFE analysis will be automated.
 - an automatic checking system supports the operator's confirmation task and operator's quick actions after automated systems are actuated.

- actions on components required within short time needed to ensure the plant availability in power operation, or to cope with transients not manageable by closed-loop controls
- tasks which directly influence plant availability (e.g., reduce the time for shutdown and start-up)
- tasks which increase safety by automatic actuation of safety systems
- monotonous and repetitive tasks, leading typically to high workload (if not automated) such as:
 - continuous control of process state variables
 - continuous set-point variations for closed loop control shall be automatic (on request by the operator)
 - start-up of standby components in the case of failures of the running component
 - tasks which have to be performed frequently during shutdown and start-up
- tasks requiring significant operator workload and attention, start-up and shutdown sequences of a main component or a group of components, notably if operator judgment is not needed
- tasks that can be conducted more frequently and accurately through automation, thereby improving plant safety or availability, checking parameters relative to thresholds, e.g., when changing a plant or system state stepwise, with several intermediate steps are supported by automation
- tasks which have to be performed frequently during shutdown and start-up
- tasks which have a long duration, particularly during shutdown and start-up, and therefore require a long duration of operator attention

The criterion above is used as a basis for identifying the minimum tasks that are allocated to automation. In addition, the allocation considers the reduced operating staffing for the US-APWR and for modernized plants, which includes only one SRO and one RO in the MCR as minimum. Therefore, in addition to the minimum level of automation, operator workload is carefully evaluated. Additional automation is generally applied to burdensome functions that do not contribute to an operator's skills in maintaining plant safety or availability. In applying additional automation, careful consideration is given to automation hold points where operator assessment and judgment adds value to the reliability of the process and to the operator's awareness of the plant status.

5.3.2.2 Other Considerations

If line-up of mechanical systems is not considered to be on the critical path for plant start-up, there is no impact on plant operation, and there are no complicated links between the different line-up actions, the corresponding actions are generally not automated.

The following automation rules are also considered when they contribute to the previous stated objectives:

- the automation has to ensure that the plant can be operated by one RO in all plant situations without multiple failures/events
- automation may be appropriate for periodic tests configuration sequences
- automation may be appropriate to standardize frequently used sequences of actions like normal/back-up switching of actuators
- automation may be appropriate to achieve adaptation of systems participating in

- load changes of the plant and needed within a short time span
- automation may be appropriate to perform functions required to change the plant state, failure of which would lead to complicated/time consuming recovery actions
- automation may be appropriate for functions required for change of plant load if manual execution would introduce a significant delay in this change
- automation may be appropriate for functions needed to set up the parameters of the I&C system for stretch-out operation.

5.3.2.3 Taking into Account Operating Experience Review

If most of the plant systems are already designed, stringent automation criteria may induce modifications of the plant systems design. In that situation, case by case review of the plant systems is necessary to ensure that operating experience is incorporated without major modification of the design. In practice, this consideration leads to sticking to existing automation level and modifying it only if strictly necessary in accordance with the experience feedback.

In order to comply strictly with the IEC60964 standard Section 3, the analysis of the sequences to be automated still has to be performed and justified even if they are based on the proven solution of existing plants. Therefore, the criteria listed above are valuable to do this task even if they are not necessarily of a great help to determine how to improve existing design (experience feedback is a much better improvement basis).

5.3.2.4 Priority Order Management for Automation

Adequate priorities between automatic and manual actions ensure that:

- simple erroneous manual actions cannot inhibit automatic plant protection actions, or automatic equipment protection actions;
- the operation staff has an appropriate time for decision making about manual control

The basic rules are:

- automatic plant protection actions and equipment protection actions have priority over manual actions;
- automatic plant protection actions can be blocked (prior to actuation) at the division level following administrative controls and plant technical specifications, and with appropriate bypass alarms and indications. Equipment protection actions cannot be blocked;
- after actuation automatic plant protection actions can be overridden at the component level by taking two deliberate manual actions. In general, equipment protection signals cannot be overridden. However, equipment protection signals that are normally expected due to process conditions (e.g., low tank level stopping a pump to prevent inadequate suction damage) may be overridden by manual signals that require continuous operator attention (e.g., pushing and holding a button continuously);
- automatic plant/equipment protection signals can be reset when the initiating condition is restored to normal or to an appropriate setpoint. Plant protection signals require manual reset; equipment protection signals can be reset

automatically. If the plant/equipment conditions degrade, the signals are automatically initiated again;

- manual actions have priority over closed and open loop process control functions;
- interlocks prevent manual actuation against prior automatic orders.

5.4 Task Analysis

5.4.1 Objective of Task Analysis

The functions allocated to plant personnel define their roles and responsibilities. Human actions (HAs) are performed to accomplish these functions. HAs are further divided into tasks. A task is a group of related activities that have a common objective or goal. The objective of the task analysis is to identify requirements for accomplishing these tasks, i.e., for specifying the requirements for the displays, data processing, controls, and support aids needed to accomplish tasks. (Reference 24 and 13) As such, the results of task analysis are identified as inputs in many HFE activities; e.g., it forms the basis for:

- staffing, qualifications, job design, and training
- HSIs, procedures, and training program design
- task support verification criteria definition

5.4.2 Scope of Task Analysis

The scope of task analysis includes:

- selected representative and important tasks that affect plant safety from the areas of operations, maintenance, test, inspection, and surveillance
- full range of plant operating modes, including startup, normal operations, abnormal and emergency operations, transient conditions, and low-power and shutdown conditions
- HAs (Human Actions) that have been found to affect plant risk by means of probabilistic risk assessment (PRA) importance and sensitivity analyses are also considered risk-important. Internal and external initiating events and actions affecting the PRA Level I and II analyses are considered when identifying risk-important actions
- where critical functions are automated, the analyses considers all human tasks including monitoring of the automated system and execution of backup actions if the system fails.

The task analysis is iterative and becomes progressively more detailed over the design cycle. It is detailed enough to identify information and control requirements to enable specification of detailed requirements for alarms, displays, data processing, and controls for human task accomplishment.

The task analysis addresses issues such as:

- the number of crew members
- crew member skills
- allocation of monitoring and control tasks to
 - 1) the definition of meaningful jobs and
 - 2) the management of crew member's physical and cognitive workload.

The task analysis results are used to define the set of alarms, displays, and controls necessary to perform crew tasks based on both task and instrumentation and control requirements. The task analysis results provide input to the design of HSIs, procedures, and personnel training programs.

5.4.3 Methodology for Task Analysis

Tasks are linked using operational sequence diagrams. Task analyses begin on a high level and involve the development of detailed narrative descriptions of what personnel have to do. The analyses define the nature of the input, process, and output needed by and of personnel. Detailed task descriptions address (as appropriate) the topics listed in Table 5.4-1

Table 5.4-1 Task Considerations

Type of Information	Example
Information Requirements	alarms and alerts parameters (units, precision, and accuracy) feedback needed to indicate adequacy of actions taken
Decision-making Requirements	decisions type (relative, absolute, probabilistic) evaluations to be performed
Response Requirements	type of action to be taken task frequency, tolerance and accuracy time available and temporal constraints (task ordering) physical position (stand, sit, squat, etc.) biomechanics - movements (lift, push, turn, pull, crank, etc.) - force needed
Communication Requirements	personnel communication for monitoring information or control
Workload	cognitive physical overlap of task requirements (serial vs. parallel task elements)
Task Support Requirements	special and protective clothing job aids or reference materials needed tools and equipment needed
Workplace Factors	ingress and egress paths to the worksite workspace envelope needed by action taken typical and extreme environmental conditions, such as lighting, temp, noise
Situational and Performance Shaping Factors	Stress reduced manning
Hazard Identification	identification of hazards involved, e.g., potential personal injury

Task analysis assesses minimum staffing for each operation step. A qualitative assessment will confirm the validity of the analysis for maximum staffing conditions. Time allocations for human actions shall consider the duration of a shift, where decrements in performance due to fatigue may be a concern.

Figure 5.4-1 shows the MHI approach to Task Analysis in the HFE process. The level of design detail is changed as the design progresses. High level Task Analysis is performed in the early design stage and detail level Task Analysis is performed in later design stage (after HSI Design and Procedure Development phase). Although detail level task analysis can be considered as a part of Human Factor V&V process, its methodology is described this section.

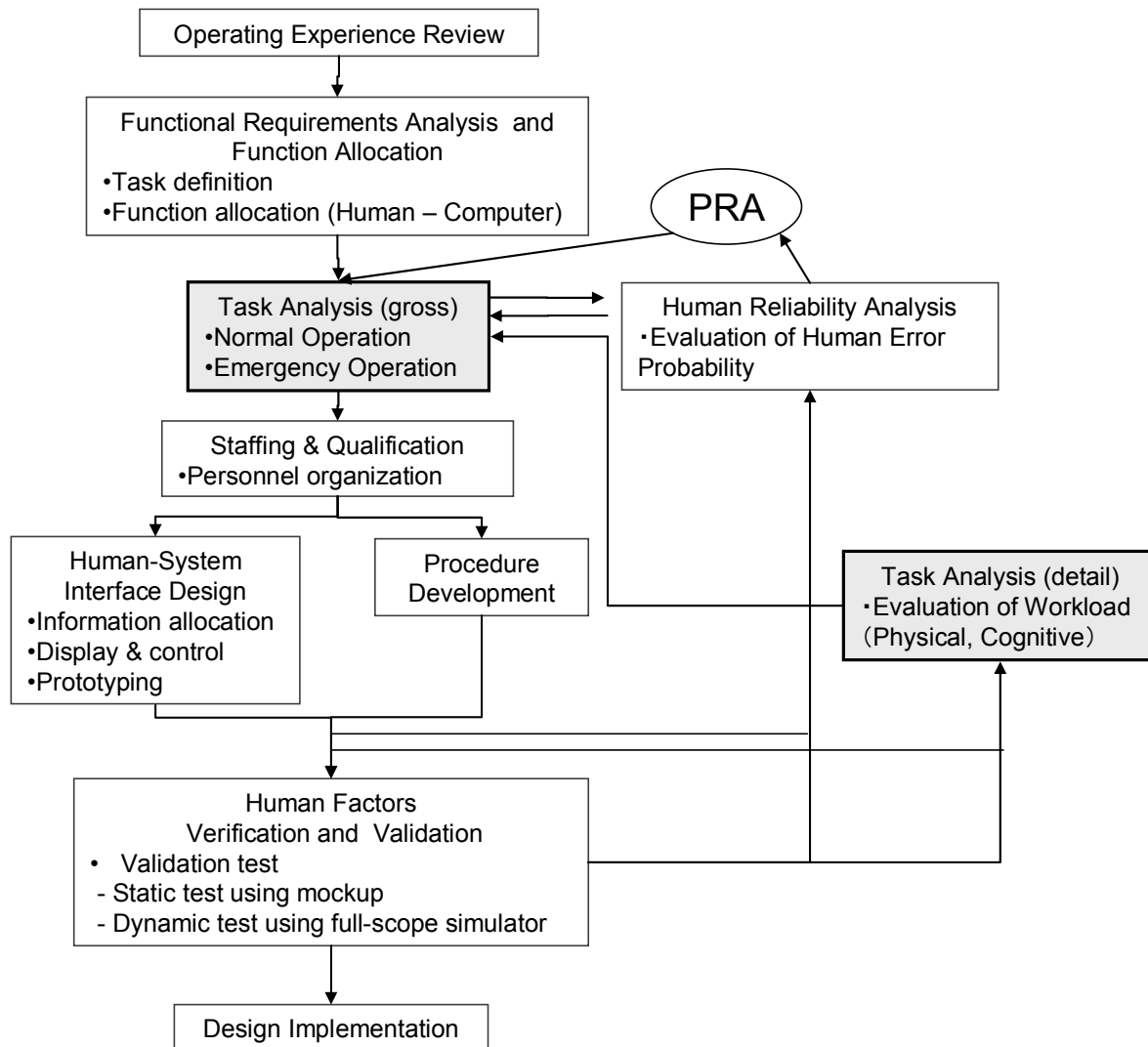
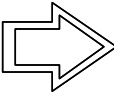
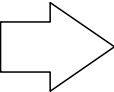

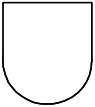


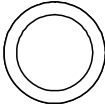
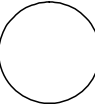
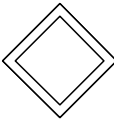
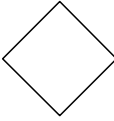
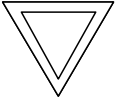
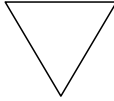


Figure 5.4-1 Task Analysis in HFE Process Flow

5.4.3.1 Method for Gross and Narrative Task Analysis Method

The operational sequence diagram (OSD) is an analysis technique that can be used from the initial design phase to the final design phase.

The OSD represents operator and computer tasks in graphical scheme sequentially. The symbols for OSD are shown in Figure 5.4-2. Through the use of symbols to indicate actions, data transmitted or received, inspections, operations, decisions and data storage, the OSD shows the flow of information through a task. The information flow is shown in relation to both time and space. If detailed information on a given action is needed, code letters (S, V, W, T) may be used to indicate the mode of actions. The OSD is used to develop and present the system reaction to specified inputs. In the OSD, the interrelationships between operators and equipment (including computers for human-machine interfaces) are easily displayed. Operator activities are sequentially categorized. Decision and action functions are clearly identified, and task frequency and load become obvious.

SHAPE			CODE	
MACHINE	HUMAN	ACTION	LETTER	MEANING
		Transmit	S	Sound
		Receipt	V	Visual
		Inspect	W	Walking
		Operate	T	Touch
		Decision		
		Storage		

* A code letter may indicate Mode of shapes

Figure 5.4-2 Symbols Used in Operational Sequence Diagram (OSD)

The OSD corresponding to each task is constructed by the following steps:

- Step 1 : Description of task scenario
 - Represent elements of task in simple linguistic form
 - Select appropriate detail level in design phase
- Step 2 : Breaking down job task into individual activities
- Step 3 : Activity assignment to human and machine
 - Use the result of Function Allocation
 - Assign each activity to operator or machine
- Step 4 : Description of activity sequence for functions assigned to operator

Table 5.4-2 shows an example of data entry in a Task Analysis Sheet which is used to record the analysis results. Fields in this table are described below:

- Operating Procedure Field: Full task contents are described in task sequence.
- OSD Description Field: Human and machine actions are represented using OSD symbols.
- Task Description Field: Key information of task execution such as plant parameter, alarm, control.
- Note Field: Remark for task execution.

An example of the OSD representation is shown in Table 5.4-2. In the column “OSD Task Description”, the contents of task are described as activities in simple form. Activity description is broken down into individual actions (OSD symbols) such as ‘Transmit’, ‘Receive’, ‘Inspect’, etc. Each action is located in appropriate column (Human: senior reactor operator or reactor operator, Machine: displays and controls) according to the output of the Function Allocation process. Finally all actions are connected to each other to represent the temporal sequence of the elements of the task.

Task Analysis sheets are developed for the full range of plant operating modes, including startup, normal operations, abnormal and emergency operations, transient conditions, and low-power and shutdown conditions. Table 5.4-3 shows an example data form of Task Analysis Summary Sheet. Each task analysis result for plant operation mode is summarized in this format, and these sheets are used for the evaluation of human workload. Fields in Table 5.4-3 are described below.

- Activity Field: Description of the work activity for plant system (Primary Loop/Secondary Loop/Electric System)
- Communication, Monitoring, Decision, Operation Field: Number of each OSD actions (receive, transmit, operate, inspect)
- Parallel Monitoring Field: Number of plant parameters that are necessary to monitor simultaneously for execution of an activity.
- Parallel Operation Field: Number of operations that are executed simultaneously in an activity
- Necessary Time Field: Estimated execution time of an activity

Table 5.4-2 Example of Task Analysis Sheet

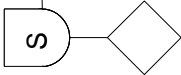
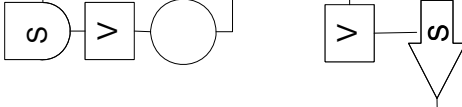







Operating Procedure	OSD Description				Task Description	Note
	Supervisor Reactor Operator	Reactor Operator	Displays Controls	Other Personnel		
Confirm ANN					Read ANN information	
1. ANN Occur					Display plant parameters	
2. Confirm plant status					Communicate via voice	
3. Report plant status from RO to SRO					Decide plant trip or not	
4. Decide plant trip or not						

Table 5.4-3 Task Analysis Summary Sheet

Activity	Primary Loop	Secondary Loop	Communication				Monitoring		Decision	Operation	Parallel Monitoring	Parallel Operation	Necessary Time
													
1.	Confirm ANN		2	1	0	1	2	1	0	0	0	0	Within 1 min
2.	Recovery Operation		3	4	2	11	25	0	5	5	0	0	Within 10 min

5.4.3.2 Detailed level Task Analysis Method

In order to evaluate an operating crew member's cognitive workload, an interaction analysis between human and computer system is necessary. To analyze cognitive workload MHI uses human information processor model. In a detailed level task analysis phase, task scenarios which are selected in the gross level task analysis are analyzed by human information processor model. The OSD actions are broken down into their constituent components and are evaluated with HSI design information. The result of the task analysis is a set of quantitative metrics such as memory workload and processing time for each scenario. The task analysis is iterative and becomes progressively more detailed over the design cycle. It is detailed enough to identify information and control requirements to enable specification of detailed requirements for the HSI design.

Goals, operators, methods, and selection rules (GOMS) is a theory of the cognitive skills involved in human-computer tasks. GOMS is used only for tasks that meet all of the following criteria:

1. Significant changes from the reference design or tasks where there is no operating history in the reference design.
2. Where the tasks are identified as risk significant through the HRA element.
3. Where the task is time critical.

GOMS is a technique similar to operational sequence diagrams. The GOMS analysis is based on preliminary operating procedures. Figure 5.4-3 shows a model for a human information processor. (Reference 8) This method is described in the reference document "The Psychology of Human-Computer Interaction". It is based upon an information processing framework that assumes a number of different stages or types of memory (e.g., sensory store, working memory, long term memory) with separate perceptual, motor, and cognitive processing.

- Perception processor (t_p : mean processing time = 100msec)
 - sensory input (audio & visual) and code information symbolically
 - output into audio & visual image storage (Working Memory)
- Cognition Processor (t_c : mean processing time = 70msec)
 - input from Working Memory and Short Term Memory
 - access Long Term Memory to determine response
 - output response into Working Memory
- Motion Processor (t_m : mean processing time = 70msec)
 - Input response from Working Memory
 - carry out response

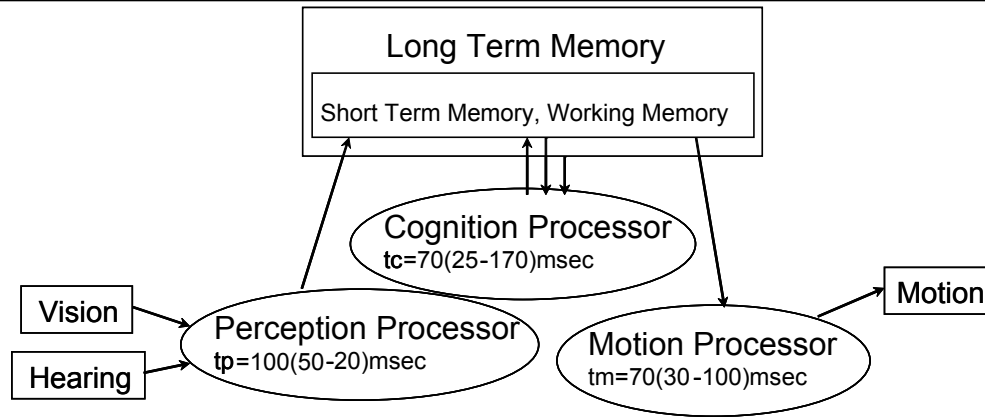


Figure 5.4-3 Model of Human Information Processor by Card et al.

Table 5.4-4 Extended Human Information Processing Model

Basic Action	Abbreviation	tp	tc	tm
simple reaction	sr	1	1	1
physical match	pm	1	2	1
name match	nm	1	3	1
class match	cm	1	4	1
move	mo	0	1	1
simple reaction without move	sr*	1	0	0
physical match without move	pm*	1	1	0
name match without move	nm*	1	2	0
class match without move	cm*	1	3	0
memory refer	mr	0	1	0

Human actions can be classified into several basic actions. Table 5.4-4 shows the relationship between basic actions and process times (tp, tc, tm). Card proposed four basic action types (simple reaction: sr, physical match: pm, name match: nm, class match: cm). MHI uses extended basic action to analyze VDU based monitoring and operation. Six basic actions (move: mo, simple reaction without move: sr*, physical match without move: pm*, name match without move: nm*, class match without move: cm*, memory refer: mr) are added to original basic actions. Total processing time for each basic action is calculated by using factor shown in Table 5.4-4. For example, typical processing time for a simple action (TP(sr)) is calculated as follows;

$$TP(sr) = 1*tp + 1*tc + 1*tm = 100 + 70 + 70 = 240 \text{ msec}$$

Table 5.4-5 shows an example of Detail Task Analysis Sheet which is used to record analysis result. Fields in this table are described below.

- Step Field: Simple description of the task step
- Personnel Field: Who perform this step?
- Equipment Field: Which information device is used for this step?
- Operation Field: Description of task step is broken down into its constituent operations.
- Information Processing Type Field: GOMS basic action corresponding to each primitive operation.
- Cognitive Workload Field: Factors for information processing type

Selected scenarios are analyzed in this form, and quantitative metrics are gathered as detailed level analysis results. This information is used for evaluating the HSI design.

Table 5.4-5 Example of Detail Task Analysis (Workload) Sheet

Task Name: Safety Injection ANN Check						Cognitive Workload		
STEP	Personnel	Equipment	Operation	Information Processing Type	tp	tc	tm	
1. Confirm first out ANN	RO	Large Display	ANN occurrence(Confirm) Look at LDP Search first out ANN display Confirm first out ANN	pm* mo mr+pm* nm*	1 0 1 1	1 1 2 2	0 1 0 0	
2. Confirm safety injection ANN	RO	Large Display	Search safety injection ANN display Confirm safety injection ANN	mr+pm* nm*	1 1	2 2	0 0	
3. Confirm reactor trip ANN	RO	Large Display	Search reactor trip ANN display Confirm reactor trip ANN	mr+pm* nm*	1 1	2 2	0 0	
4. Confirm turbine trip ANN	RO	Large Display	Search turbine trip ANN display Confirm turbine trip ANN	mr+pm* nm*	1 1	2 2	0 0	
					9	18	1	

5.5 Staffing and Qualification Requirements

The plant specific report for the Staffing and Qualifications program element will define the staffing and qualifications for personnel that perform operations or maintenance tasks directly related to plant safety. Tasks directly related to plant safety are addressed in this analysis for the full range of plant operating modes, including the following:

- Startup I Shutdown
- Normal operations
- Abnormal and Emergency operations
- Transient conditions

The scope of tasks covered by the analysis includes operational tasks, plant maintenance tasks, and plant surveillance and testing. The report will define the basis for the staffing numbers and qualification requirements, with justification for changes from the US-Basic HSIS. Staffing will be confirmed through Task Analysis and V&V program elements.

5.5.1 Operator Staffing Level

Operator staffing is based on the following three qualifications;

a. Senior Reactor Operator (SRO)

SROs are licensed pursuant to 10 CFR Part 55.54 "Operators". Shift Supervisor (SS) is a licensed SRO and is responsible for the plant's operation for the duration of the shift.

b. Shift Technical Advisor (STA)

A degreed engineer who has fulfilled the course requirements and operator training requirements defined in NUREG-0737 TMI Action plan.

c. Reactor Operator (RO)

A RO is licensed pursuant to 10 CFR Part 55.54 "Operators".

5.5.2 Number of Operators per Shift

10 CFR 50.54(m) defines the minimum requirement of operator staffing as follows;

- 1 SRO located within the MCR
- 1 SRO located at the plant
- 1 RO located at the controls of the plant in the MCR
- 1 RO located at the plant

In addition, NUREG-0737 requires one STA located at the plant. NUREG-0737 allows an SRO to also fulfill this requirement if the SRO also has an engineering degree with the appropriate course background.

Based on these requirements, the minimum operator staffing roles and responsibilities that are the basis for the US-APWR design are defined as follows.

- One RO at the controls of the plant within the MCR at all times. This RO is typically located at the Operator Console.
- At least one more RO present at the facility during its operation in order to shift above RO's temporary absence because of the meal time or sudden injury, etc. for redundancy and for abnormal conditions, including anticipated operational occurrences(AOOs), DBAs and degraded HSI conditions discussed in Section 4 above. This RO can also be accommodated at the Operator Console, but continuous presence in the MCR is not required.
- One SRO within the MCR at all times. This is typically the control room supervisor. The SRO is typically located at the Supervisor Console.
- At least one more SRO present at the facility during its operation in order to shift above SRO's temporary absence because of the meal time or sudden injury, etc. for redundancy. This SRO position is typically fulfilled by the Shift Supervisor of the plant. This SRO is typically located in an office which is in close proximity to the MCR. For minimum staffing, this SRO also fulfils the STA requirement. However, a separate STA may also be designated. The HSI design accommodates the STA at a separate STA Console within the MCR.

The US-APWR is designed to be operated in normal operation by one SRO and one RO in the MCR. Other operating staffs available at the plant augment the minimum staff during abnormal plant conditions and degraded HSI conditions. The following activities have been demonstrated based on the above staffing basis:

- Task Analysis
- Human Reliability Analysis
- HSI design (including MCR layout)
- Verification and Validation

The minimum operator staffing structure is as shown in the following figure;

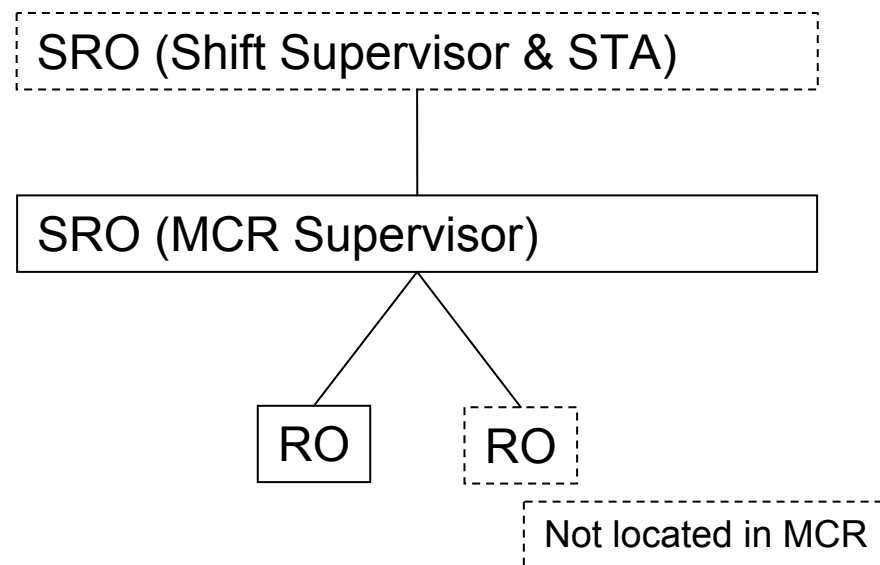


Figure 5.5-1 Operation Personnel Staffing and Organization (Minimum)

The HSI design of the US-APWR also accommodates other staffing structures, including the following maximum continuous staffing in the MCR.

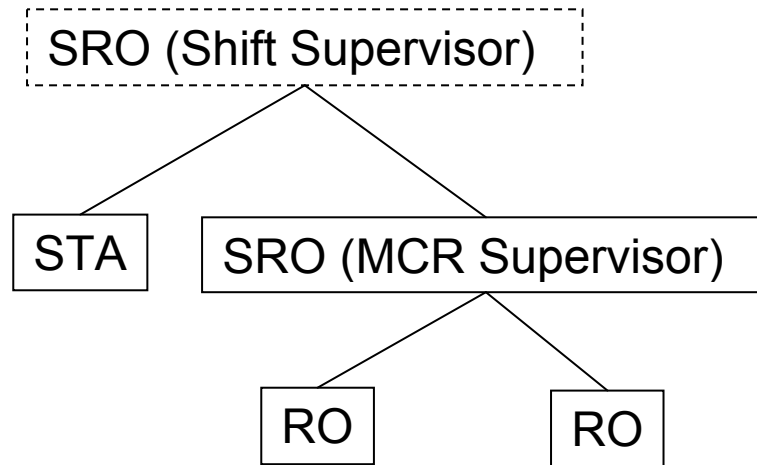


Figure 5.5-2 Operation Personnel Staffing and Organization (Typical)

5.6 Human Reliability Analysis

5.6.1 Objectives of HRA

Human reliability analysis (HRA) seeks to evaluate the potential for, and mechanisms of, human errors that may affect plant safety. Thus, it is an essential element in achieving the HFE design goal of providing a design that minimizes personnel errors, allows their detection, and provides recovery capability. (References 12, 23 and 41)

5.6.2 Scope of HRA

The HRA is conducted as an integrated activity to support both the HFE design and PRA activities. Figure 5.6-1 illustrates the relationship between the PRA/HRA and the rest of the HFE program, including the concept of performing an initial PRA/HRA and then a final one at completion of design. The quality of the HRA depends in large part on the analyst's understanding of personnel tasks, the information related to those tasks, and the factors that influence human performance of those tasks. The development of information to facilitate the understanding of the causes and modes of human error is an important human factors activity. The HRAs make use of descriptions and analyses of operator functions and tasks as well as the operational characteristics of HSIs. HRA can provide valuable insights into the desirable characteristics of the HSI design. Consequently, the HFE design gives special attention to those plant scenarios, risk-important human actions, and HSIs that have been identified by PRA/HRA as being important to plant safety and reliability.

The HRA is performed iteratively as the design progresses. The PRA and HRA are performed early in the design process to provide insights and guidance both for systems design and for HFE purposes. The robustness of the HRA depends, in large part, on the analyst's understanding of personnel tasks, the information related to them, and the factors which influence human performance. Accordingly, the HRA is carried out interactively as the design progresses.

As described in NUREG-1764, initial risk screening process is a part of PRA activities. Input information for HRA includes risk-important human action and result of task analysis process. Quantitative analysis of human errors is carried out using such input information from the cognitive viewpoint. If new risk-important human action is found in HRA, the feedback information is provided for PRA.

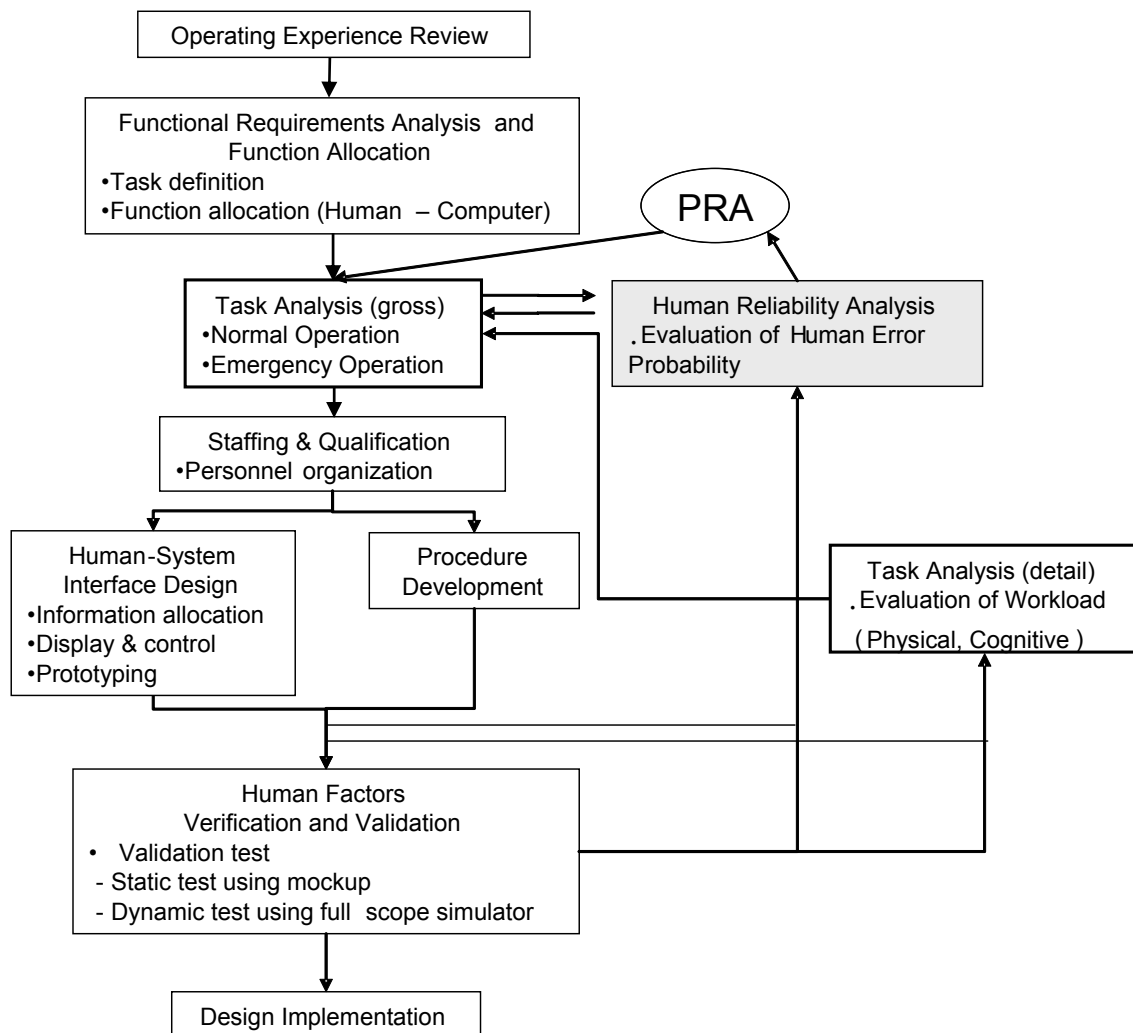


Figure 5.6-1 HRA in HFE Process Flow

5.6.3 HRA Methodology

HRA has focused on omission of human error, but recent studies indicate that the analysis from the cognitive viewpoint is also important in preventing human errors, especially in some contexts where it affects the occurrence of commission errors. MHI uses the technique for human error rate prediction (THERP) for the analysis of human errors.

THERP method was developed by Swain and Guttmann and documented as NUREG/CR-1278 in 1983. THERP method is used most widely for basic HRA. In the THERP handbook, the types of human error are summarized as data tables with standard occurrence probabilities assigned to each.

The fundamentals of THERP are shown in Figure 5.6-2. The procedure is divided into four fundamental steps. The first step is to investigate the objective task, divide it into detailed task

steps and form a success-fail binary tree, a so-called event tree. The second step is to select a corresponding basic human error probability (BHEP) from the associated database for each step. An example of the table is shown in the right half of Figure 5.6-2. The third step is to modify the BHEP for specific situations by multiplying it by a value of the performance shaping factor (PSF), which is in the range of $1/EF$ to EF (Error Factor), reflecting the influence of human factors. EF , meaning the error factor, is a numeral defined for each type of task in the table of the THERP. The modified value is called the human error probability (HEP). The final step is to calculate the HEP through the task.

THERP is founded on the notion that human errors are induced by not only the difficulty of the operation but also the working conditions. Conversely, human errors might be reduced by improvement of the factors concerning the PSF, for example easy-to-read manual, freedom from stress, etc. In other words, human errors depend on the conditions or background under which the operation is performed.

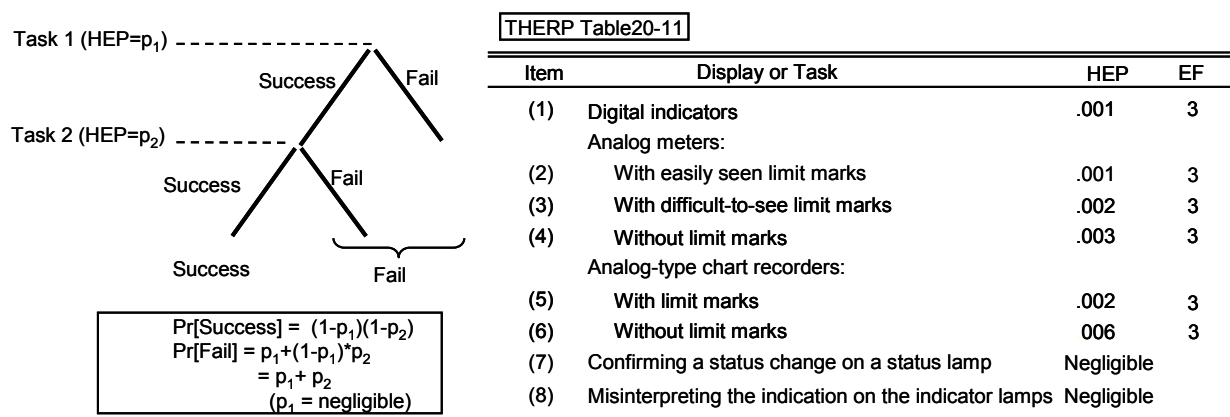


Figure 5.6-2 HEP Evaluation in THERP

5.6.4 HRA using THERP

HRA sheets are prepared for tasks corresponding to risk important HAs. Table 5.6-1 shows the data entry in an HRA sheet. Fields in Table 5.6-1 are described below.

- Step Field: Task step number; each task step contains several activities
- Personnel Field: Reactor Operator (RO) or Senior Reactor Operator (SRO)
- Display, Controls Field: Equipment used for task step
- Activity Field: Detailed task description, task step is composed from activity
- Primary Action field :

Omission Error

IA (Initiate Action)

OS (Omit Step)

Commission Error

SD (Select Display)

SC (Select Control)

RV (Read Value)

CR (Check Read)
RT (Read Text)
IC (Incorrect Calculation)
OC (Operate Control)
AC (Arithmetic Calculation)

- Action Type field:

PU (Perceptual Unit), SA (Separate Action)

- Recognition and confirmation of ANN : IA + SD=PU (message type)

RT=SA

:IA + SD + CR=PU(window type)

- Read and check value : SD+CR=PU

RV=SA

- Confirmation of switch status : SC+CR=PU

- Confirmation of status lamp : SD+CR=PU

- Calculation : SD=SA

IC=SA

- Operation : SC+OC=PU (on-off type control)

: SC=SA (multi selection control)

- H.E Element Field: HSI design information for human error table selection

L: Selection using label

F: Grouping is used in HSI design

U: Location of information is easily identified

- H.E Table Field: Table number in THERP handbook (NUREG/CR-1278)

- Standard H.E Field: Value of basic HEP which is determined by Action Type and H.E Element information

- Adjust Factor Field: Description of dependency (High Dependency :HD, Low Dependency : LD)

- Modified H.E Field: Basic HEP x EF(Error Factor) or DF(Dependency Factor)

- CAL Field: Description of calculation method

- HEP Field: Value of HEP calculated by specified method

- EF Field: Value of Error Factor

- SF Field: Value of Stress Factor

- Final HEP: Final value of HEP

THERP has been used as standard HRA method for 20 years since the early days of the development of Japanese PWR main control room by MHI, MELCO and Japanese PWR power utilities.

5.6.5 HRA Integration

Risk-important HAs are integrated into the HFE program as follows:

- Risk-important HAs and their associated tasks and scenarios are specifically addressed during function allocation analyses, task analyses, HSI design, procedure development, and training development. Proper consideration of HAs helps verify that these tasks are well supported by the HSI design and can be executed within acceptable human performance capabilities (e.g. within time and workload requirements).
- The HFE design team characterizes risk-important human-system interactions by identifying the performance shaping factors (PSF). The team then applies HFE guidelines to the HSI to optimize the PSF, thereby enhancing the overall human success probability.
- HRA assumptions such as decision-making and diagnosis strategies for dominant sequences are validated by walkthrough analyses with personnel with operational experience using a plant-specific control room mockup or simulator. Reviews are conducted before the final quantification stage of the PRA as part of the V&V process.
- The V&V Team ensures V&V activities are designed to specifically address human performance for risk-significant HAs. The verification analysis is most rigorous for HSI that supports tasks shown by the HRA to be risk significant. Verification includes operating procedures and training material. In addition, the validation scenarios encompass all human actions shown by the HRA to be risk significant. Validation encompasses the complete HSI design, including operating procedures, and is conducted with operators that have been trained in accordance with the HFE training program. Human performance for risk significant HAs is specifically monitored during validation scenarios.

Table 5.6-1 Example of Human Reliability Analysis Sheet

Task Name :												
Step	Personnel	Display, Controls	Operation	Primitive Action	Action Type	H.E. Element	H.E. Table	Standard H.E.	Adjust Factor	Modified H.E.	CAL	HEP
1.	RO-1 SRO	H/W ANN	Ann (Confirm) Read first out ann Safety Injection Reactor Trip Turbine Trip Ann Ann Ann	IA SD CR	IA+SD+CR=PU		20-23 #3	0.0010	LDa	0.0010 0.05.00	*	0.0001
2.	RO-1 SRO	CRT (AUTO)	Confirm plant trip status (System check) Reactor Trip Turbine Trip Dual Check	OS 2SD 2CR CR	IA 2SD+2CR=2PU CR=SA		20-7 #5. 20-5.#6 20-11#8 20-11#8	0.0100 0.0010 0.0010 0.0010	LDa ZD LD	0.0100 0.05.00 0.0010 0.0010	* * *2 *	0.0000 0.0001 0.0001
3.	RO-1 SRO	CRT (AUTO)	Confirm safety injection status and CV isolation (System check) Safety Injection CV Isolation Dual Check	OS SD*5. CR*10 CR	IA 5.SD+10CR =5.OPU CR=SA		20-7#5. 20-5.#6 20-11#8 20-11#8	0.0100 0.0010 0.0010 0.0010	LDa ZD LD	0.0100 0.05.00 0.0010 0.05.00	* * *5. *	0.0000 0.0003 0.00025.
4.	RO-1 SRO	"RCP Trip "ANN (A,B,C,D) RCP Control SW	Confirm RCP status (System check) Confirm "RCP Trip "ANN (*4) Confirm RCP status (*4) (GREEN)	OS SD*4 CR*4 CR*4	IA 4SD+4CR=PU 4SD+4CR=PU	F	20-7#5. 20-5.#6 20-11#8 20-12#3	0.0100 0.0010 0.0010 0.0010	LDa ZD MD	0.0100 0.05.00 0.0010 0.15.00	* * * *	0.0000 0.0002 0.00015.
5.	RO-1 SRO	CRT	Confirm RCS pressure (System check) Read PRZ pressure value and history data	OS SD RV/CR	IA SD=SA RV+CR=PU		20-7#5. 20-5.#6 20-9#3 20-10#2	0.0100 0.0010 0.0010 0.0010	LDa ZD	0.0100 0.05.00 0.0010 0.0010	* * +	0.0000 0.0020 0.01000

:(1/N)

5.7 HSI Design

5.7.1 HSI Design Objective

The HSI design process represents the translation of function and task requirements into HSI characteristics and functions. The HSI is designed using a structured methodology that guides designers in identifying and selecting candidate HSI approaches, defining the detailed design, and performing HSI tests and evaluations. The methodology includes the development and use of HFE guidelines, e.g., a style guide to define the design-specific conventions. The availability of an HSI design methodology helps verify standardization and consistency in applying HFE principles. (References 24, 18, 19 and 20)

5.7.2 Scope of HSI Design

The HFE program encompasses the HSI used by operators and operations support personnel in the MCR, RSR, TSC and EOF. In addition, the program encompasses HSI in local areas of the plant which supports:

- On-line testing, radiological protection activities, and required chemical monitoring supporting technical specifications
- Maintenance required by technical specifications
- Emergency and abnormal conditions response

The concept of operations is as described in Section 4.1, and includes:

- Crew composition (Section 4.1.f)
- Roles and responsibilities of individual crewmembers (Section 4.1.g)
- Personnel interaction with plant automation (Sections 4.1.a, 4.1.b, 4.1.e)
- Use of control room resources by crewmembers (Sections 4.1.c and 4.1.d)
- Methods used to ensure good coordination of crewmember activities, including non-licensed operators, technicians, and maintenance personnel. These coordination tools/methods include:
 - Large display panel (LDP) (Section 4.9)
 - LCSs (Section 4.2.5)
 - Tagging (Section 4.5)

In addition, distribution of plant data via the unit bus and the plant station bus is described in MUAP-07004. Voice communications systems and video communications systems, such as industrial television (ITV), are described in plant licensing documentation.

The concept of operations is encompassed by the functional requirements report and staffing report which are the output of Sections 5.3 and 5.5, respectively. These reports focus on changes from the reference design(s), which are determined primarily from the OER in Section 5.2. The Task Analysis from Section 5.4 is the primary input to design of the HSI inventory. That inventory is implemented within the HSI features, described in Section 4 and in accordance with the design details documented in the Style Guide. The style guide is developed based on historical practices, changes as needed per the OER, and in conformance to the guidance of NUREG-0700. HRA identifies the portion of the HSI design that requires special attention during all phases of the HFE program, including V&V. The HSI

design is documented as described in Section 5.7.3.3. Testing and evaluation of the HSI design is described in the Verification and Validation phase of the HFE program, as described in Section 5.10.

5.7.3 HSI Design Methodology

The concept and design description of Mitsubishi's standard HSI system (i.e. the US Basic HSI) are described in Section 4.0. The US Basic HSI is a direct evolution from the Japanese Standard HSI Design. It is not a new design concept. The minor differences in the US Basic HSI design have been the result of the Phase 1 V&V program conducted with US operators, as described in Appendix C. Human performance issues identified from operating experience with the predecessor design are tracked as HEDs and are monitored and resolved as part of the plant specific HFE process. In this section, the methodology of HSI design to guide designers in the development of the HSI inventory for the plant specific HSI system is explained.

The basic functional requirements for the HSI design described in Section 4.0 are identified in Reference 24 IEC-60964 Chapter 4, "Functional Design Specification" with additional analytical detail provided in Appendix A, "Design Guide for Control Rooms," Section A.4. During the plant specific design process the functional requirements for the plant specific HSI inventory are added reflecting the output from the task analysis, including alarm, information and control content and characteristics for specific displays.

5.7.3.1 Input Information to HSI Design Process

The following sources of information provide input to the HSI design process:

- Analysis of Personnel Task Requirements - The analyses performed in earlier stages of the design process (operational experience review, functional analysis and function allocation, task analysis, staffing) are used to identify requirements for the HSIs.
- System Requirements - Constraints imposed by the overall instrumentation and control (I&C) system are considered throughout the HSI design process. These constraints are understood by the HSI design team based on the interdisciplinary skills and training identified in Section 5.1.2.2.
- Regulatory Requirements - Applicable regulatory requirements are identified as inputs to the HSI design process.
- Operational experience review – Lessons learned from other complex human-machine systems, especially predecessor designs and designs involving similar HSI technology are used as an input to HSI design.
- Functional requirement analysis and function allocation – The HSIs support the operator's role in the plant (e.g., appropriate levels of automation and manual control).
- Task analysis – The set of requirements to support the role of personnel is provided by task analysis. The task analysis identifies:
 - Tasks that are necessary to control the plant in a range of operating conditions for normal through accident conditions
 - Detailed information and control requirements (e.g., requirements for display range, precision, accuracy, and units of measurement)
 - Task support requirements (e.g., special lighting and ventilation requirements)

- Risk-important HAs and their associated performance shaping factors, as identified through HRA, are given special attention in the HSI design process.
- Staffing/qualifications and job analyses – The results of staffing/qualifications analyses provide input for the layout of the overall control room and the allocation of controls and displays to individual consoles, panels, and workstations. This establishes the basis for the minimum and maximum number of personnel to be accommodated and requirements for coordinating activities between personnel.
- Other Requirements – Other plant specific requirements are identified from plant specific documentation and used as inputs to the HSI design. Plant specific documentation includes, for example, electrical and mechanical flow diagrams, functional diagrams, tech manuals, design bases documents, setpoint and operating range documents, accident analysis, the D3 coping analysis, etc.

In the HSI design phase, a concept of operations is developed indicating crew composition and the roles and responsibilities of individual crew members based on anticipated staffing levels. Functional requirements for the HSIs are developed to address the concept of operations, personnel functions & tasks and personnel requirements. The functional requirement specification would serve as the initial source of input to the HSI concept design. Design-specific HFE design guidance (style guide) is developed in the HSI detailed design and integration phase. Testing and evaluation of HSI designs is conducted throughout the HSI development process and evaluations would be performed iteratively. The methodology used for testing includes the trade-off evaluations for various HSI elements and performance-based tests.

Issues from all program elements that may impact the basic HSI design features, as described in Section 4, are entered into the HFE Issues Tracking System. These issues are tracked to closure through completion of the HSI design process. Other outputs of previous program elements provide input to development of the plant specific HSI inventory (i.e., alarms, indications, controls, and procedures).

The output of the preceding process is input for the HSI design process. Input information includes functional requirement of operation, result of PRA, result of HRA, performance requirement for personnel, various regulatory requirement.

5.7.3.2 HSI Detailed Design and Integration

HSI system in the MCR is composed from operator console, large display panel, diverse HSI panel, supervisor console, safety technical advisor console, data management console. MHI uses style guide to keep design consistency between various computer displays. The style guide conforms to NUREG-0700.

The style guide includes following items:

- Guideline for general display format
- Guideline for display element
- Display design policy

Guideline for general display format includes following:

- Display design consistency
Consistent interface design conventions are evident for all display features, and displays are consistent in word choice, format, and basic style with requirements for data and control entry. There is an explicit mapping between the characteristics and functions of the system to be represented and the features of the display representation.
- Understandability of Information
Information is displayed consistently according to standards and conventions familiar to users. The characteristics and features of the display used to represent the process are readily perceived by the operator. The methods by which lower-level data are analyzed to produce higher-level information and graphical elements are understandable to users.
- Grouping of Information
Related information is organized into groups. Information that must be compared or mentally integrated is presented in the close spatial proximity and use similar physical dimensions to convey meaning. If information needs to be mentally integrated, similar color codes are used for the information items.
- Readability of Information
Important display elements and codes are identifiable and readable from the maximum viewing distance and under minimal ambient lighting conditions. Coding shall not interfere with the readability of displayed information.
- Distinctive Coding
Distinctive means of coding/highlighting is used when a user's attention needs to be directed to changes in the state of the system, critical or off-normal data, and hazardous conditions. When a graphic display contains some outstanding or discrepant feature that merits attention by a user, supplementary text is displayed to emphasize that feature.
- Uncluttered Displays
Displays are as uncluttered as possible.
- Indication of Display
A display feature is provided to indicate to the user that the system is operating properly. Information system failures (due to sensors, instruments, and components) result in distinct display changes, which directly indicate that depicted plant conditions are invalid.
- Display Update Rate Requirements
The maximum update rate is determined by the time required for the user to identify and process the changed feature of the display.

Guideline for display elements includes following:

- Character
Rule for using character in title, message and label is provided, and guideline includes appropriate character size, height-to-width ratio.
- Labels
Each aspect of a display (e.g., data group, field, or message) contains a distinct, unique, and descriptive label.
- Color
Where color is used for coding, it is employed conservatively and consistently. Table 5.7-1 shows the example of color coding rule.
- Tables and Lists
Information is organized in some recognizable logical order to facilitate scanning and assimilation. A table is constructed so that row and column labels represent the information a user has prior to consulting the table. Labels include the unit of measure for the data in the table; units of measurement are part of row or column labels.
- Graphs
Graphs convey enough information to allow the user to interpret the data without referring to additional sources. When multiple curves are included in a single graph, each curve is identified directly by an adjacent label, rather than by a separate legend.
- Mimics
Mimics and diagrams contain the minimum amount of detail required to yield a meaningful pictorial representation. All flow path line origin points are labeled or begin at labeled components. All flow path line destination or terminal points are labeled or end at labeled components. Flow directions are clearly indicated by distinctive arrowheads. Where symbols are used to represent equipment components and process flow or signal paths, numerical data is presented reflecting inputs and outputs associated with equipment.
- Icons and Symbols
The primary use of icons in graphic displays is to represent actual objects or actions. Icons are designed to look like the objects, processes, or operations they represent, by use of literal, functional, or operational representations. Icons are simple, closed figures when possible. Special symbols to signal critical conditions are used exclusively for that purpose. Table 5.7-2, 3 shows the example of component symbols.

Display design policy includes the following:

- Operation console display
The display of soft controls allows users to quickly assess the status of individual components of a control system and their relationships with other components. Displays are designed to avoid occurrence of misunderstanding of plant status. Soft controls and related process information are integrated in one display.
- Large display panel
Large display panel provides continuously visible process information. The display consists of fixed information display area and flexible display area. The fixed display area continually provides plant information in fixed locations, and the variable display area displays screens selected by the operator or automatically displays related operational VDU screens.

- Alarm display
All alarms are displayed in system categories (primary systems, a turbine system and an electrical system) and displayed in each display area in chronological order with color code, blinking and audible tone.

The HSI detailed design process, which integrates the plant specific HSI Inventory using the Basic HSI design features, including the HSI style guide, ensures the following, for both new plant and plant control room upgrades:

- The HSI design supports personnel in their primary role of monitoring and controlling the plant, while minimizing the demands associated with interface management. The operational visual display units (VDUs) provide access to all information and controls, both Safety and Non safety. The LDP provides a continuous display to support situation awareness and crew interaction and coordination for all modes of operation.
- The HSI design addresses the safety parameter display system (SPDS) parameters referenced in 10 CFR 50.34(f)(2)(iv). The LDP provides continuous display for the status of all critical safety functions and the plant systems used to control those safety functions. The electronic procedure system supports execution of the functional recovery EOPs.
- The HSI design minimizes the probability of error in the performance of risk-important HAs and provides the opportunity to detect errors, if they should occur. There are a minimum of two actions required for all controls, to reduce the potential for erroneous operator actions, which may cause a transient. In addition, operational VDU displays are designed to support credited manual operator actions for event-based mitigation.
- All control functions are accessible in the main control room and no LCS controls are credited for normal operation or accident condition operator response under normal HSI conditions. The basis for the control room layout, and the organization of HSIs within consoles, panels, and workstations – the MCR is designed to support the range of crew tasks and staffing (MCR layout is discussed in Section 4.3.1); operational VDUs which are used during all normal and emergency modes of operation are centrally located.
- The control room supports a range of anticipated staffing situations. The design accommodates minimum and typical staffing, as described in Section 5.5; in addition, sufficient space is available to accommodate shift turnover transitions.
- The HSI characteristics, including lighting, ergonomics and layout design, mitigate excessive fatigue. The HSI characteristics support human performance under a full range of environmental conditions. The control of the control room environmental conditions, including emergency lighting, ventilation, and control room habitability, are discussed in plant licensing documentation.
- Inspection, maintenance, tests, and repair of HSIs can be accomplished without interfering with other control room tasks and without impacting plant control functions.
- The strategies for gathering and processing information and executing actions, are consistent with the needs identified in the task analysis.

- The relationships between plant systems are clearly and accurately depicted through the graphic displays presented on the Operational VDUs and the LDP.

The specific alarms, indications, controls and procedures, which compose the HSI system, are defined based primarily on the HSI inventory requirements resulting from the Task Analysis. The resulting HSI inventory is configured based on the HSI features of the US Basic HSIS described in Section 4, with specific graphic displays designed in accordance with the Style Guide. The integrated components of the HSI system are verified and validated, as described in Section 5.10. Verification activities utilize static HSI simulation tools. Validation activities employ full scale dynamic simulators.

The style guide encompasses the subset of NUREG-0700 guidance that is applicable to the HSI features described in Section 4.

The layout for panels with conventional HSI devices (eg. alarms, indicators, controls) should follow historical practices which arrange alarms at the top of the panel, indicators in the middle and controls in the lower section. This historical practice typically supports importance, frequency of use, and sequence of use.

5.7.3.3 HSI Tests and Evaluations

Testing and evaluation of HSI designs are conducted throughout the HSI development process and evaluations are performed iteratively. Trade-off evaluations are executed for selecting alternative HSI design plan from viewpoint of reliability and usability. Some prototype of HSI design (part) is made for performance-based tests.

The HSI design is documented to include the detailed HSI description including its form, function and performance characteristics, the basis for the HSI requirements and design characteristics with respect to operating experience and literature analyses, tradeoff studies, engineering evaluations and experiments, and benchmark evaluations records of the basis of the design changes.

Appendices A and B described the tests and evaluations conducted for the Japanese Standard HSI System, which is the basis of the US Basic HSIS described in Section 4.0. Appendix C describes the additional tests and evaluations conducted for the development of the US Basic HSIS (Phase 1), and the additional tests and evaluations that will be conducted for the plant specific application of that system (Phase 2), and the site specific application of that system (Phase 3). The V&V activities conducted during Phase 2b and Phase 3a of the HFE program are conducted on the 'final', integrated design. Phases 2 and 3 are applicable to new plants and operating plant modernization programs.

5.7.3.4 HSI Design Documentation

Section 4 "Design Description" defines:

- US Basic HSI design basis
- US Basic HSI functional specification that includes specifications for data processing

The following design documents complete the US Basic HSI design specification:

- The US Basic HSI Style Guide, as described above.

-
- The US Basic HSI Nomenclature which defines the standard acronyms and abbreviations and equipment description guidelines used in the HSI design.
 - The Component Control Design Guide that describes generic control logic and information processing logic to support operator control face plate operation, including associated indications and alarms.
 - The following key design documents complete the integrated plant specific HSI design: Graphic display and panel layout drawings
 - HSI database, which defines characteristics (e.g. instrument ranges, alarm prioritization) and links the VDU display icons, parameters, trends, alarms, soft controls, etc. and panel hardware devices to the database of the control and protection systems
 - Logic and algorithm diagrams for HSI function processing, such as OK status monitoring, BISI and critical safety function monitoring.
 - Detailed room and console configuration diagrams.

Table 5.7-1 Example of Color Coding Rule

Element	Main Color	
Component	Start, Open	Red, White(Open)
	Stop, Close	Green, White(Close)
	Uncertain	Yellow
Fixed Area	Green, Cyan	
Background	Black	
Variable Value / Characters	Normal	Green, White
	Abnormal	Red
	Uncertain	White, Yellow
Switches	Normal	Green, Gray
	Selected	Magenta, Gray
	Answer Back	Yellow, Magenta
Abnormal	Red, Yellow, Green	

Table 5.7-2 Example of Component Symbol (Pump)





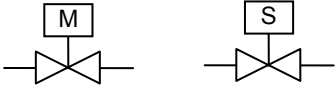
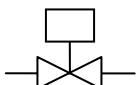


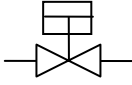
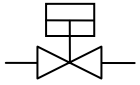
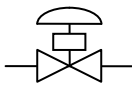
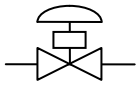
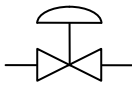
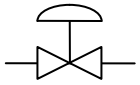
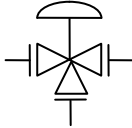
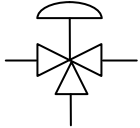
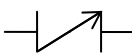

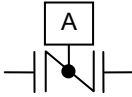
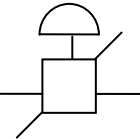
Method			Remarks
Display	Color	Contents	
	White	Normal/ Start	Right Left Up Down: 4type
	White	Normal/Stop	
	Red	Abnormal/ Start	
	Red	Abnormal/ Stop	

Table 5.7-3 Example of Component Symbol (Valve)

Symbol for PID	Symbol for Display	
	Display	Remark
		<div>Close</div>  <div>Open</div> 
Piston Valve 		
Air-operated Valve (with Positioner) 		
Air-operated Valve 		
		
Stop Valve 		
Butterfly Valve 		

5.8 Operating Procedure Development Plan

5.8.1 Procedures to be Developed

The procedures for the US-APWR are categorized as follows:

- Normal Operating Procedure (NOP)
 - Plant operating procedures (including startup, power, and shutdown operations)
 - System operating procedures (including startup, power, and shutdown operations) (note) Above two categories contents same technical information, but they differs
 - Alarm response procedure (ARP)
 - Maintenance procedure
 - Periodic test procedures
- Emergency Operating Procedure (EOP)
 - Event-base EOP
 - Symptom-base EOP

a. Procedures for Normal Operation

Normal operating procedures are of two types:

- **Plant operating Procedures** for changing the state of the plant (start-up, load change, shutdown, outage, etc.)
- **System operating procedures** for the operation of individual plant systems (line-up, start-up, shutdown, change of operating mode, etc.) This category corresponds to the various operating modes

The presentation of these procedures in form of computerized formats has to respect the following requirements:

- the operator has to know the objectives to follow/to ensure: visualization of the current state and of the pursued objectives,
- the operator has to know the state of the means, systems and functions which are available to ensure or to re-establish a given objective
- the operator is to be guided in the resolution of conflicts (if any) in the management of priorities about which function to treat first (presentation of an adequate decision logic)
- the procedure provide detailed descriptions for the execution of tasks and actions by providing adequate step programs for manual execution, or by reference to appropriate automatic sequences
- guidance of the operator is to be structured, with several levels of detail (objectives; tasks; actions),so as to enable operator to execute the procedure at any level of detail

The ARP is provided for each of alarm items. In case of failures of plant systems or unexpected plant state evolution, the alarm system warns the operator and guides operator to the corresponding actions using the associated ARP.

b. Procedures for Emergency Operation

The approach adopted for the US Basic HSIS to provide accident response operation consists of both event-based and symptom-based emergency operating procedures (EOP). As in US PWRs, operators enter the highest level emergency procedure (typically referred to as E-0) based on a reactor trip or ESF actuation. Steps within the highest level EOP lead operators to event specific EOPs, or symptom-based EOPs which direct actions to monitor and maintain critical safety functions. The principal characteristics of this approach are the following:

- The event-base Procedures are provided for the following:
 - Failure events involving digital I&C systems and HSI systems
 - Transients and design-basis accidents
 - Reasonable risk-significant, beyond-design-basis events, which are determined from the plant specific PRA
- The symptom-base procedures also provided to maintain plant safety critical functions as follows:
 - Reactivity Control
 - RCS Inventory
 - Core Cooling
 - Secondary Heat Sink
 - RCS Integrity
 - Containment Integrity

The procedure defines priority between the event and critical functions.
It also defines symptoms for each critical function.

- The operator has to know the state of the means, systems or functions which are available to ensure or to re-establish a given objective,
- The operator is to be guided in the resolution of conflicts between safety objectives in the management of priorities concerning which function to treat first,
- The operator is to be guided in the resolution of conflicts between different means (a single means is potentially used for several objectives; this may cause conflicts: it may be needed to ensure an objective, it can be rejected because it endangers an other objective),
- In case of failures of systems or in case of interaction of functions or systems, the procedure proposes substitutions.
- The procedures provide descriptions for the fulfilment of tasks and actions. Notably, this guidance may be only paper based even if other parts of the procedure are computerized.

Emergency procedures consider the degraded HSI conditions described in Section 4.11.

5.8.2 Procedures Development Process

The procedures development team consists of following personnel, some of them are to be a member of the HFE team:

- Human Factors Engineer
provides task analyses results and HRA results of risk-important human actions

-
- Systems Engineer
provide knowledge of the processes involved in reactivity control and power generation of procedures
 - Nuclear Engineer
system-based technical requirements and specifications
 - I&C Engineer and Computer System Engineer
provides digital I&C system (including failure modes) and computer-based HSI technology impact to the procedures especially for introduction of computer-based procedures system
 - Plant Operator
provide knowledge of operational tasks and procedure formats, especially as presented in emergency procedure guidelines and operational procedures of current and predecessor plants
 - Systems Safety Engineer
provides risk-important human actions identified in the HRA/PRA
 - Maintainability/Inspectability Engineer
provide input in the areas of maintainability and inspectability to the development of procedures

The basis for procedure development comes from the Task Analysis, as shown in Figure 5.4-1, and from operating procedure guidelines developed by plant system designers. Procedures from reference US operating plants are also evaluated to ensure differences are justified based on plant design differences. The US operating plant references are identified in plant licensing documentation. The procedure basis also includes HEDs resulting from any HFE program element, including V&V activities, whose resolution requires procedure emphasis. Procedure emphasis may also be warranted for risk-significant HA's identified in the HRA.

A style guide is developed to establish the process for developing technical procedures that are complete, accurate, consistent, and easy to understand and follow. The guide contains objective criteria so that procedures developed in accordance with it are consistent in organization, style, and content. The guide is used for all procedures within the scope of this element.

The guide provide instructions for procedure content and format including the developing of action steps and the specification of acceptable acronym lists and acceptable terms to be used. The procedure style guide also defines a hierarchical procedure numbering scheme so that procedures that have a related or similar purpose are grouped and/or placed at the same level in the hierarchy. The V&V team shall ensure that features, such as consistency in format and numbering, facilitate easy access to correct procedures.

The content of the procedures incorporate the following elements as existing procedures of Japan and US:

- title and identifying information, such as number, revision, and date
- statement of applicability and purpose
- prerequisites
- precautions (including warnings, cautions, and notes)
- important human actions
- limitations and actions
- acceptance criteria
- check-off lists
- reference material

The most of operator experience is reflected in the present Japanese and US operating procedures. However the OER results described in section 5.2 are reviewed for checking necessity of reflection to the US-APWR procedures.

Preliminary procedures are provided before the activity of HSI V&V.

The procedures are verified first by analytical validation, such as task analysis and HRA.

They are validated and finalized in the integrated system validation described in section 5.10.

5.8.3 Operating Procedure Maintenance

After the plant is constructed and starts operation, operating experience of other plants and the changes that are made in the plant, including changes to HSI designs of the HSI system, are to be verified for needs of procedure changes. Modified procedures are verified, by the HFE V&V team, with respect to content, format, integration, and effect on personnel tasks significant to plant safety.

Any procedure changes needed after the original procedure validation will be conducted by the same process as the original procedures, described above:

- The procedure development team will include the same disciplines.
- The same procedure style guide will be used.
- The same process will be used for analytical verification and integrated system validation.
- The same tracking and resolution process is used to resolve HEDs generated during validation activities.
- The same process as described in Section 4.8 is used to convert the revised paper procedure to its electronic procedure format, and to control the configuration of both formats.

5.9 Training Program Development Plan

This section describes key elements of the Training Program Development process.

5.9.1 Training Program

The training program for the HSI system is developed in accordance with the “Technical Report on Template for an Industry Training Program Description”, NEI 06-13A. (Reference 6) The IAEA’s Systematic Approach to Training (SAT) program (Reference 42) will be followed and following points are clarified:

- Clarify technical ability for performing operator’s task
- Develop and execute training method to accomplish the technical ability
- Reflect training results and improve training method logically

This method also complies with NRC’s “INSPECTION MANUAL CHAPTER 1245”.

The training facility is settled at the corresponding NPP site at least two years before the fuel loading.

The basis for the training program includes:

- Plant design documentation - Electrical and Mechanical Flow Diagrams, Functional Diagrams, Tech Manuals, Design Bases Documents, Setpoint and operating range documents, accident analysis and the Licensing Basis.
- HFE program documentation - the OER, the FRA/FA, the Task Analysis, the HRA, the HSI design, the plant procedures.
- HEDs resulting from any HFE program element, including V&V activities, whose resolution requires training emphasis.

5.9.2 Operator Training Simulator Fidelity

The training simulator meets the requirements of Regulatory Guide 1.149 “Nuclear Power Plant Simulation Facilities for Use in Operator Training and License Examinations.” Training simulator satisfies the following requirements addressed in ANSI/ANS 3.5 (Reference 9):

- Simulator’s MCR and RSS console and their HSI system does not deviate from those of the reference. So, part-task simulators are unnecessary and not used.
- The following parameters will match the reference unit data within 1%:
 - Temperature (T) average
 - T-hot
 - T-cold
 - MWe
 - Power range nuclear instrumentation readings
 - Reactor coolant system pressure
 - Steam generator pressure
 - Pressurizer level.

The following parameters will match the reference unit data within 2%:

- Steam generator feeds flow

- Reactor coolant system flow
- Steam generator level
- Letdown flow
- Charging flow
- Steam flow
- Turbine first stage pressure.
- Instructor is able to use training simulator's basic functions, such as initialization, switch, check, freeze/run, snapshot, slow time/fast time, recorder power off, emergency power off, backtrack, record/replay, annunciator control, etc.,

Simulator training is provided in accordance with industry guidance for licensed operators including NEI 06-13A, Rev 1.

NEI 06-13A describes the contents for the following training programs:

LICENSED OPERATOR TRAINING

- Licensed Operator Initial Training Program
- Continuing Training for Licensed Personnel

TRAINING FOR POSITIONS LISTED IN 10 CFR 50.120

- Non-Licensed Operator (NLO) Initial Training
- Shift Manager Initial Training
- Shift Technical Advisor Initial Training Program
- Instrumentation and Control (I&C) Technician Initial Training
- Electrical Maintenance Initial Training Program
- Mechanical Maintenance Initial Training Program
- Radiological Protection Technician Initial Training
- Chemistry Technician Initial Training
- Engineering Personnel Initial Training
- Continuing Training for Personnel Listed in 10 CFR 50.120

GENERAL EMPLOYEE TRAINING (GET) PROGRAM

- Plant Access Training
- Radiation Worker Training Program
- General Employee Requalification Training

SELECTED OTHER TRAINING PROGRAMS

- Fire Protection Training
- Emergency Plan Training Program
- Physical Security Training Program
- Station Management Training Program

Appendix A of NEI 06-13A, Rev.1 describes the Cold License Training plan for new plant construction and initial operation.

5.9.3 Class Room Training for Operators and Technicians

Class room training facility is also provided and following skills are taught in the course:

- Reactor technology

- Turbine and generator technology
- Nuclear power safety regulations
- Quality assurance
- Human factors
- Digital I&C system

Class room training will be conducted using static presentation material, and computer based training using personal computers. To the extent practical the plant models used in the computer based training will be the same models used in the plant-referenced simulator.

5.9.4 Instructor Qualifications and Training

Instructor of training facility must have following skills and qualification:

- Instructional Skills
 - Training plan, Learning materials, Writing test
 - Training implementation, Evaluation, Critique and Reporting
 - Administrative skill
- Technical Skills
 - Knowledge of Nuclear power plant system
 - Design basis, Plant characteristics, Operating procedures and Simulators
 - Theoretical and practical technical skill based on working experience
- Interpersonal Skills
 - Elicit trainees' opinion and question, sincere gratitude
 - Corporate colleague and other staff
- College diploma and working Experience
- Operating Test
 - Initial Training Course : manipulate simulator
 - Continuing Training Course : Diagnose
- Assessment of instruction skill
 - Lecture
 - simulator training
- Assessment of produced training materials
- Assessment of training records

5.9.5 Role of the HFE Design Team in the Training Development Program

HFE Design Team provides following input to the training development program to identify the areas where training is required and for the development of the training material:

- **Licensing Basis** - Final Safety Analysis Report, system description manuals and operating procedures, facility license and license amendments, licensee event reports, and other documents identified by the staff as being important to training.
- **Operating Experience Review** - previous training deficiencies and operational problems that may be corrected through additional and enhanced training, and positive characteristics of previous training programs.
- **Function Analysis and Allocation** - functions identified as new or modified
- **Task Analysis** - tasks identified during task analysis as posing unusual demands including new or different tasks, and tasks requiring a high degree of coordination, high workload, or special skills.

- **Human Reliability Analysis** - coordinating individual roles to reduce the likelihood and/or consequences of human error associated with risk-important HAs and the use of advanced technology of digitalized I&C and computerized HSI system.
- **HSI Design** - design features of the computerized HSI system whose purpose or operation is to be different from the past experience or expectations of personnel.
- **Plant Procedures** - tasks that have been identified during procedure development as being problematic (e.g., procedure steps that have undergone extensive revision as a result of plant safety concerns).
The CBP system is the most characteristic difference in the computerized HSI system.
- **Verification and Validation (V&V)** - training concerns identified during V&V, including HSI usability concerns identified during validation or suitability verification and operator performance concerns (e.g., misdiagnoses of plant event) identified during validation.

The training program is developed in cooperation with the training department of the COL applicant for the US-APWR or the licensee for operating plant modernization. The details of the training program development plan are provided in plant licensing documentation. The roles of all organizations (e.g., MHI, plant owners, and vendors) are specifically defined in the Training Implementation Procedure for the development of training requirements, the development of training information sources, the development of training materials, and the implementation of the training program.

5.9.6 Training Program Modifications

Training program modifications include development of new or revised training material, changes in instructing techniques or changes in the frequency of training. Modifications to the training program, may result from:

- (1) HEDs identified during validation, as discussed in Section 5.10.2.2.5,
- (2) design changes, which are addressed in Section 5.11, or
- (3) from the evaluation of human performance, which is addressed in Section 5.12.

Training program changes will be implemented using the same process as the development of the original training program.

5.9.7 Retraining

Personnel undergo periodic retraining. The periodicity of the retraining is established based on regulatory requirements (e.g., Training and Qualification of Nuclear Power Plant Personnel, NRC Regulations Title 10, Code of Federal Regulations, Part 50.120, Appendix E) and Human Performance Monitoring (see Section 5.12). Human performance deficiencies are identified as HEDs and tracked to resolution. HEDs may indicate the need for retraining based on a previous training program, or retraining based on a program with changes to address the specific deficiency encountered.

For operating plant upgrades or any HSI changes that occur after the initial training and initial HSI design deployment, the training program ensures plant personnel are retrained on all tasks that are affected by the new HSI design. The extent of retraining is dependent on the extent to which the task is impacted. For example, it is not necessary to retrain personnel on the function of a plant fluid system if the new HSI does not change the operation or performance of that system.

5.9.8 Training Effectiveness

The trainees are evaluated to determine their mastery of the learning objectives taught. Methods for this evaluation include written and oral tests, as well as a review of personnel performance during walkthroughs, simulator exercises, and evaluation of on-the-job performance.

Deficiencies commonly applicable to multiple trainees are considered training program deficiencies. These deficiencies are identified as HEDs and are tracked to resolution. Training courses are maintained under a quality assurance program that contains configuration controls to ensure all training modifications are tracked.

5.10 Human Factors Verification and Validation

The V&V program is conducted in multiple phases, as described at a high level in Appendix C, and in more detail in the each plant specific V&V Implementation Plan. For example, the V&V Implementation Plan for the US-APWR is provided in Section 18.10 of the DCD.

The V&V program activities conducted during Phase 1, which applies to the US Basic HSIS, is generically applicable to all applications of the US Basic HSIS (i.e. to the US-APWR and operating plant upgrades). Phase 1 V&V will not be repeated. The V&V program activities conducted during Phases 2 and 3, as described in Appendix C for the US-APWR, will be uniquely repeated for all plant/site specific applications. Phases 2 and 3 are carried out on final plant/site specific HSI design. The HSI facilities for all phases of the V&V program include the complete HSI system. However, the specific V&V activities are focused on changes from the previous NRC approved reference design. Since the first application of the US Basic HSIS has no prior NRC approved reference, the V&V activities are more extensive than expected for subsequent applications. Subsequent applications of the US Basic HSIS will focus primarily on plant specific changes that result in changes to the HSI Inventory (i.e. displays, alarms, controls and procedures). The details of each plant specific V&V program are provided in each plant specific V&V Implementation Procedure.

5.10.1 Principle of Verification and Validation (V&V)

There are four major human factor verification and validation (V&V) activities: Operational Condition Sampling, Design Verification, Integrated System Validation, and Human Engineering Discrepancies (HEDs) Resolution. (Reference 17 and 28)

Operational Condition Sampling is the activity intended to identify the range of operational conditions relevant to guide V&V activities.

The Human Factors Verification and Validation program involves two types of Design Verification activities: HSI Task Support Verification and HFE Design Verification. HSI Task Support Verification is an evaluation whose purpose is to verify that the HSI supports personnel task requirements as defined by task analyses. HEDs are identified for: (1) personnel task requirements that are not fully supported by the HSI, and (2) the presence of HS components which may not be needed to support personnel tasks. HFE Design Verification is an evaluation to verify that the HSI is designed to accommodate human capabilities and limitations as reflected in HFE guidelines, such as those provided in NUREG-0700. HEDs are identified if the design is inconsistent with HFE guidelines.

Integrated System Validation is an evaluation using performance-based tests to determine whether an integrated system design (i.e., hardware, software, and personnel elements) meets performance requirements and acceptably supports safe operation of the plant. HEDs are identified if performance criteria are not met.

HED Resolution is an evaluation to provide reasonable assurance that the HEDs identified during the V&V activities have been acceptably assessed and resolved. HED Resolution is performed iteratively with V&V.

Figure 5.10-1 shows an overview of the verification and validation activities.

MHI has experience conducting HFE V&V in Japanese PWR plants. The HFE V&V was conducted in two steps: during the development phase and in the actual plant design implementation phase. This experience is described in Appendix B. For the US-APWR plants, both the development phase and design implementation phase of HFE V&V are conducted. |

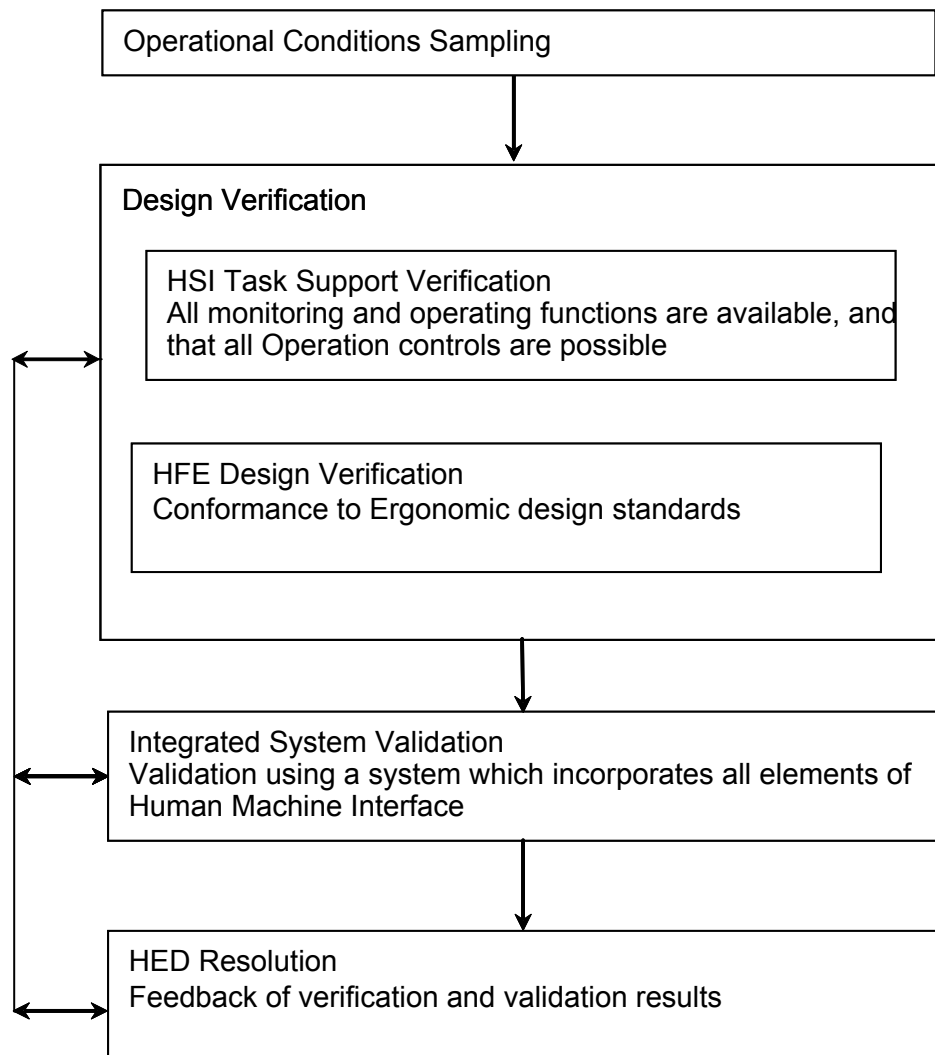


Figure 5.10-1 Overview of Verification and Validation Activities

5.10.2 Implementation Plan for HFE V&V

5.10.2.1 Operational Conditions Sampling

The sampling methodology identifies a range of operational conditions to guide V&V activities. The following sampling dimensions are addressed below: plant conditions, personnel tasks, and situational factors known to challenge personnel performance.

a. The following plant conditions are included:

- Normal operational events including plant startup, plant shutdown or refueling, and significant changes in operating power
- Failure events
- Transients and accidents, including accidents with concurrent Common Cause Failure conditions
- Reasonable, risk-significant, beyond-design-basis events, which are determined from the plant specific PRA
- Consideration of the role of the equipment in achieving plant safety functions (as described in the plant safety analysis report (SAR)) and the degree of interconnection with other plant systems

b. The following types of personnel tasks are included:

- Risk-significant HAs, systems, and accident sequences
- OER-identified difficult tasks
- Range of procedure guided tasks – These are tasks that are well defined by normal, abnormal, emergency, alarm response, and test procedures
- Range of knowledge-based tasks - These are tasks that are not as well defined by detailed procedures
- Range of human cognitive activities
- Range of human interactions
- Tasks that are performed with high frequency

c. The sample reflects a range of situational factors that are known to challenge human performance, such as:

- Operationally difficult tasks
- Error- forcing contexts
- High-workload conditions
- Varying-workload situations
- Fatigue and circadian factors
- Environmental factors

The results of the sampling are combined to identify a set of scenarios to guide subsequent analyses.

5.10.2.2 Design Verification

5.10.2.2.1 Inventory and Characterization

The inventory includes all HSI components associated with the personnel tasks based on the identified operational conditions.

The inventory describes the characteristics of each HSI component. The following is a minimal set of information required for the characterization of each component in the inventory:

- A unique identification code number or name
- Associated plant system and subsystem
- Associated personnel functions/subfunction
- Type of HSI component
 - computer-based control
 - hard-wired control
 - computer-based display
 - hard-wired display
- Display characteristics and functionality
- Control characteristics and functionality
- User-system interaction and dialog types
- Location in data management system
- Physical location in the HSI

5.10.2.2.2 HSI Task Support Verification

HSI task support verification confirms that the HSI provides all alarms, information, and control capabilities required for personnel tasks.

In the HSI task support verification, the HSIs and their characteristics (as defined in the HSI inventory and characterization) are compared to the personnel task requirements identified in the task analysis, by the HFE V&V team. In addition, Plant designers, including plant safety analysis engineers, verify draft procedures from a plant system design point of view and plant safety. Static task support verification confirms the procedures and displays have the necessary information and controls.

HEDs are identified when:

- An HSI needed for task performance is not available
- HSI characteristics do not match the personnel task requirements
- An HSI is identified as available but is not needed for any task.

HEDs are documented to identify the HSI, the relevant task criterion, and basis for the discrepancy.

5.10.2.2.3 HFE Design Verification

HFE design verification is to verify the characteristics of the HSI and environment in which it is used conform to HFE guidelines.

For HFE design verification, a design-specific HFE guideline document is prepared. The design-specific HFE guideline document is compared to the HFE guidelines contained in NUREG-0700 to confirm the guidelines in the design-specific HFE guideline document satisfy the guidelines in NUREG-0700.

The design-specific HFE guideline document includes the following guidelines:

- Display screen format organization
- Font size for each display screen
- Touch size for touch screen operation
- Color coding
- Display Labeling coding
- Ergonomic requirement for display
- Standard of controllers and switches
- Guidelines for display design (guidelines and coding rules for display screen implementation)

5.10.2.2.4 Integrated System Validation

Integrated system validation is the process by which an integrated system design (i.e., hardware, software, and personnel elements) is evaluated using performance-based tests to determine whether it acceptably supports safe operation of the plant.

Integrated system validation is conducted after significant HEDs that are identified in verification reviews are resolved. Dynamic validation confirms the procedures and displays using a full scale plant simulator test facility. Validation test scenarios are designed and monitored by the HFE V&V team. HSIS problems are extracted as human engineering discrepancies (HEDs) and are tracked to closure using the HFE issues tracking system.

a. Test Objectives

Detailed objectives are developed to provide evidence that the integrated system adequately supports plant personnel in the safe operation of the plant.

The objectives are as follows:

- Validate the role of plant personnel.
- Validate that the shift staffing, assignment of tasks to crew members, and crew coordination (both within the control room as well as between the control room and local control stations and support centers) is acceptable.
- Validate that for each human function, the design provides adequate alerting, information, control, and feedback capability for human functions to be performed under normal plant evolutions, transients, design-basis accidents, and selected, risk-significant events that are beyond-design basis.
- Validate that those specific personnel tasks can be accomplished within time and performance criteria, with a high degree of operating crew situation awareness, and with acceptable workload levels that provide a balance between a minimum level of vigilance and operator burden. Validate that the operator interfaces minimize operator error and provide for error detection and recovery capability when errors occur.

- Validate that the crew can make effective transitions between the HSIs and procedures in the accomplishment of their tasks and that interface management tasks such as display configuration and navigation are not a distraction or undue burden.
- Validate that the integrated system performance is tolerant of failures of individual HSI features.
- Identify aspects of the integrated system that may negatively affect integrated system performance.

In addition to the objective data of operator performance, as described above, performance measures include subjective operator and observer feedback collected via questionnaires and verbal debrief sessions, using:

- Post-scenario operator forms (including 5-point Likert rating questions)
- Post-scenario observer form
- Final operator feedback forms (including 5-point Likert rating questions)
- HED forms

b. Validation Test Facility

The validation test facility used to perform validation evaluations satisfies the following requirements. The facility used for validation test is consistent with the criteria of the American National Standard “Nuclear power plant simulators for use in operator training” ANSI/ANS 3.5-1998 as a guide. The scope of the plant dynamics is limited to the scope of integrated system validation test. The validation test facility is planned to be constructed at MELCO’s factory in the US. The test facility is a full scale HSI mockup with a full-scope simulator.

- Interface Completeness – The test facility completely represents the integrated system. This includes HSIs and procedures not specifically required in the test scenarios. For example, adjacent controls and displays may affect the ways in which personnel use those that are addressed by a particular validation scenario.
- Interface Physical Fidelity –A high degree of physical fidelity in the HSIs and procedures are represented, including accurate presentation of alarms, displays, controls, job aids, procedures, communications, interface management tools, layout and spatial relationships.
- Interface Functional Fidelity –A high degree of functional fidelity in the HSIs and procedures are represented. All HSI functions are available. High functional fidelity includes HSI component modes of operation, i.e., the changes in functionality that can be invoked on the basis of personnel selection and/or plant states.
- Environment Fidelity –A high degree of environment fidelity is represented. The lighting, noise, temperature, and humidity characteristics reasonably reflect those expected. Thus, noise contributed by equipment, such as air handling units and computers are represented in validation tests.
- Data Completeness Fidelity –Information and data provided to personnel completely represent the plant systems monitored and controlled from that facility.
- Data Content Fidelity – A high degree of data content fidelity are represented. The information and controls presented are based on an underlying model that accurately reflects the reference plant. The model provides input to the HSI in a manner such that information accurately matches that which is actually presented in the reference plant.
- Data Dynamics Fidelity – A high degree of data dynamics fidelity are represented. The process model are capable of providing input to the HSI in a manner such that information flow and control responses occur accurately and in a correct response time; e.g., information are provided to personnel with the same delays as would occur in the plant.
- For important actions at complex HSIs remote from the main control room, where timely and precise human actions are required, the use of a simulation or mockup are considered to verify that human performance requirements can be achieved. (For less risk-important HAS or where the HSIs are not complex, human performance may be assessed based on analysis such as task analysis rather than simulation.)
- The test facility is verified for conformance to the test facility characteristics identified above before validations are conducted.

c. Plant Personnel

Participants in the validation tests are representative of actual plant personnel who interact with the HSI. They are licensed operators.

To properly account for human variability, a sample of participants is used.

In the selection of personnel, consideration is given to the assembly of minimum and normal crew configurations, including shift supervisors, reactor operators, shift technical advisors, etc., that participate in the test.

To prevent bias in the sample, the following participant characteristics and selection practices are to be avoided:

- Participants who are part of the design organization
- Participants in prior evaluations
- Participants who are selected for some specific characteristic, such as using crews that are identified as good or experienced.

d. Scenario Definition

The operational conditions selected for inclusion in the validation tests are developed in detail so they can be performed on a simulator.

Scenarios have appropriate task fidelity so that realistic task performance is observed in the tests and test results can be generalized to actual plant operations.

When evaluating performance associated with operations remote from the main control room, the effects on crew performance due to a potentially harsh environment (i.e., high radiation) are realistically simulated (i.e., additional time to don protective clothing and access to radiologically controlled areas).

e. Performance measurement

A hierarchical set of performance measures are used that include measures of the performance of the plant and personnel.

- For plant performance, the following measurements are used:
 - Alarm history
 - Event log (plant trip time, ECCS actuation time, etc.)
 - HSIs use history (display screen request history, operational history, etc.)

- Personal task measurement

For each specific scenario, the tasks that personnel are required to perform are identified and assessed. Two types of personnel tasks are measured: primary (e.g., start a pump), and secondary (e.g., access the pump status display). Following measurements are used:

- Time
- Operation and monitoring log
- Errors (omission and commission)
- Amount achieved or accomplished
- Subjective report of participants
- Behavior categorization by observers

- Situation awareness

Situation Awareness will be modified as follows. As described in Section 4.1d, the primary purpose of the Large Display Panel (LDP) is to provide Spatially Dedicated Continuously Visible (SDCV) information to operation personnel to enhance situation awareness. One purpose of the Safety VDUs is to provide SDCV displays for accident monitoring, as described in Section 4.6.1. The content of the SDCV information on the LDP and Safety VDUs is determined based on industry and NRC guidance for SDCV Minimum Inventory, as described in Section 4.12d. The content and display style guide of the LDP and Safety VDUs will be verified and validated. Therefore, since the purpose of SDCV HSI is to achieve adequate situation awareness, and the HSI design meets the best available industry and NRC guidance for SDCV HSI, situation awareness will not be measured.

However, the Integrated System Validation Program explicitly evaluates the ability of operators to maintain situation awareness, especially with regard to the status of automated systems and critical safety functions. Test scenarios include instances where automatic safety systems, that support critical safety functions, fail or partially fail to actuate as required. The evaluation examines the ability of operators to detect the failures and to manually take control to maintain the critical function. Performance acceptance criteria are established for each test scenario, and post scenario Likert rating questions address the following:

- Ability to maintain the 'big picture' with respect to current plant state and direction of process variables
- Ability to maintain awareness of the critical plant safety functions (e.g., based on the information provided on the LDP)
- Ability of the SRO to adequately supervise operator activities and control actions from the SRO workstation

The role of operators as supervisors of automated systems was explicitly addressed in the Phase 1B V&V program, as documented in Part 3 of MUAP-09019.

- Cognitive workload

Cognitive workloads evaluated based on the method described in subsection 5.4.3.2

f. Test Design

Scenario Assignment – Important characteristics of scenarios are balanced across crews. Normally the same scenario is used for every crew.

The order of presentation of scenario types to crews is carefully balanced to provide reasonable assurance that the same types of scenarios are not always being presented in the same linear position. e.g., the easy scenarios are not always presented first.

Test procedures including the description of NUREG-0711 section 11.4.3.2.6.2 “Test Procedures” are prepared.

Test administration personnel receive training on:

- The use and importance of test procedures
- Experimenter bias and the types of errors that may be introduced into test data through the failure of test conductors to accurately follow test procedures or interact properly with participants
- The importance of accurately documenting problems that arise in the course of testing, even if due to test conductor oversight or error.

Participants are trained to provide reasonable assurance that their knowledge of plant design, plant operations, and use of the HSIs and procedures is representative of experienced plant personnel.

Participants are trained to reach near asymptotic performance (i.e., stable, not significantly changing from trial to trial). One day and half day training is enough for training to use HSIs, based on the experience in Japan.

g. Data Analysis and Interpretation

Validation test data are analyzed through a combination of quantitative and qualitative methods. The relationship between observed performance data and the established performance criteria is clearly established and justified based upon the analyses performed.

For performance measures used as pass/fail indicators, failed indicators are resolved before the design can be validated. Where performance does not meet criteria for the other performance measures, the results are evaluated using the HED evaluation process.

The degree of convergent validity is evaluated, i.e., the convergence or consistency of the measures of performance.

The data analysis is independently verified for correctness of analysis.

The inference from observed performance to estimated real-world performance allows for margin of error.

h. Validation Conclusions

The validation conclusions are clearly documented including the statistical and logical bases for determining that performance of the integrated system is acceptable.

Validation limitations are considered in terms of identifying their possible effects on validation conclusions and impact on design implementation. These include:

- Aspects of the tests that were not well controlled
- Potential differences between the test situation and actual operations, such as absence of productivity-safety conflicts
- Potential differences between the validated design and the plant as built.

5.10.2.2.5 Human Engineering Discrepancy Resolution

HED Resolution is an activity that is performed iteratively with V&V. HED Resolution is performed after design verification and integrated system validation.

5.10.3 Organization of V&V Team

The V&V team includes personnel independent of the designers involved in the HSI initial design.

The V&V team includes personnel who have the following expertise:

- plant operation (maybe operators) and operator training
- Human System Interface design
- Human factor engineering

5.11 Design Implementation Plan

For new plants the ITAAC is used to confirm that the implemented HSI system is consistent with the validated HSI system. Inspections, Tests, Analysis, and Acceptance Criteria (ITAAC) are included in the DCD submittal.

The US Basic HSIS is applied to operating plant modernization using the same analysis, design and V&V process as for new plants. The final integrated design is validated using a full scope simulator, as described for Phases 2 and 3 of the US-APWR program in Appendix C. The Design Implementation Program confirms through inspections and tests that the implemented HSI system is consistent with the validated HSI system. Any changes to the design that may be needed after final integrated validation are assessed for their risk significance. The risk significance considers the scope of the change as well as the potential impact on plant safety functions. Based on the risk significance, some or all of the previous elements described in the HFE Program Plan are executed for the modified design.

The Design Implementation Plan element of the HFE Program Model also applies to operating plant modernization. It would also apply to HSI changes to the US-APWR after COL approval.

HSI modifications to a licensed design will utilize the HSI features described in Section 4. If there are changes to the basic HSI features described in Section 4, those changes will undergo a complete evaluation to determine what portions of the HFE program must be repeated. Effects on the HSI style guide will be included in this evaluation.

For any HSI change to a licensed design the potential impact on Human Actions is assessed and a risk significance level is assigned in accordance with the criteria in NUREG-1764. The risk significance considers the scope of the change as well as the potential impact on plant safety functions. Based on the risk significance some or all of the previous elements described in the HFE Program Plan are executed for the new design. The scope for each element is limited to the HSI change and any interfaces that may be affected by the change.

Facility design changes are documented and analyzed for their potential impact on HSIs. Those design implementation issues that negatively impact human performance are identified as HEDs and are tracked and dispositioned. HFE design modifications are documented in a periodic status report.

Design implementation is addressed in plant specific licensing documentation.

5.12 Human Performance Monitoring Plan

The goal of this element is to ensure that plant personnel have maintained the skills necessary to accomplish human actions within the time and performance criteria confirmed during the HSI validation program. The Human Performance Monitoring Plan ensures that no significant safety degradation occurs because of any changes that are made in the plant, including changes to HSI designs, procedures and training.

In addition, the Human Performance Monitoring Plan ensures that no significant safety degradation occurs because of any changes that are made in the plant, including changes to HSI designs, procedures and training.

The plan requires periodic monitoring and documentation of human performance in actual or simulated plant conditions. Trends are maintained so that degraded performance is identified prior to reaching unacceptable levels. Corrective actions are tracked to resolution.

The human performance monitoring program is developed in cooperation with the training department of the COL applicant or potential applicant to apply HSI modernization. The human performance monitoring program will be described in Plant Licensing Documentation.

6.0 REFERENCES

This section lists the references cited in this topical report, except for applicable codes and standards and regulatory guidance in section 3.

1. MUAP-07004, "Safety I&C System Description and Design Process"
2. MUAP-07005, "Safety System Digital Platform-MELTAC"
3. MUAP-07006, "Defense-in-Depth Diversity"
4. PQD-HD-19005, "Quality Assurance Program(QAP) Description for Design Certification of US-APWR"
5. "Cyber Security Program for Nuclear Power Reactors", NEI 04-04, February 2005.
6. "Technical Report on Template for an Industry Training Program Description", NEI 06-13A
7. System 80+ Design Certification Document (DCD)
8. Card, S.K, et al, "The Psychology of Human-Computer Interaction", Hillsdale, NJ: Lawrence Erlbaum Associates, (1983)"
9. ANSI/ANS-3.5 -1998 Nuclear Power Plant Simulators for Use in Operator Training
10. ANSI/ANS 5.8 -1994 Time Response Design Criteria for Safety-Related Operator Actions
11. EPRI NP-3659 Human Factors Guide for Nuclear Power Plant Control Room Development
12. NUREG/CR-1278, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications
13. NUREG/CR-3371 Task Analysis of Nuclear Power Plant Control Room Crews
14. NUREG/CR-2623 The Allocation of Functions in Man-Machine Systems: A Perspective and Literature Review
15. NUREG/CR-3331 A Methodology for Allocation of Nuclear Power Plant Control Functions to Human and Automated Control Functions to Human and Automated Control
16. NUREG/CR-6400 HFE Insights For Advanced Reactors Based Upon Operating Experience
17. NUREG/CR-6393 Integrated System Validation: Methodology and Review Criteria
18. NUREG/CR-6633 Advanced Information Systems: Technical Basis and Human Factors Review Guidance

-
19. NUREG/CR-6634 Computer-Based Procedure Systems: Technical Basis and Human Factors Review Guidance
 20. NUREG/CR-6635 Soft Controls: Technical Basis and Human Factors Review Guidance
 21. NUREG/CR-6636 Maintenance of Digital Systems: Technical Basis and Human Factors Review Guidance
 22. NUREG/CR-6637 Human-System Interface and Plant Modernization Process: Technical Basis and Human Factors Review Guidance
 23. NUREG/CR-6689 Proposed Approach for Reviewing Changes to Risk-Important Human Actions
 24. IEC 60964-1989 Design for control rooms of nuclear power plants
 25. IEC 60960-1988 Functional Design Criteria for a Safety Parameter Display System for Nuclear Power Stations First Edition
 26. IEC 60965-1989 Supplementary control points for reactor shutdown without access to the main control room
 27. IEC 61227-1993 Nuclear power plants—control rooms—operator controls
 28. IEC 61771-1995 Nuclear power plants — main control room — verification and validation of design
 29. IEC 61772-1995 Nuclear power plants — main control room — Visual display unit (VDU) application to main control room in nuclear plants
 30. IEC 61839-2000 Nuclear power plants — Design control rooms — Functional analysis and assignment
 31. IEC 62096-2001 Instrumentation and Control: Guidance for the Decision on Modernization
 32. IEC 60911-1987 Measurement requirements for reactor core sub cooling monitoring
 33. IEC 62241-2004 Nuclear power plants — main control room —Alarm Functions and Presentation
 34. ISO 11064-1-2000 Ergonomic Design of Control Centres — Part 1: Principles for the Design of Control Centres
 35. ISO 11064-2-2000 Ergonomic Design of Control Centres — Part 2: Principles for the Arrangement of Control Suites
 36. ISO 11064-3-1999 Ergonomic Design of Control Centres — Part 3 Control Room Layout
 37. ISO 11064-4:2004 Ergonomic Design of Control Centres — Part 4: Layout and Dimensions of Workstations
-

-
38. ISO 11064-6:2005 Ergonomic Design of Control Centres — Part 6: Environmental Requirements for Control Centres
 39. IEEE Std. 845-1999 IEEE Guide to the Evaluation of Human-System Performance in Nuclear Power Generating Stations
 40. IEEE Std. 1023-1988 IEEE Guide to the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations
 41. IEEE Std. 1082-1997 A Guide for Incorporating Human Action Reliability Analysis for Nuclear Power Generating Stations
 42. IAEA-TECDOC-1057 Experience in the Use of Systematic Approach to Training for Nuclear Power Plant Personnel
 43. N0-EJ30102 Component Control and Monitoring Circuit Basic Design Guide
 44. MUAP-08014,"Human System Interface Verification and Validation (Phase 1a)"
 45. MUAP-09019,"HSI Design"
-

7.0 FUTURE LICENSING SUBMITTALS

The complete MHI digital I&C design is described in four topical and technical reports:

- Safety I&C System Description And Design Process
- Digital Platform
- HSI System Description and HFE Process (this report)
- Defense in Depth and Diversity

Table 7.0-1 summarizes the additional information related to this topical report to be submitted for NRC approval in future Plant Licensing Documentation. Table 7.0-1 summarizes all items identified in previous sections of this report. This Plant Licensing Documentation, in combination with the contents of this topical report, the contents of the other topical and technical reports identified above, and any items for Plant Licensing Documentation described in those other topical and technical reports is expected to be sufficient to allow the NRC to make a final safety determination. Other documentation generated during the design process is available for NRC audit, as may be needed to allow the NRC to fully understand the MHI design and design process. These documents will be made available in the MNES office, which is in close proximity to the U.S. NRC office.

Table 7.0-1 Future Licensing Submittals

Description	Section
HFE Program Management Plan	5.1
Operating experience Review Plan*	5.2
Functional Requirements Analysis and Function Allocation Plan *	5.3
Task Analysis Plan *	5.4
Staffing & Qualification Plan*	5.5
Human Reliability Analysis Plan *	5.6
Human-System Interface Design Plan*	5.7, Chapter 4
Procedure Development Plan*	5.8
Training Program Development Plan*	5.9
Human Factors Verification & Validation Plan and Report	5.10, Appendix B
Design Implementation Plan	5.11
Human Performance Monitoring Plan	5.12

* Reports associated with each of these items are available for NRC audit during the design process in accordance with the plant specific licensing project schedule.

Appendix A History of Development of Japanese PWR Main Control Room by Mitsubishi and Japanese PWR Power Utilities

	Period	Objectives	HFE V&V
1. Development of advanced main control room	1996.10-2003.3	Establishment of total HSI design <ul style="list-style-type: none"> ● Large display panel ● VDU for operation and monitoring ● Decision support system 	Static validation test: 12 crews, 36 persons Dynamic validation test: #1 12 crews, 39 persons #2 12 crews, 37 persons #3 12 crews, 37 persons
2. Development of advanced alarm information display system	1994.10-1996.10	Development of alarm processing and display design	Static validation test: 12 crews, 24 persons Dynamic validation test: 12 crews, 34 persons
3. Development of emergency operation support system	1993.8-1996.3	Development of plant status diagnosis and operation guidance system	Dynamic validation test: 46 crews, 138 persons
4. Development of advanced main control board	1987.4 - 1991.3	Establishment of basic design <ul style="list-style-type: none"> ● VDU based monitoring and operation ● Compact operation console 	Static validation test: 12 crews, 24 persons Dynamic validation test: #1 13 crews, 43 persons #2 13 crews, 44 persons #3 12 crews, 39 persons

Appendix B HFE V&V Experience in Japan

a. Verification and Validation in the Development Phase

Before applying the Advanced Main Control Board to an actual plant, design verification and validation of the standard specification were carried out and completed in the development phase of the control board. In verifying the standard specification, international standards IEC-60964, IEC-61171, and the US guideline NUREG-0711 were used for HSI design verification criteria for the Main Control Boards (MCBs).

The verification and validation were performed in two steps, step I and step II, as shown in Figure B-1. Step I or the “Static Verification” consists of design inspection and design verification of the standard specification. In step II, “Dynamic Validation”, a full scale full fidelity control board was setup (see Figure B-2) and actual plant situations were simulated iteratively using the plant simulator.

Both steps I and II were conducted by experienced plant operators, more than one hundred operators participated in the dynamic validation, which enabled operation practices to be implemented in the design from the development phase.

The validation facility used for validation test of the computerized main control board (DIATOM: Diamond Atomic Touch Operation and Monitoring system) is shown in Figure B-2.

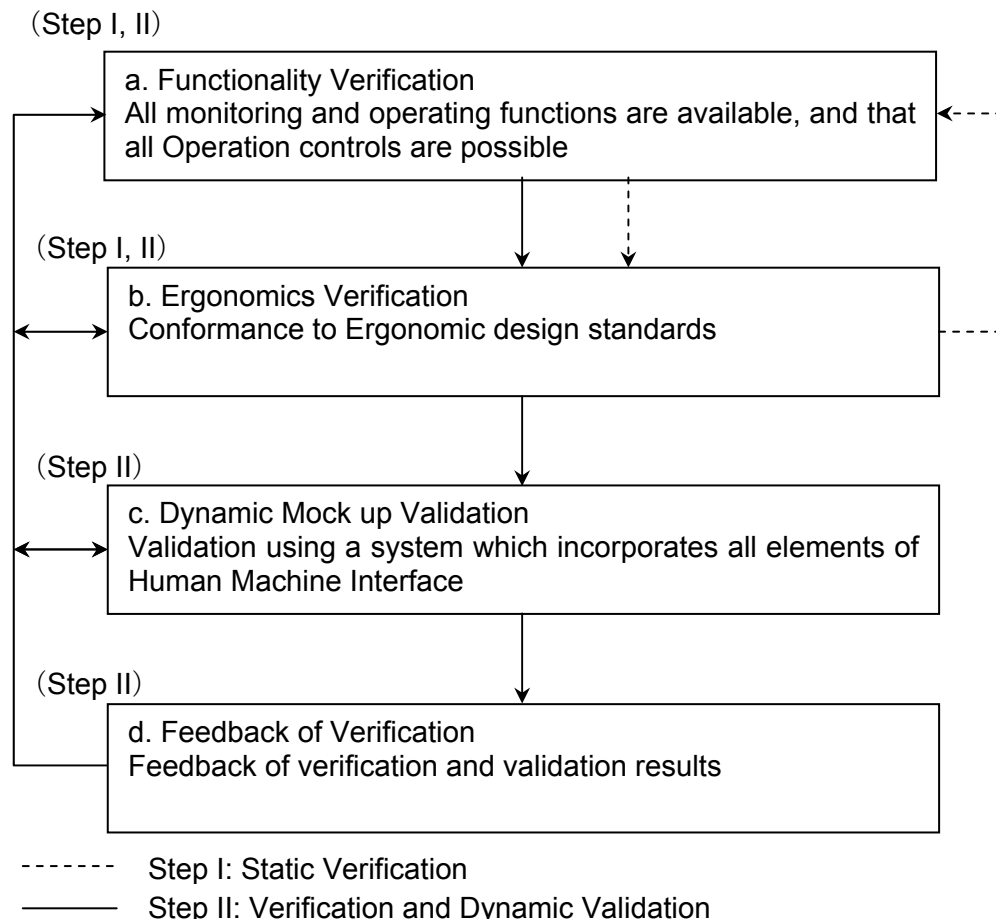


Figure B-1 HFE Verification and Validation Flow in the Development Phase

b. Verification and Validation in the Design Implementation Phase

Verification and validation in the Design Implementation Phase was conducted for the deviations from the standard design developed by the development phase.

Because, the deviations from the standard design were small, V&V in the implementation phase was conducted using a static method as follows.

- Full scale mockup test: - layout in the main control room was confirmed using plant specified full scale static mockup facility.
- Scenario based validation - Plant specified VDU formats verified by scenario based validation method using PC based static VDU format navigation system.

Details of HSI verification and validation in Japan are described in the following documents.

“The Development and Validation of Standardized Main Control Boards for full digital PWR I & C system”, Trans. At. Energy Soc. Japan, Vol.2, No.3, pp. 307 ~ 35. (2003)

“The advanced main control console for next Japanese PWR plants”, Proc. ICONE-9, Nice, (2001)



Figure B-2 The Facility Used in Development Phase

Appendix C Phased Implementation Plan

MHI is applying the HSI system to US nuclear power plants through a phased implementation program. US utility operators are engaged in each phase. Each phase will utilize a full scale HSI simulator with high fidelity plant simulation models.

The first engagement of US utility operators occurred in what is referred to as “Phase 1a – US Assessment of Japanese Basic HSI System”. This phase identified any changes needed from the Japanese Basic HSI System due to US cultural or operating method differences. Phase 1a was conducted using a full scale simulation of the Japanese HSI System with known changes for language and cultural differences. Phase 1a used a high fidelity simulation model for a conventional 4 loop PWR plant.

Phase 1a also included completion of the Operating Experience Review program element. This program element expands the OER originally done for the Japanese Standard HSI System to encompass operating experience at US nuclear plants and to encompass additional generic digital HSI technology experience.

Phase 1a was completed 12/2008. (References 44 and 45)

The second engagement of US operators occurred in what is referred to as “Phase 1b – US-APWR US Basic HSIS”. This phase design, verified and validate any changes needed from Phase 1a due to any Human Engineering Deficiencies (HEDs) identified from Phase 1a. The HSI system simulator of Phase 1a was modified, as necessary, for Phase 1b. Phase 1b was completed by 6/2009. This will include an update of Section 4 of this topical report to reflect the design changes made to the US Basic HSIS, as ordinarily described in Section 4. Completion of Phase 1b marks the completion of the US Basic HSIS. This is the US Basic HSIS that will be applied to all US new plant and operating plant upgrade applications. This is the US Basic HSIS for which MHI is seeking NRC generic approval via this topical report.

The first application of the generically approved US Basic HSIS will be for the US-APWR. As defined by the HFE Program Plans in the US-APWR DCD, the specific HSI Inventory for the US-APWR (i.e., specific alarms, indications, controls and operating procedures) is generated by the execution of these program elements. MHI refers to this first application of the US Basic HSIS, as Phase 2. “Phase 2a – US-APWR HFE Analysis” will include completion of the following additional program elements:

- Function Requirements and Function Allocation
- Human Reliability Analysis
- Task Analysis

Phase 2a was completed 06/2009. (Reference 45)

“Phase 2b - US-APWR HSI System Design” will design the US-APWR HSI inventory, including operating procedures, based on the analysis done in Phase 2a, and it will verify and validate that HSI inventory. Phase 2b will also create the US-APWR staffing, training program and human performance monitoring program.

Phase 2b validation is conducted using a full scale simulation of the US-APWR HSI system which includes the US-APWR HSI Inventory implemented within the US Basic HSIS from Phase 1b. Phase 2b validation uses a high fidelity simulation model for the US-APWR.

For the US-APWR, Phase 2 will be completed by 12/2017.

Phase 2 will be repeated for each operating plant upgrade. This phase will generate the HSI system for that specific plant (i.e., the plant specific HSI inventory implemented on the US Basic HSIS from Phase 1b). For each plant, Phase 2 validation will be conducted on a full scale HSI simulator with a high fidelity simulation of the specific plant model. However, the scope of Phase 2, for any specific operating plant, will be tailored, as described in the "Plant Licensing Documentation", which includes the plant specific HFE Program Plan.

Phase 2 for the US-APWR is ~98% applicable to all US-APWR sites. ~2% of the Phase 2 HFE activities will be based on site specific assumptions, for systems such as the Ultimate Heat Sink and Switchyard. Therefore, MHI included a third phase in the HFE program, which is specific for each US-APWR site. "Phase 3a – Site Specific HSI System", validates the site specific assumptions from Phase 2, or conducts a design change process, where needed. Depending on the extent of those changes, Phase 3a may include additional validation activities using the site specific Operator Training simulator. For the first US-APWR, which is CPNPP 3&4, Phase 3a will be completed 9/2012.

When Phase 3a is complete the Operator Training simulator is turned over to the site's training department for "Phase 3b- Site Specific Operator Training". Operator training will be complete for the first US-APWR by 2016 to support pre-op testing and fuel load.

It is noted that due to the minimal standardization in most current US plants, for an operating plant upgrade, Phase 2 is a plant specific and site specific activity. However, there may be some applications where Phase 2 would be applicable to a group of plants, such as for CE System 80 plants or Westinghouse SNUPPS Plants, and then Phase 3a would be added for each site specific application. Otherwise, for an operating plant upgrade, Phase 3 will only include Site Specific Operator Training.



Figure C-1 The Facility used for Phase 1 V&V in U.S.

Appendix D Scope of the US Basic HSI System and Plant Specific HSI System

The HSI system described in Section 4 of the topical report is what MHI refers to as the US Basic HSIS. The table below identifies the “Scope of the US Basic HSIS” and how it is applied to specific plants. The column labeled “Plant Specific HSI Inventory” reflects the systems (mechanical, electrical and I&C), safety analysis, D3 coping analysis and HFE analysis, for each plant. These analyses are reassessed for each plant even though the analyses may be very similar among different plant types.

Within this context “Plant” refers to a specific nuclear unit or a family of units that share the same design. For example, the US-APWR is a plant, as is System 80 and SNUPPS. When “Plant” refers to a family of units that share the same design, there are site specific variations, such as interconnections to the grid and to the ultimate heat sink. HFE analysis is a Phase 2 activity for each plant. For plant families, site specific variations are accommodated in Phase 3. These Phases of the HFE program are described in Appendix C.

MUAP-07007 Section	Scope of the US Basic HSI System	Plant Specific HSI system
4.1 Design Basis	Use of soft touch controls, and displays based on computer processed data. Standardized visual coding.	None
a. Integration of monitoring and operation	Methods of integrating multi-channel data and controls. Areas where multi-channel HSI is utilized.	None
b. automatic verification of component status	Automated checking method, display and alarm method (icons and behavior, display on LDP with drill-down displays). Applies to all functions automatically initiated by the RPS and ESFAS, and all system level safety related interlocks.	Specific safety functions, interlocks, components and their acceptable states.
c. Inter-linked screen request	Navigation methods and selection options (procedures, alarms, graphics, controls).	Specific linked screens.
d. Use of Large Display Panel for situation awareness and information sharing	Information selection criteria (critical power and safety functions, and their success paths) and display method (icons and behavior).	Critical safety functions and success paths differ between NSSS vendors. Success paths vary for power production functions based on BOP design.
e. Alarm prioritization system	Alarm processing method, prioritization method, display and acknowledgement method.	Specific alarm conditions.
f. Main Control Room Staff	Minimum and maximum number of operators.	Actual number of operators for each operating crew
g. Applicable plant personnel	US Basic HSI addresses the needs of operations staff only.	HSI needs of non-operating personnel is outside the scope of the US Basic HSI.
4.2 HSI System Facilities	HFE design process encompasses all facilities identified. However, US Basic HSI design is used only at MCR, RSR and TSC.	HSI design for EOF and local stations.

MUAP-07007 Section	Scope of the US Basic HSI System	Plant Specific HSI system
4.2.1 Main Control Room	Content of physical work areas, HSI devices and layout of consoles, design basis for MCR fire propagation.	Actual console and work area arrangements are based on architectural constraints.
4.2.2 Remote Shutdown Room	Design basis, HSI devices and layout of console, transfer design.	Actual console arrangement is based on architectural constraints.
4.2.3 Technical Support Center	Content of physical work areas. HSI detailed design and content is same as MCR.	HSI devices and layout of consoles. Actual console and work area arrangements are based on architectural constraints.
4.2.4 Interface with Emergency Operation Facility	HSI inventory is received from SPDS. SPDS design basis and information content is part of US Basic HSI design.	Detailed HSI implementation design is unique for each plant. EOF implementation detail is the licensee's responsibility.
4.2.5 Local Control	None	HSI design is unique for each plant.
4.3 Layout Design 4.3.1 Main Control Room Layout (including subsection a-c)	General arrangement and maximum distance between consoles. Minimum LDP character size.	Actual console and work area arrangements are based on architectural constraints.
4.3.2 Operator Console Layout	Number and arrangement of VDUs at each console. Location of Class 1E switches for system level actuation of safety functions. Design basis of LDP, Operational VDUs, Safety VDUs, diverse HSI. LDP size.	Specific safety function switches and diverse HSI devices. LDP size is addressed in 4.9.2.
4.4 Display Overview and Navigation 4.4.1 Display Overview	Purpose of each VDU type.	None
4.4.2 Display Navigation System a. Operational VDU b. Safety VDU c. Alarm display navigation d. Operating procedure display navigation	Display hierarchy, and vertical and horizontal navigation method within the hierarchy. Features and style guide for navigation touch controls.	Specific navigational links on Operational VDUs and Procedure VDUs.
4.5 Operational VDU Display Design 4.5.1 Operation Devices	Display type and approximate screen size.	Actual screen size based on technology evolution and availability.
4.5.2 Operation Method a. Calling Up Switches	Method of navigating to pop-up control windows. Ability to relocate pop-up control windows.	None.
b. Controller and Mode Selector	Design basis and content for displays with fixed controls. Available functions for modulating controls.	Design of specific displays with fixed controls, and the grouping of fixed controls are based on task analysis.
c. Displaying Screens Related to Soft Operations	Style guide for soft controls.	None
4.5.3 Switch Features a. ON/OFF Switches Operation Related Information Display Feature	Features and layout of discrete control window. Tag-out method and displays.	None
b. Manual Operation of controller Information Display Feature	Features and layout of modulating control window.	None
c. Provisions to Prevent Erroneous Operation	Control access and activation features. Operation of cascaded controls.	Specific functions that utilize cascaded controls
4.6 Safety VDU Display Design 4.6.1 Operable Devices	Display type and approximate screen size.	Actual screen size based on technology evolution and availability.
4.6.2 Operational VDUs Connect/Disconnect	Interlock description for control of safety components from Operational VDUs.	None

MUAP-07007 Section	Scope of the US Basic HSI System	Plant Specific HSI system
4.6.3 Monitor Screen	Navigation method, layout and content of monitoring screens	Specific menus and displayed parameters.
c. Operation Screen	Navigation method, layout and content of control screens.	Specific menus and displayed components.
4.7 Alarm System	Design basis.	
4.7.1 Alarm Display System	Alarm display locations, categorization, acknowledgment states and icon behavior.	None
a. Display Location		
b. Allocation of roles between the Alarm VDU and the Large Display Panel	Correlation between alarms on LDP and alarm VDU. Navigation methods, acknowledgement methods, design and behavior of displays for dynamically prioritized alarms.	Specific alarm conditions.
4.7.2 Alarm Prioritization	Static prioritization categories.	Static prioritization category for each alarm.
c. Prioritization Based on Specific Importance (Static Prioritization)		
d. Prioritization Based on Dynamic Prioritization (Dynamic Prioritization)	Categories and rules for dynamic alarm prioritization.	Initial category, dynamic logic and associations, and resulting category for each alarm.
4.7.3 Coding by Alarm Sound	Sound coding for first out alarms, dynamic prioritization categories, bypasses and permissives.	None
4.7.4 First-out Alarms Displaying	Trigger categories, display locations, time sequenced display.	Specific trigger conditions.
4.7.5 Acknowledging and Resetting Alarms & Stopping Alarm Sound	Alarm control functions and locations for acknowledgement and sounds.	None
4.7.6 Avoiding Nuisance Alarms	Design basis of logic to distinguish normal vs. alarm conditions.	Actual alarm distinction logic.
4.7.7 Link to Related Display	Navigational links from alarms on alarm VDU to displays on Operational VDU and procedures on Procedure VDU	Specific linked displays and procedures are defined for each alarm.
4.8 Computer-Based Operating Procedure	Screen layout, style guide, navigation and paging controls, hyperlink controls, place keeping controls. Paper to electronic conversion method and configuration control.	Specific procedures.
4.9 Large Display Panel	Goals of LDP	None
4.9.1 Purpose of Large Display Panel Installation		
4.9.2 Large Display Panel Screen Display Features	None	Screen size is adjusted to accommodate architectural constraints. For example, smaller screens may be used and duplicated, as necessary.
4.9.2.1 Fixed Display Area	Design basis for different plant conditions.	Specific indications and alarms vary based on safety functions and success paths. Table 4.9-1 is typical.
4.9.2.2 Variable Display Area	Design basis for automatic display presentation. Controls for manual display selection.	Specific conditions that activate automatic display presentation.

MUAP-07007 Section	Scope of the US Basic HSI System	Plant Specific HSI system
4.9.3 Alarm Display on the Large Display Panel	Style guide for LDP component and icons and related alarms.	Specific components represented.
a. Flow Sheet Image		
b. Abbreviation of Alarm Name		
c. Message Slot System	Style guide for LDP process parameters and related alarms.	Specific parameters represented.
d. First-out Alarm	Alarm categories and display method	Specific alarms within each category.
e. Shared Alarms	Prioritization display and behavior for grouped alarm icons.	Grouped alarm icons and the specific alarms within each group.
f. SDCV Alarms and BISI status	Design basis categories.	Specific alarms within each category.
4.10 Automatic Checking of Actuators	Design basis for component status monitoring.	Specific components monitored.
4.10.1 Integration of Monitoring and Operation		
4.10.2 Automatic Checking of Actuators for Events	Design basis and method for automatic checking of automatic safety function actuators.	Specific functions and specific components within each function, to correspond with EOPs.
4.10.3 Automatic Verification of Critical Safety Functions	Design basis and method for automatic checking of critical safety function status.	Specific functions and specific parameters and logic within each function, to correspond with EOPs.
4.11 Response to HSI Equipment Failures	Design basis for normal and degraded HSI conditions.	None
4.11.1 Standard Configuration	Design basis for normal HSI conditions. Operation is confirmed during Phase 1 V&V activities.	Operation is confirmed during Phase 2/3 V&V activities.
4.11.2 Degraded HSI Systems by a Single Failure	LDP failure and contingency conditions. Workstation VDU failure conditions. Operation is confirmed during Phase 1 V&V activities.	Operation is confirmed during Phase 2/3 V&V activities.
4.11.3 Loss of All Non-safety HSI	HSI for continued operation. Operation is confirmed during Phase 1 V&V activities.	Operation is confirmed during Phase 2/3 V&V activities.
4.11.4 Loss of All Digital Non-safety and Safety HSI (CCF)	HSI for coping with accident conditions. Operation is confirmed during Phase 1 V&V activities.	Operation is confirmed during Phase 2/3 V&V activities.
4.11.5 Loss of MCR	HSI for coping with conditions that require MCR evacuation. V&V conducted for 4.11.3 bounds this condition.	V&V activities are limited to location and actuation of MCR/RSR transfer switches.
4.12 Key Technical Issues		
a. Multi-channel operator stations	Design basis for multi-channel Operational VDUs and backup channelized Safety VDUs.	Specific information and controls on each display.
b. HSI to accommodate reduced operator staffing	Design basis for HSI features that facilitate minimum operator staffing.	None
c. Operation under Degraded Conditions	See 4.11, above.	See 4.11, above.
d. Minimum inventory of HSI	Minimum inventory is defined for SDCV HSI and HSI to accommodate degraded HSI conditions. Class 1E HSI is provided for all Class 1E instrumentation and plant components.	Specific inventory within each design basis category.
e. Computer based procedures	Design basis and quality program.	Specific procedures are developed under the plant quality program.
5.1 Human Factors Engineering Program Management		
5.1.1 Human Factors Engineering Program	HFE program management basis. Program goals, assumptions, constraints;	For the US-APWR the program management plan is in Section 18.1 of the

MUAP-07007 Section	Scope of the US Basic HSI System	Plant Specific HSI system
	applicable facilities, procedures, personnel.	DCD. Each plant will have a program management plan.
5.1 Human Factors Engineering Program Management 5.1.1 Human Factors Engineering Program	HFE program management basis. Program goals, assumptions, constraints; applicable facilities, procedures, personnel.	For the US-APWR the program management plan is in Section 18.1 of the DCD. Each plant will have a program management plan.
5.1.2 Human Factors Engineering Design Team and Organization	Roles and qualifications for Design Team and V&V Team personnel.	Division of responsibility between design organizations. Specific team members are identified in each program element report.
5.1.3 Human Factors Engineering Processes and Procedures	Overview of key processes	Implementation procedures for each program element are addressed below.
5.1.4 Human Factors Engineering Issues Tracking	Database description and tracking process.	HEDs for each project are identified and tracked.
5.1.5 Human Factors Engineering Technical Program and Milestones	Identification and relationship of each HFE program element.	Schedule for completion of each HFE program element.
5.2 Operating Experience Review (OER)	Process description. The OER report in Part 2 of "US-APWR Human System Interface Verification and Validation (Phase 1a) Technical report" (MUAP-08014) identifies issues that are resolved through the US Basic HSIS.	Issues that are resolved through the Plant Specific HSI Inventory are assessed for each plant. For the US-APWR the implementation plan is in Section 18.2 of the DCD. The OER report in Part 2 of "US-APWR Human System Interface Verification and Validation (Phase 1a) Technical report" (MUAP-08014) contains the implementation procedure and OER report. The OER report identifies issues that are resolved through the Plant Specific HSI Inventory of the US-APWR. Each plant will have an implementation plan and report. The report will summarize the implementation procedure.
5.3 Functional Requirement Analysis and Functional Allocation	Scope of program element, and emphasis on changes from historical practices.	For the US-APWR the implementation plan is in Section 18.3 of the DCD. The FRA/FA procedure and report will be included in "US-APWR Human System Interface Design Technical report". Each plant will have an implementation plan and report. The report will summarize the implementation procedure.
5.3.1 Functional Requirements Analysis	Decomposition method based on critical safety functions, plant events that threaten those functions, success paths to control the critical safety functions. Decomposition example.	Plant specific functional decomposition.
5.3.2 Function Allocation	Function allocation rules and considerations for manual/automatic task allocation.	Plant specific manual/automatic task allocation.

MUAP-07007 Section	Scope of the US Basic HSI System	Plant Specific HSI system
5.4 Task Analysis 5.4.1 Objective of Task Analysis	Relationship of Task Analysis to other program elements.	For the US-APWR the implementation plan is in Section 18.4 of the DCD. The TA procedure and report will be included in "US-APWR Human System Interface Design Technical report". Each plant will have an implementation plan and report. The report will summarize the implementation procedure.
5.4.2 Scope of Task Analysis	Task selection criteria.	Actual tasks selected for analysis.
5.4.3 Methodology for Task Analysis	Task decomposition and workload analysis methods, with increased level of detail as design progresses.	Plant specific analysis for successive design phases.
5.5 Staffing and Qualification Requirements	Personnel responsible for O&M directly related to plant safety. Minimum and maximum design basis for operations staff. Actual operations staffing is plant specific. Maintenance staff is plant specific.	For the US-APWR the implementation plan is in Section 18.4 of the DCD. The US-APWR Staffing analysis will be implemented in Phase 2b. Each plant will have an implementation plan and report. The report will summarize the implementation procedure.
5.5.1 Operator Staffing Level	Qualifications for operating personnel.	No additional information.
5.5.2 Number of Operators per Shift	Minimum and maximum operations staff and their role.	Actual operations staff.
5.6 Human Reliability Analysis 5.6.1 Objectives of HRA	Basis of program element.	For the US-APWR the implementation plan is in Section 18.6 of the DCD. The HRA procedure and report will be included in "US-APWR Human System Interface Design Technical report". Each plant will have an implementation plan and report. The report will summarize the implementation procedure.
5.6.2 Scope of HRA	Task selection based on risk significance.	Specific high risk tasks identified.
5.6.3 HRA Methodology	Overview of THERP methodology.	No additional information.
5.6.4 HRA using THERP	Analysis process using THERP.	Summary of THERP analysis for specific tasks. Confirmation that HSI assumptions in PRA are correct.
5.7 HSI Design 5.7.1 HSI Design Objective	Design basis.	For the US-APWR the implementation plan is in Section 18.7 of the DCD. The US-APWR HSI design will be implemented in Phase 2b. Each plant will have an implementation plan and report. The report will summarize the implementation procedure.
5.7.2 Scope of HSI Design	Selection basis for facilities and tasks.	Plant specific facilities and tasks identified.

MUAP-07007 Section	Scope of the US Basic HSI System	Plant Specific HSI system
5.7.3 HSI Design Methodology	See table entries for Section 4.	See table entries for Section 4.
5.8 Operating Procedure Development Plan 5.8.1 Procedures to be Developed	Scope of Operating Procedures	For the US-APWR the implementation plan is in Section 18.8 of the DCD. The US-APWR Operating Procedures will be developed in Phase 2b. Each plant will have an implementation plan and report. The report will summarize the implementation procedure.
5.8.2 Procedures Development Process	Description of multi-disciplined procedure development process.	Plant specific procedures for all operating scenarios.
5.9 Training Program Development Plan 5.9.1 Training Program	Program basis.	For the US-APWR the implementation plan is in Section 18.9 of the DCD. The US-APWR Training program will be developed in Phase 2b. Each plant will have an implementation plan and report. The report will summarize the implementation procedure.
5.9.2 Operator Training Simulator Fidelity	Simulation requirements.	Plant specific simulator design.
5.9.3 Class Room Training for Operators and Technicians	Scope of classroom training.	Plant specific training courses.
5.9.4 Instructor Qualifications and Training	Instructor requirements	Actual instructor qualifications.
5.9.5 Role of the HFE Design Team in the Training Development Program	Program basis.	Plant specific training courses.
5.9.6 Training Program Modifications	Program basis.	Plant specific training courses.
5.9.7 Retraining	Program basis.	Plant specific training courses.
5.10 Human Factors Verification and Validation 5.10.1 Principle of Verification and Validation (V&V)	Program basis	No additional information.
5.10.2 Implementation Plan for HFE V&V	Key elements of V&V plan.	For the US-APWR the implementation plan is in Section 18.10 of the DCD. The US-APWR V&V will be implemented in phase 2b. Each plant will have an implementation plan and report. The report will summarize the implementation procedure.
5.10.3 Organization of V&V Team	Requirements for V&V team qualifications.	Actual personnel qualifications.
5.11 Design Implementation Plan	Overview of design change implementation plan for new plants and operating plants.	For the US-APWR the implementation plan is in Section 18.11 of the DCD. This plan governs design changes after validation. Each plant will have an implementation plan and report. The report will summarize the implementation procedure.
5.12 Human Performance Monitoring Plan	Program basis	For the US-APWR the implementation plan is in Section 18.12 of the DCD. The documents the process and responsibilities for

MUAP-07007 Section	Scope of the US Basic HSI System	Plant Specific HSI system
		tracking HEDs to resolution. Each plant will have an implementation plan and report. The report will summarize the implementation procedure.