

Safety I&C System Description and Design Process

Non-Proprietary Version

May 2011

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

Revision History

Revision	Date	Page (section)	Description
0	March 2007	All	Original issued
1	July 2007		<p>The following items are revised based on NRC comments or erratum correction.</p> <p>xii List of Acronyms “Design Certification Document” →”Design Control Document”</p> <p>5 Erratum correction (3.1) (b) “Invokes IEEE Std. 603-1991” → “(h) Invokes IEEE Std. 603-1991”</p> <p>10 Conformance to RG 1.209 is added. (3.3)</p> <p>17 Figure 4.1-1 is modified. (4.1) <ul style="list-style-type: none"> • Erratum correction “operational procedure VDU” → “operating procedure VDU” • The figure is changed to colored Figures. </p> <p>21 (11)“Operation Procedures VDU Processor” (4.1) →”Operating Procedure VDU Processor”</p> <p>22 Description of engineering tool is modified. (4.1) <ul style="list-style-type: none"> • “portable personnel computer” →”personnel computer” • Description for administrative control of engineering tool connection is added. </p> <p>27 Description of the input route for DAS signal is added. (4.1)</p> <p>31 Description of the sensor inputs signal to PSMS is added. (4.2.1)</p> <p>34 Description of SLS I/O module is modified. (4.2.3) <ul style="list-style-type: none"> • “power interface devices” → “Power interface (PIF) modules” • Description of PIF modules is added. </p> <p>44 Figure 4.2-2 is changed to colored Figures. (4.2.6)</p>

Revision	Date	Page (section)	Description
1 (continued)		49 (4.5)	Figure 4.4-1 is modified. <ul style="list-style-type: none"> • Erratum correction “Manual RT signal for ...” • The figure is changed to colored Figures.
		50,51 (4.5)	Figure 4.4-2 and 4.4-3 are changed to colored Figures.
		54 (5.1.7)	Erratum correction in Figure 5.1-1 “component” → “component”
		60 (5.2.5)	Composition of Electrical Power is modified. <ul style="list-style-type: none"> • “non-safety AC” → “safety-rated AC” • Description of non-safety AC transfer is deleted. • “Emergency Generators through qualified isolation devices” → “Alternate Power Source”
		61,62 (5.2.5)	Figure 5.2-1, 5.2-2 and 5.2-3 are modified. <ul style="list-style-type: none"> • Transformer is changed to Safety Class in Figure 5.2-1 and 5.2-2. • “Emergency Generator” is changed to “Alternate AC Power Source” in Figure 5.2-3. • “Safety Division” and “Example of UPS for Backup Power Source” is deleted in Figure 5.2-3.
		71 (6.4.1)	Description of Engineering Tools is modified.
		82 (7.0)	Description of document availability is added.
2	December 2008	xiv	The following items are revised based on RAI response (UAP-HF-08144), and erratum correction and clarification are implemented. <p>List of Acronyms</p> <ul style="list-style-type: none"> • Balance of Plant (BOP) is added • “Combined Licensing” → “Combined License”
		2, 3 (3.1)	Description of conformance to GDC 15 is added to follow the response (UAP-HF-08144) to RAI-01.

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

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

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

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

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

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

Revision	Date	Page (section)	Description
4 (continued)		34 (4.2.3)	Editorial correction Description of a fail mode of a PIF module is added to follow the response (UAP-HF-10045) to RAI 516-4027.
		35 (4.2.3)	Editorial correction Description of Functional Assignment Analysis of SLS is added.
		36 (4.2.3)	Editorial correction <ul style="list-style-type: none"> ▪ “The SLS interlocks” → “The SLS receives interlocks from the RPS” “through the application software” → “through the component level application software”
		36 (4.2.4 b)	Following sentences are added to follow the action item at the public meeting. <ul style="list-style-type: none"> ▪ However, ...Class 1E criteria. ▪ For all design basis event, ... Class 1E criteria.
		38 (4.2.5 a)	Editorial correction <ul style="list-style-type: none"> ▪ “IEEE 603” → “IEEE 603-1991”
		41 (4.2.5 c)	Editorial correction <ul style="list-style-type: none"> ▪ “HSI” → “Class 1E credited HSI”
		41 (4.2.5 c)	Editorial correction Description of the write permission function of PSMS controllers is added.
		42 (4.2.5 c)	Editorial correction <ul style="list-style-type: none"> ▪ “component level” → “component level Lock function”
		42 (4.2.5 c)	Editorial correction Description of the priority between S-VDU and O-VDU is revised.
	43 (4.2.6)	Editorial correction <ul style="list-style-type: none"> ▪ “and processors” → “, processing logic and outputs” 	

Revision	Date	Page (section)	Description
4 (continued)		44 (4.2.6)	<p>Editorial correction</p> <ul style="list-style-type: none"> ▪ “or train level” → “, train or component level” ▪ “Spurious actuation... in the plant safety analysis.” → deleted ▪ “disconnect and termination” → “disconnect terminations” ▪ “within the PIF module” → “within the 2-out-of-2 logic of the PIF module”
		51 (4.3)	<p>Following sentence is added to follow the action item at the public meeting.</p> <ul style="list-style-type: none"> ▪ “This automated cross-channel checking is credited to replace manual cross-channel checking in plant technical specification surveillances.”
		51 (4.4)	<p>Following sentence is added to follow the action item at the public meeting.</p> <ul style="list-style-type: none"> ▪ “Manual testing overlaps with self-diagnostics to ensure the integrity of the self-diagnostics.”
		51-54 (4.4.1)	<p>Descriptions of equivalent tests in conventional plants are added.</p>
		52 (4.4.1)	<p>Description of Analog process Inputs is added.</p>
		54 (4.4.1)	<p>Description of the configuration of the RTS output interface for each reactor trip breaker is added.</p>
		54 (4.4.2)	<p>Editorial correction</p> <ul style="list-style-type: none"> ▪ “an Operational VDU or Safety VDU” → “any VDU (eg. Operational VDU or Safety VDU)”
		55 (4.4.3)	<p>Description of the failure impact of MELTAC components on system response time is added.</p>
		55 (4.5)	<p>Editorial correction</p> <ul style="list-style-type: none"> ▪ “I/O modules” → “controller failures (including I/O modules)”
	59 (5.1)	<p>Description of Credit for leak detection in Defense-in-Depth and Diversity analysis is deleted to follow the action item at the public meeting.</p>	

Revision	Date	Page (section)	Description
4 (continued)		60-61 (5.1.5)	Editorial correction <ul style="list-style-type: none"> ▪ “BTP HICB-19” → “BTP 7-19”
		61 (5.1.6)	Section 5.1.6 Credit for leak detection in Defense-in-Depth and Diversity analysis is deleted to follow the action item at the public meeting.
		62 (5.1.8)	Editorial correction Description of Appendix C and D is added.
		63 (5.1.9)	Editorial correction <ul style="list-style-type: none"> ▪ “The self-diagnostics discussed above” → “These manual surveillance tests, along with the self-diagnostics and software memory integrity tests discussed above,”
		63 (5.1.10)	Editorial correction <ul style="list-style-type: none"> ▪ “Technical Specifications” → “plant’s maintenance procedures”
		64-65 (5.1.13)	Descriptions of Priority logic are modified to follow the action item at the public meeting.
		67 (5.1)	Figure 5.1-3 is modified to follow the action item at the public meeting.
		68 (5.1)	Figure 5.1-4 is modified to follow the action item at the public meeting.
		69 (5.1)	Editorial correction Figure 5.1-5 is revised.
		70 (5.2.1)	Editorial correction <ul style="list-style-type: none"> ▪ “Seismic Category 1” → “Seismic Category I”
		71 (5.2.5)	Editorial correction Description of power sources for the PSMS is revised.
		74 (6.0)	Reference to the application software life cycle is added to follow the action item at the public meeting.
	77 (6.2)	Editorial correction <ul style="list-style-type: none"> ▪ “...described in this section” → “...summarized in this section” 	

Revision	Date	Page (section)	Description
4 (continued)		77 (6.2)	Editorial correction Following sentence is added. <ul style="list-style-type: none"> ▪ The details are described in MUAP-07017.
		78 (6.2.2 (4))	Editorial correction <ul style="list-style-type: none"> ▪ "...described in this section" → "...summarized in this section"
		78 (6.3)	Editorial correction Description of software life cycle requirements is modified.
		82 (6.4)	Editorial correction <ul style="list-style-type: none"> ▪ "...described in this section" → "...summarized in this section"
		82 (6.4)	Editorial correction Following sentence is added. <ul style="list-style-type: none"> ▪ The details are described in the US-APWR DCD Chapter 7 and MUAP-07017.
		83 (6.4.3)	Editorial correction <ul style="list-style-type: none"> ▪ "the cyber security requirements of NEI 04-04, or equivalent" → "the current NRC cyber security requirements"
		83 (6.4.3)	Editorial correction Followings items are deleted. <ul style="list-style-type: none"> ▪ It is noted that ... to all projects. ▪ In addition, ... cyber security program. ▪ For example, for the US-APWR ▪ In addition, ... resulting defensive model.
		84 (6.5.1)	Editorial correction Added the reference for Functional Assignment Analysis technical report.
		84 (6.5.1)	Editorial correction <ul style="list-style-type: none"> ▪ "Table 6.2-1" → "Table 6.5-1"
		87 (6.5.3)	Editorial correction References to the response time of safety I&C system are added.
	88 (6.5.4)	References are revised to follow the action item at the public meeting.	

Revision	Date	Page (section)	Description
4 (continued)		90 (6.5.6)	Editorial correction Reference to seismic analysis is added.
		91 (6.5.7)	Editorial correction <ul style="list-style-type: none"> “...is based on RG 1.180” → “...complies with RG 1.180”
		92 (6.5.8)	Editorial correction Reference to fire protection and fire protection program is added.
		93 (6.5)	Editorial correction Figure 6.5-4 is revised.
		94 (7.0)	Chapter 7 FUTURE LICENCING SUBMITTALS is deleted due to revision as Technical Report.
		95 (8.0)	Editorial correction References are modified and updated.
		105 (A.5.5)	Editorial correction Description of failure modes of the trip mechanism of the reactor trip breakers and ESF components is added to be equivalent to DCD Chapter 7.
		106 (A.5.6.1)	Description of the justification for the single RCS flow instrument tap is added to follow the action item at the public meeting.
		107 (5.6.3.3)	Editorial correction <ul style="list-style-type: none"> “... the PCMS includes Signal Selection Algorism which prevents...” → “... the PCMS Signal Selection Algorithm prevents...”
		108 (A.5.7)	Description of the Software Memory Integrity test is added to follow the action item at the public meeting.
	111 (A.5.11)	Description of identification of safety related documents is added to follow the action item at the public meeting.	
	116 (A.6.3)	Editorial correction <ul style="list-style-type: none"> “PCMS basic platform software” → “PCMS Signal Selection Algorithm software” 	

Revision	Date	Page (section)	Description
		116 (A.6.3)	Editorial correction Description of Configuration Management is modified.
		119 (A.6.8.1)	Editorial correction · “Nominal setpoint” → “Nominal trip setpoint”
		119 (A.6.8.1)	Descriptions of the allowable value and nominal trip setpoint are modified to follow the action item at the public meeting.
		120, 121 (A.7.3)	Description of the train level latching is revised to follow the action item at the public meeting.
		128 (C.1)	Description of Malfunction and spurious actuation is modified to follow the action item at the public meeting.
		130-158 (Appendix D)	Appendix D is added to follow the action item at the public meeting.
5	October 2010	12 (3.5)	Subsection 3.5 is added with addition of Appendix E to follow Closure Plan for US-APWR Instrumentation and Control Open Issues (UAP-HF-10237).
		12 (3.6)	Subsection number is renumbered.
		13 (3.7)	Subsection number is renumbered.
		15 (3.8)	Subsection number is renumbered.
		17 (Figure 4.1-1)	Revised the footnote to follow UAP-HF-10237.
		22 (4.1 a. (18))	Description of Engineering Tool is revised to follow UAP-HF-10237.
		30 (Figure 4.1-5)	The followings are revised. <ul style="list-style-type: none"> · Configuration of communication sub-system is clarified. · Connection from VDU processors to Consoles are corrected · Number of groups of Safety Logic System is corrected.

Revision	Date	Page (section)	Description
5 (continued)		42 (4.2.5 c)	Description of capability to change MELTAC software for the item “No ability to alter safety software” is revised to follow UAP-HF-10237.
		43 (4.2.5 c)	Description of manual permissive is added to the item “Acceptable safety function performance” for further clarification.
		46 (4.2.7)	The bulleted item for Maintenance Network is added to follow UAP-HF-10237.
		53 (4.4.1)	Description of manual permissive is added to the item “Manual ESF Actuation” for further clarification.
		66 (5.1.13 (1))	Description of the priority logic between S-VDU and O-VDU commands is corrected.
		67 (5.1.13 (3))	Misdescription of permissive for the DHP is deleted.
		67 (5.1.13 (3))	Description of capability to change software is added.
		69 (Figure 5.1-3)	The followings are revised. <ul style="list-style-type: none"> ▪ Priority logic between S-VDU and O-VDU commands ▪ Manual permissive logic ▪ Lock signal
		70 (Figure 5.1-4)	Lock logic is revised.
		82 (6.3.1 (11))	The item “Software Test Plan” is added to be consistent with BTP 7-14.
		84 (6.4.1)	Description of software change is added.
		84 (6.4.1)	Description of Maintenance Network is added.
		99 (A4.3)	Description of manual bypass permissive is added for further clarification.
	120 (A6.6)	Description of manual bypass permissive is added for further clarification.	
	120 (A6.7)	Description of manual bypass permissive is added for further clarification.	

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Table of Contents

List of Tables
List of Figures
List of Acronyms

1.0 PURPOSE	1
2.0 SCOPE	1
3.0 APPLICABLE CODE, STANDARDS AND REGULATORY GUIDANCE	2
3.1 Code of Federal Regulations.....	2
3.2 Staff Requirements Memoranda	6
3.3 NRC Regulatory Guides.....	6
3.4 NRC Branch Technical Positions	10
3.5 NRC Interim Staff Guidance.....	12
3.6 NUREG-Series Publications (NRC Reports).....	12
3.7 IEEE Standards.....	13
3.8 Other Industry Standards	15
4.0 SYSTEM DESCRIPTION	16
4.1 Overall I&C System Architecture	16
4.2 Detailed Description of Safety-Related Systems.....	31
4.2.1 Reactor Protection System (RPS)	31
4.2.2 ESF Actuation System (ESFAS).....	32
4.2.3 Safety Logic System	34
4.2.4 Safety-Related HSI System	36
4.2.5 Plant Control and Monitoring System	38
4.2.6 Diverse Actuation System.....	43
4.2.7 Digital Data Communication	44
4.3 PSMS Self-diagnostic Features	51
4.4 PSMS Manual Testing and Calibration Features	52
4.4.1 Manual Testing.....	52
4.4.2 Manual Calibration (CHANNEL CALIBRATION).....	56
4.4.3 Response Time Test	56
4.5 PSMS On-line Maintenance	57
5.0 DESIGN BASIS	62
5.1 Key Technical Issue	62
5.1.1 Multi-Channel Operator Station	62
5.1.2 HSI to Accommodate Reduced Operator Staffing	62
5.1.3 Operation under Degraded Conditions.....	63
5.1.4 Integrated RPS & ESFAS with Functional Diversity	63
5.1.5 Common Cause Failure Modes for Defense-in-Depth and Diversity Analysis.....	64
5.1.6 This section intentionally left blank	64
5.1.7 Output Module for PSMS and DAS	64
5.1.8 Control System Failure Mode	65
5.1.9 Credit for Self-Diagnosis for Technical Specification Surveillance.....	65
5.1.10 Unrestricted Bypass of One Safety-Related Instrument Channel.....	66
5.1.11 Minimum Inventory of HSI.....	67
5.1.12 Computer Based Procedures	67
5.1.13 Priority Logic.....	67

5.2 This section intentionally left blank.....	75
6.0 DESIGN PROCESS	76
6.1 This section intentionally left blank.....	76
6.2 This section intentionally left blank.....	76
6.3 This section intentionally left blank.....	76
6.4 This section intentionally left blank.....	76
6.5 Analysis Method	77
6.5.1 FMEA Method.....	77
6.5.2 Reliability Analysis Method	78
6.5.3 Response Time Analysis Method.....	79
6.5.4 Accuracy Analysis Method	80
6.5.5 Heat Load Analysis Method.....	82
6.5.6 Seismic Analysis Method.....	82
6.5.7 EMI Analysis Method	83
6.5.8 Fire Protection Analysis	84
7.0 This section intentionally left blank	86
8.0 REFERENCES	87
Appendix A Conformance to IEEE 603-1991	88
A.1. Scope.....	88
A.2. Definitions	88
A.3. References.....	88
A.4. Safety System Designation.....	88
A.4.1 Design Basis Events	88
A.4.2 Safety Functions and Corresponding Protective Actions	88
A.4.3 Permissive Conditions for Each Operating Bypass Capability	88
A.4.4 Variables Required to be Monitored for Protective Action	89
A.4.5 The Minimum Criteria for Each Action Controlled by Manual Means	90
A.4.6 Spatially Dependent Variables.....	91
A.4.7 Range of Conditions for Safety System Performance.....	91
A.4.8 Functional Degradation of Safety Functions	91
A.4.9 Reliability.....	92
A.4.10 The Critical Points in Time or the Plant Conditions	92
A.4.11 Equipment Protective Provisions.....	92
A.4.12 Other Special Design Basis.....	94
A.5. Safety System Criteria	94
A.5.1 Single Failure Criterion.....	94
A.5.2 Completion of Protective Action	95
A.5.3 Quality	95
A.5.4 Equipment Qualification	95
A.5.5 System Integrity.....	95
A.5.6 Independence	95
A.5.7 Capability for Test and Calibration.....	98
A.5.8 Information Displays.....	100
A.5.9 Control of Access	101
A.5.10 Repair.....	101
A.5.11 Identification	101
A.5.12 Auxiliary Features.....	102
A.5.13 Multi-Unit Stations	102
A.5.14 Human Factors.....	102
A.5.15 Reliability.....	102
A.5.16 Common Cause Failure (IEEE 603-1998).....	103

A.6. Sense and Command Features - Functional and Design Requirements.....	103
A.6.1 Automatic Control	103
A.6.2 Manual Control	104
A.6.3 Interaction between the Sense and Command features and other Systems	106
A.6.4 Derivation of System Inputs	106
A.6.5 Capability for Testing and Calibration	106
A.6.6 Operating Bypasses	106
A.6.7 Maintenance Bypass	107
A.6.8 Setpoint	108
A.7. Executive Features - Functional and Design Requirements.....	109
A.7.1 Automatic Control	109
A.7.2 Manual Control	109
A.7.3 Completion of Protective Action	109
A.7.4 Operating Bypass	110
A.7.5 Maintenance Bypass	110
A.8. Power Source Requirements	110
Appendix B Conformance to IEEE 7-4.3.2 -2003.....	111
B.1. Scope.....	111
B.2. References.....	111
B.3. Definitions and abbreviations.....	111
B.4. Safety System Design Basis.....	111
B.5. Safety System Criteria	111
B.5.1 Single Failure Criterion.....	111
B.5.2 Completion of Protective Action	111
B.5.3 Quality	111
B.5.4 Equipment Qualification	112
B.5.5 System Integrity.....	112
B.5.6 Independence	113
B.5.7 Capability for Test and Calibration.....	115
B.5.8 Information Displays.....	115
B.5.9 Control of Access	115
B.5.10 Repair.....	115
B.5.11 Identification	115
B.5.12 Auxiliary Features.....	115
B.5.13 Multi-Unit Stations	115
B.5.14 Human Factors.....	115
B.5.15 Reliability.....	115
B.6. Sense and Command Features - Functional and Design Requirements.....	115
B.7. Executive Features - Functional and Design Requirements.....	115
B.8. Power Source Requirements	115
Appendix C Prevention of Multiple Spurious Commands and Probability Assessment	116
C.1. Prevention of Multiple Spurious Commands.....	116
C.2. Probability Assessment	118
Appendix D Analysis of Operational VDU (O-VDU) and PCMS Spurious Commands.....	119
D.1 Purpose	119
D.2 Evaluation Condition.....	123
D.3 Failure Tolerance Methods	124
D.4 Analysis	127
Appendix E Conformance to ISG-04	157

E1. Interdivisional Communications	158
E2. Command Prioritization.....	175
E3. Multidivisional Control and Display Stations	180
E3.1 Independence and Isolation	180
E3.2 Human Factors Considerations.....	186
E3.3 Diversity and Defense-in-Depth (D3) Considerations	189
Appendix F Safety-related Digital I&C Design Detail Conformance to Essential Safety Criteria	192
F.1 RPS.....	193
F.1.1 Redundancy.....	193
F.1.2 Independence	193
F.1.3 Determinism.....	197
F.1.4 Diversity	198
F.1.5 Simplicity.....	198
F.2 ESFAS, SLS, COM and Safety-Related HSIS	204
F.2.1 Redundancy.....	204
F.2.2 Independence	204
F.2.3 Determinism.....	212
F.2.4 Diversity	212
F.2.5 Simplicity.....	212
Appendix G The Failure Modes and Effects Analyses (FMEA) for PSMS	223
G.1 Purpose	223
G.2 Evaluation Condition.....	223
G.3 Analysis and Conclusion	223
Appendix H Bases for the Selection of the US-APWR PAM Variables.....	260
H.1 Type A Variables	260
H.2 Type B Variables	261
H.3 Type C Variables	262
H.4 Type D Variables	262
H.5 Type E Variables	263

List of Tables

Table 6.5-1	Deleted	
Table A.4.4-1	Deleted	
Table A.4.4-2	Deleted	
Table A.5.16-1	Deleted	
Table D.4-1	Analysis of Spurious Erroneous Manual or Automatic Stop Commands for Normally Stopped Component	...127
Table D.4-2	Analysis of Spurious Erroneous Manual Stop Commands for Normally Operated Component	...129
Table D.4-3	Analysis of Spurious Erroneous Manual or Automatic Start Commands for Normally Stopped Component	...130
Table D.4-4	Analysis of Spurious Erroneous Manual or Automatic Open Commands for Normally Opened Valve	...131
Table D.4-5	Analysis of Spurious Erroneous Manual or Automatic Open Commands for Normally Closed Valve	...133
Table D.4-6	Analysis of Spurious Erroneous Manual Close Commands for Normally Opened Valve	...134
Table D.4-7	Analysis of Spurious Erroneous Manual Close Commands for Normally Closed Valve	...136
Table D.4-8	Analysis of Spurious Erroneous Manual Open and Close Commands for Normally Opened Valve	...138
Table D.4-9	Analysis of Spurious Erroneous Automatic Close Commands Normally Opened Valve	...140
Table D.4-10	Analysis of Spurious Erroneous Automatic Close or Stop Commands	...141
Table D.4-11	Analysis of Spurious Erroneous Manual Bypass (Operating Bypass) Commands for Safety-Related Function	...142
Table D.4-12	Analysis of Spurious Erroneous Manual Bypass (Maintenance Bypass) Commands for Safety-Related System	...144
Table D.4-13	Analysis of Spurious Erroneous Manual Bypass (Maintenance Bypass) Commands for Safety-Related Interlock	...147
Table D.4-14	Analysis of Spurious Erroneous Manual Bypass Commands for Accumulator Discharge Valve Open Interlock	...149
Table D.4-15	Analysis of Spurious Erroneous Manual Lock (Stop, Open, Close Lock, etc) Commands for Safety-Related Component	...151
Table D.4-16	Analysis of Spurious Erroneous Manual Reset Commands for Safety-Related Function Signal	...154
Table D.4-17	Analysis of Spurious Erroneous Manual Reset Commands for Reactor Trip	...156
Table F.2-1	Signal List and Functional Independence Design from operational VDU to PSMS	...221
Table F.2-2	Signal List and Functional Independence Design from PCMS to PSMS	...222
Table G.2-1	FMEA for RT in PSMS (for Figure G1-1)	...226

Table G.2-2	FMEA for ESF Actuation in PSMS (for Figure G1-1)	...235
Table H.1-1	Basis for Differences between NUREG-1431 Table 3.3.3-1 and the US-APWR Type A PAM List	...264
Table H.2-1	Basis for Type B Differences between RG 1.97 Rev.3 and the US-APWR PAM List	...267
Table H.3-1	Basis for Type C Differences between RG 1.97 Rev.3 and the US-APWR PAM List	...269
Table H.4-1	Basis for Type D Differences between RG 1.97 Rev.3 and the US-APWR PAM List	...271
Table H.5-1	Basis for Type E Differences between RG 1.97 Rev.3 and the US-APWR PAM List	...276

List of Figures

Figure 4.1-1	The Overall Architecture of the I&C System	...17
Figure 4.1-2	Deleted	
Figure 4.1-3	Deleted	
Figure 4.1-4	Configurations of the Reactor Protection System	...28
Figure 4.1-5	Configurations of the ESFAS,SLS, and Safety-Related HSI	...29
Figure 4.1-6	Configurations of the Reactor Trip Breakers	...30
Figure 4.2-1	Configuration of RSC/MCR Transfer System	...46
Figure 4.2-2	Electrical Independence Features between PCMS and PSMS	...47
Figure 4.2-3	Manual Actuation Configuration for Two-Train ESFAS	...48
Figure 4.2-4	Manual Actuation Configuration for Four-Train ESFAS	...49
Figure 4.2-5	Overlap Testability for DAS	...50
Figure 4.4-1	Overlap Testability for Reactor Trip	...58
Figure 4.4-2	Overlap Testability for ESF Actuation	...59
Figure 4.4-3	Overlap Testability for Safety VDU	...60
Figure 4.4-4	Coverage of Self-diagnostics and Manual Testing	...61
Figure 5.1-1	Signal Interface of Output Module	...64
Figure 5.1-2	Configuration Example of Reactor Control System	...70
Figure 5.1-3	Priority Between Commands from Safety VDU and Operational VDU	...71
Figure 5.1-4	Priority for Manual and Automatic Signals of Safety and Non-Safety Demand	...72
Figure 5.1-5	State-based Priority in PIF	...73
Figure 5.1-6	Manual Permissive Logic for Bypass Signals from Operational VDU	...74
Figure 5.2-1	Deleted	
Figure 5.2-2	Deleted	
Figure 5.2-3	Deleted	
Figure 5.2-4	Deleted	
Figure 6.1-1	Deleted	
Figure 6.2-1	Deleted	
Figure 6.5-1	Typical FTA for Failure of ESF Actuation	...79
Figure 6.5-2	Breakdown Response Time for Reactor Trip	...80
Figure 6.5-3	Typical Calculation Model for Channel Uncertainty of the Instrumentation Loop	...81
Figure 6.5-4	Configuration of Fire Protection for Diverse Actuation System	...85
Figure A.6.2-1	Manual Control	...105
Figure B.5.6-1	Software Isolation (Non-Safety VDU / Safety-Related System)	...114
Figure C.2-1	Probability Assessment Flow	...118
Figure E-1	Component Control Signal Interface from Operational VDU to Safety-Related System	...190

Figure E-2	Operational/Maintenance Bypass, Reset and Lock Signal Interface from Operational VDU to Safety-Related System	...191
Figure F.1-1	Independence Design of RPS	...199
Figure F.1-2	Communication Independence Design among Different Train RPS	...200
Figure F.1-3	Communication Independence Design from RPS to Unit Bus	...201
Figure F.1-4	Overall Signal Interfaces of 2-out-of-4 Bypass Logic	...202
Figure F.1-5	MELTAC Platform Basic Software Processes and Execution Order	...203
Figure F.2-1	Independence Design of ESFAS	...213
Figure F.2-2	Independence Design of SLS	...214
Figure F.2-3	Independence Design of COM	...215
Figure F.2-4	Independence Design of Safety VDU	...216
Figure F.2-5	Communication Independence Design from RPS to ESFAS	...217
Figure F.2-6	Communication Independence Design from COM-1 to Unit Bus	...218
Figure F.2-7	Communication Independence Design from Unit Bus to COM-2	...219
Figure F.2-8	Communication Independence Design between Safety VDU Trains	...220
Figure G.1-1	System Configuration for FMEA of RT and ESF Actuation in PSMS	...225

List of Acronyms

ALR	Automatic Load Regulator
ATWS	Anticipated Transient Without Scram
AVR	Auto Voltage Regulator
BISI	Bypassed or Inoperable Status Indication
BOP	Balance of Plant
CCB	Configuration Control Board
CCF	Common Cause Failure
CDF	Core Damage Frequency
COL	Combined License
OTS	Commercial-Off-The-Shelf
CPU	Central Processing Unit
CRDM	Control Rod Drive Mechanism
DAS	Diverse Actuation System
DMC	Date Management Console
DBA	Design Basis Accident
DC	Design Certification
DCD	Design Control Document
DHP	Diverse HSI Panel
DI	Digital Input
DO	Digital Output
ECC	Error Check and Correct memory
ECCS	Emergency Core Cooling System
EHG	Electro-Hydraulic Governor
ELM	Engineering Line Manager
EMI	Electro-Magnetic Interference
EOF	Emergency Operations Facility
EPM	Engineering Project Manager
EPS	Emergency Power Supply system
ESF	Engineered Safety Features
ESFAS	Engineered Safety Features Actuation System
FMEA	Failure Modes and Effects Analyses
FTA	Fault Tree Analysis
HDSR	Historical Data Storage and Retrieval
HSI	Human System Interface
HSIS	Human System Interface System
HVAC	Heating, Ventilation, and Air Conditioning
I&C	Instrumentation and Control
ICTS	In-Core Temperature System
ID	Identification
ITAAC	Inspections, Tests, Analyses, and Acceptance Criteria
IV&V	Independent Verification and Validation
LBLOCA	Large Break Loss Of Coolant Accident

LCO	Limiting Condition for Operation
LDP	Large Display Panel
LERF	Large Early Release Frequency
LOCA	Loss Of Coolant Accident
LOOP	Loss Of Offsite Power
M/G	Motor Generator
MCR	Main Control Room
MELCO	Mitsubishi Electric Corporation
MHI	Mitsubishi Heavy Industries
MSLB	Main Steam Line Break
MTBF	Mean Time Between Failure
NIS	Nuclear Instrumentation System
OBE	Operational Basis Earthquake
O-VDU	Operational Visual Display Unit
PAM	Post Accident Monitor
PCMS	Plant Control and Monitoring System
PIF	Power Interface
PRA	Probabilistic Risk Assessment
PRC	Process Recording Computer
PSMS	Protection and Safety Monitoring System
QA	Quality Assurance
RCS	Reactor Coolant System
RFI	Radio Frequency Interface
RG	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
RT	Reactor Trip
RTA	Reactor Trip Actuation
RTB	Reactor Trip Breaker
RTD	Resistance Temperature Detector
SDCV	Spatially Dedicated Continuously Visible
SER	Safety Evaluation Report
SLS	Safety Logic System
SBO	Station Black Out
SPDS	Safety Parameter Display System
SRSS	Statistical Square Root Sum
SSA	Signal Selection Algorithm
SSE	Safe Shutdown Earthquake
S-VDU	Safety Visual Display Unit
SWC	Surge Withstand Capability
Tcold	reactor coolant inlet Temperature

Thot	reactor coolant outlet Temperature
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

1.0 PURPOSE

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

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

2.0 SCOPE

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

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

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

3.0 APPLICABLE CODE, STANDARDS AND REGULATORY GUIDANCE

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

Equipment - This refers to the components that are the subject of this Report. "Equipment" includes the MHI safety-related digital I&C systems and the MELCO safety-related digital I&C platform. "Equipment" does not include the MHI non-safety digital I&C or HSI systems nor the MELCO non-safety digital I&C or HSI platforms. It is noted that the MHI non-safety digital I&C systems utilize the MELCO non-safety digital I&C platform which is the same as the MELCO safety-related digital I&C platform. However, some QA aspects of design and manufacturing are not equivalent between safety-related and non-safety systems/platforms.

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 meets the requirements of 10CFR50 Appendix B.
- GDC 2 : Design Bases for Protection against Natural Phenomena
This Equipment is seismically qualified. The Equipment is located within building structures that provide protection against other natural phenomena. Specific buildings and Equipment locations are described in the US-APWR DCD.
- GDC 4 : Environmental and Dynamic Effects Design Bases
This Equipment is located in a mild environment that is not adversely effected by plant accidents.
- GDC 5 : Sharing of Structures, Systems, and Components
There is no sharing of this Equipment among nuclear power units.
- GDC 12 : Suppression of Reactor Power Oscillations
Specific reactor trip functions implemented within this Equipment are described in the US-APWR DCD Chapter 7.
- GDC 13 : Instrumentation and Control
Specific instrumentation and control functions implemented within this Equipment are described in the US-APWR DCD Chapter 7.
- GDC 15 : Reactor Coolant System Design
Steady state and transient analyses are performed to assure that RCS design conditions are not exceeded during normal operation. Protection and control setpoints implemented within this Equipment are based on these analyses. Specific analysis and setpoints are described in the US-APWR DCD Chapter 15.
- GDC 17 : Electric Power Systems
The electric power sources for this Equipment and the plant components controlled

by this Equipment are discussed in the US-APWR DCD Chapter 7 and Chapter 8. This document describes the interface requirements for these power sources.

GDC 19 : Control Room

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

GDC 20 : Protection System Functions

Specific protection system functions implemented within this Equipment are described in the US-APWR DCD Chapter 7.

GDC 21 : Protection System Reliability and Testability

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

GDC 22 : Protection System Independence

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

GDC 23 : "Protection System Failure Modes"

All detected failures are alarmed. The reactor trip functions are designed to fail to an actuated trip state on loss of all power, on failures that are not automatically detected, or on failures that are automatically detected and would prevent proper execution of the trip function. The Engineered Safety Features functions are designed to fail to an unactuated state. The unactuated state avoids spurious plant transients, therefore it is considered the safe state.

GDC 24 : Separation of Protection and Control Systems

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

GDC 25 : Protection System Requirements for Reactivity Control Malfunctions
Specific functions implemented within this Equipment to protect against Reactivity Control Malfunctions are described in the US-APWR DCD Chapter 15. Specific features designed into the MHI non-safety control systems to limit the extent of Reactivity Control Malfunctions are described in the US-APWR DCD Chapter 15.

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

(2) 10CFR50.34 (f)(2) Post-TMI Requirements

- (iii) Control room
The Human Factors design aspects of the HSI and the control room are described in the HSI System Topical Report, MUAP-07007.
- (iv) Safety Parameter Display
The non-safety HSI systems provide safety parameter displays in the control room. Some data presented on safety parameter displays originates in this Equipment.
- (v) Bypassed and inoperable status indication
This indication is provided by this Equipment and by the non-safety HSI system. All bypassed or inoperable signals for safety-related systems originate in this Equipment.
- (xi) Relief and safety-related valve position Indication
- (xii) Auxiliary feedwater system initiation and flow indication
- (xiii) Pressurizer heater control
- (xiv) Containment isolation systems
- (xvii) Accident monitoring instrumentation
- (xviii) Inadequate core cooling monitoring
- (xix) Instruments for monitoring plant conditions following core damage
- (xx) Pressurizer level indication and controls for pressurizer relief and block valves
Specific functions implemented within this Equipment to meet the Post-TMI requirements, items xi thru xx above, are described in the US-APWR DCD Chapter 7.

(3) 10 CFR 50.36 Technical specifications

- (1) Safety-related limits, limiting safety-related system settings, and limiting control settings.
This Equipment is used to maintain safety-related limits. The MHI non-safety control systems are used to maintain control limits.
- (2) Limiting conditions for operation.
This Equipment is configured with N or N+1 redundancy, as discussed above for compliance to GDC 21. For systems with N+1 redundancy there are no limiting conditions for operation (LCO) related to bypassed or out of service conditions for a single instrument channel.

-
- (3) Surveillance requirements
This Equipment includes extensive automatic testing, as discussed above for compliance to GDC 21. Provisions are included for periodic 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. The test interval for all manual tests is based on reliability and risk based analysis.

 - (4) 10 CFR 50.49 Environmental Qualification of Electric Equipment Important To Safety For Nuclear Power Plants
This Equipment is located in a mild environment. A mild environment is an environment that would at no time be significantly more severe than the environment that would occur during normal plant operation, including anticipated operational occurrences. Therefore this criteria is not applicable. This criteria is applicable to some instrumentation that interfaces to this Equipment. The qualification of this instrumentation is described in the US-APWR DCD Chapter 7.

 - (5) 10 CFR 50.55a
 - (a)(1) Quality Standards for Systems Important to Safety
This Equipment was originally developed under a Japanese nuclear quality program that is equivalent to 10CFR50 Appendix B. Other licensing documents describe this equivalence. An approved 10CFR 50 Appendix B quality program is now in effect for all Equipment.

 - (h) Invokes IEEE Std. 603-1991
See conformance to IEEE 603-1991

 - (6) 10 CFR 50.62 ATWS Rule
The Diverse Actuation System (DAS), which is used to actuate plant systems for ATWS mitigation, is described briefly in this Report, and in more depth in the Topical Report for Defense in Depth and Diversity, MUAP-07006. The DAS is diverse from this Equipment, with the exception of the final module that interfaces to plant ESF components. This common module is part of the PSMS described in this Report. The diversity between this Equipment and the DAS is described in the Topical Report for Defense in Depth and Diversity, MUAP-07006.

 - (7) 10 CFR 52.47
 - (a)(1)(iv) Resolution of Unresolved and Generic Safety Issues
 - (a)(1)(vi) ITAAC in Design Certification Applications
 - (a)(1)(vii) Interface Requirements
Conformance to the requirements in items iv thru vii, above, are described in the US-APWR DCD and its references.

 - (a)(2) Level of Detail
The content of this Report, together with the additional information described in other digital system Topical Reports and the US-APWR DCD, is sufficient to allow the NRC staff to reach a final conclusion on all safety-related questions associated with the design. The information includes performance requirements and design information sufficiently detailed to permit the preparation of acceptance and inspection requirements by the NRC, and procurement specifications and construction and installation specifications by an applicant.
-

- (b)(2)(i) Innovative Means of Accomplishing Safety Functions
In the near term, the Equipment is expected to be applied to conventional I&C safety-related and non-safety functions typical of current operating plants and new evolutionary plants. In the longer term, the Equipment is expected to be applied to more innovative safety-related functions as may be typical of new passive plants. All specific plant safety-related functions are described in the US-APWR DCD Chapter 7.
- (8) 10 CFR 52.79(c) ITAAC in Combined Operating License Applications
The inspections, tests, analyses and acceptance criteria that demonstrate that this Equipment has been constructed and will operate in conformity with the Commission's final safety conclusion, will be described in the the US-APWR DCD Tier 1.

3.2 Staff Requirements Memoranda

- (1) SRM to SECY 93-087
- II.Q Defense against Common Cause Failures in Digital I&C Systems
Compliance is described in the Topical Report on Defense-in-Depth and Diversity, MUAP-07006.
 - II.T Control Room Annunciator (Alarm) Reliability
Alarm signals are generated from this Equipment and from MHI non-safety I&C systems. Alarm annunciators are provided by the MHI non-safety HSI system, which is internally redundant. The overall integrated design conforms to separation and independence criteria between trains and between safety and non-safety trains.

3.3 NRC Regulatory Guides

- (1) RG 1.22 Periodic Testing of Protection System Actuation Functions
See GDC 21 compliance. Protection actuation functions are completely testable through a combination overlapping automatic and manual tests. Manual tests can only be conducted when a train is bypassed. Trains are interlocked to prevent concurrent bypassing of redundant functions in more than one redundant train.
- (2) RG 1.29 Revision 3 Seismic Design Classification
The Equipment is designated Seismic Category I. Specific portions of the Equipment whose continued function is not required are designated Seismic Category II. Seismic Category II Equipment is designed so that the Safe Shutdown Earthquake (SSE) will not cause a failure which will reduce the functioning of the safety-related function to an unacceptable level.
- (3) RG 1.47 Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems
See compliance to 10CFR50.34 (f)(2)(v). Alarms are provided for all bypassed or inoperable safety-related 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-related function at the train level. The ability to manually actuate bypassed or inoperable alarms at the train level is provided for conditions that are not automatically detected.
- (4) RG 1.53 Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems

-endorses IEEE Std 379-2000

See compliance to GDC 21 and 24. Safety-related functions are designed with N or N+1 trains. Each train is independent from the other safety trains and from non-safety trains. Independence ensures that credible single failures cannot propagate between trains within the system and therefore can not prevent proper protective action at the system level. Single failures considered in the trains are described in the Failure Modes and Effects Analyses (FMEA) for each system. The FMEA method for the Equipment is provided in this report. The FMEA for safety-related I&C system of the US-APWR is discussed in the US-APWR DCD Chapter 7.

(5) RG 1.62 Manual Initiation of Protective Actions

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

(6) RG 1.75 Physical Independence of Electric Systems

-endorses IEEE 384-1992

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

(7) RG 1.89 Qualification for Class 1E Equipment for Nuclear Power Plants

-endorses IEEE323-1974

The environmental qualification of this Equipment is by an appropriate combination of type testing and analysis. This Equipment is located in a mild environment that is not adversely effected by plant accidents. Therefore qualification for temperature, humidity and radiation is by analysis of component specifications, room ambient conditions and heat rise calculations for the installed configuration. Seismic qualification and EMI qualification are by type testing. This Equipment has no known aging mechanisms; random failures will be detected through periodic surveillance and testing.

(8) RG 1.97 Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants

-endorses IEEE Std. 497-2002

This Equipment is used to process and display signals from accident monitoring instrumentation of all variable types. It meets all the applicable requirements. Signals from some accident monitoring instrumentation are also transmitted from this Equipment to the non-safety HSI system for displays and alarms. Independence is maintained between all trains. Specific accident monitoring instrumentation for the US-APWR is described in the US-APWR DCD Chapter 7.

-
- (9) RG 1.100 Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants
This Equipment is designated Seismic Category I. It is designed and qualified to withstand the cumulative effects of a minimum of five (5) Operational Basis Earthquakes (OBEs) and one (1) Safe Shutdown Earthquake (SSE) without loss of safety-related function or physical integrity. The input spectrum is selected to envelope all anticipated applications. Conformance to this envelope for the US-APWR applications is discussed in the US-APWR DCD Chapter 7.
- (10) RG 1.105 Setpoints for Safety-Related Instrumentation
-endorses ISA-S67.04-1994 and ANS-10.4-1987
The uncertainties associated with the Equipment are described in the MELTAC Platform Technical Report, MUAP-07005. This includes uncertainties for signal conditioning modules, signal splitters, instrument loop power suppliers and analog to digital converters. The uncertainties associated with specific process instrumentation and the resulting safety-related setpoints are demonstrated in MUAP-09022, US-APWR Instrument Setpoint Methodology. The methodology used to combine all uncertainties to establish safety-related setpoints is described in MUAP-09022 and briefly summarized in this report.
- (11) RG 1.118 Periodic Testing of Electric Power and Protection Systems
-endorses IEEE 338-1987
See compliance to GDC 21, 10CFR50.36 and RG 1.22. All safety-related functions are tested either automatically or manually. Manual tests do not require any system reconfiguration, such as jumpers or fuse removal.
- (12) RG 1.151 Instrument Sensing Lines
-endorses ISA-S67.02
Compliance is described in Section 7.1.3.7 of the US-APWR DCD Chapter 7.
- (13) RG 1.152 Criteria for Programmable Digital Computers in Safety Systems of Nuclear Power Plants
-endorses IEEE 7-4.3.2-2003
The methods used for specifying, designing, verifying, validating and maintaining software for this Equipment complies with these requirements. The life cycle process for the digital platform software is described in the MELTAC Platform Technical Report, MUAP-07005. The life cycle process for the system application software is described in MUAP-07017.
- (14) RG 1.153 1996 Criteria for Safety Systems
-endorses IEEE Std 603-1991
Compliance with the General Design Criterion identified in this Regulatory Guide is discussed above. Compliance with IEEE 603-1991 is discussed below.
- (15) RG 1.168 Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
-endorses IEEE Std 1012-1998 and IEEE Std 1028-1997
This Equipment uses processes for verification, validation, reviews and audits that comply with this Regulatory Guide. The design processes for the digital platform are described in the MELTAC Platform Technical Report, MUAP-07005. The design processes for the digital safety-related systems are described in this MUAP-07017.

- (16) RG 1.169 Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
-endorses IEEE Std 828-1990 and IEEE Std 1042-1987
This Equipment is designed and maintained using a Configuration Management process that complies with this Regulatory Guide. The Configuration Management process for the digital platform is described in the MELTAC Platform Technical Report, MUAP-07005. The Configuration Management process for the digital safety-related systems is described in MUAP-07017.
- (17) RG 1.170 Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
-endorses IEEE Std 829-1983
The test documentation for this Equipment complies with this Regulatory Guide. The test documentation for the digital platform is described in the MELTAC Platform Technical Report, MUAP-07005. The test documentation for the digital safety-related systems is described in MUAP-07017.
- (18) RG 1.171 Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
-endorses IEEE Std 1008-1987
Unit testing for this Equipment complies with this Regulatory Guide. This unit testing for the digital platform is described in the MELTAC Platform Technical Report, MUAP-07005. Unit testing for the digital safety-related systems is described in MUAP-07017.
- (19) RG 1.172 Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
-endorses IEEE Std 830-1993
The Software Requirements Specifications for this Equipment complies with this Regulatory Guide. The Software Requirements Specifications for the digital platform are described in the MELTAC Platform Technical Report, MUAP-07005. The Software Requirements Specifications for the digital safety-related systems are described in MUAP-07017.
- (20) RG 1.173 Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
-endorses IEEE Std 1074-1995
The Software Life Cycle Process for this Equipment complies with this Regulatory Guide. The Software Life Cycle Processes for the digital platform is described in the MELTAC Platform Technical Report, MUAP-07005. The Software Life Cycle Processes for the digital safety-related systems is described in MUAP-07017.
- (21) RG 1.180 Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems
-endorses MIL-STD-461E, IEC 61000 Parts 3, 4, and 6, IEEE Std C62.41-1991, IEEE Std C62.45-1992, IEEE Std 1050-1996
This Equipment complies with the EMI/RFI requirements of this standard. Qualification testing for the digital platform is described in the MELTAC Platform Technical Report, MUAP-07005. Requirements and features of the digital safety-related systems that ensure compliance to the platform qualification envelope are described in this Report.

-
- (22) RG 1.209 Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants
-endorses IEEE323-2003
This Equipment, which consists of safety-related computer-based I&C systems, is located in a mild environment. There is no change in the environment due to plant accidents. This equipment is tested and analyzed to satisfy the mild environmental qualification requirements.
- (23) RG 1.204 Guidelines for Lightning Protection of Nuclear Power Plants
The US-APWR DCD Chapter 8 describes conformance to RG 1.204 for the plant's electrical and grounding systems (e.g., Section 8 of the FSAR). In addition, the MELTAC digital platform complies with the electrical surge requirements defined by RG 1.180. In aggregate, this conformance provides suitable lightning protection.
- (24) RG 1.206 Combined License Applications for Nuclear Power Plants
For the US-APWR the level of detail needed for the NRC staff to make a final safety determination is described in the DCD and COLA (Combined License Application). This document is intended to supplement the information provided in the DCD and COLA. This document may be referenced directly by the COLA or indirectly (via reference to the US-APWR DCD, which references this document).

3.4 NRC Branch Technical Positions

- (1) BTP 7-1 Guidance on Isolation of Low-Pressure Systems from the High-Pressure Reactor Coolant System
- (2) BTP 7-2 Guidance on Requirements of Motor-Operated Valves in the Emergency Core Cooling System Accumulator Lines
- (3) BTP 7-3 Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps out of Service
- (4) BTP 7-4 Guidance on Design Criteria for Auxiliary Feedwater Systems
- (5) BTP 7-5 Guidance on Spurious Withdrawals of Single Control Rods in Pressurized Water Reactors
- (6) BTP 7-6 Guidance on Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode
Compliance with BTP 7-1 thru 6, above, is described in the US-APWR DCD Table 7.1-2.
- (7) BTP 7-8 Guidance for Application of Regulatory Guide 1.22
All functions of the protection system are testable at power.
- (8) BTP 7-9 Guidance on Requirements for Reactor Protection System Anticipatory Trips
Reactor trip on turbine trip function is an anticipatory trip used in the protection system as described in DCD Chapter 7. For this non-safety trip the following requirements are met:
 - All non-safety equipment is isolated from the safety-related system to prevent electrical fault propagation and adverse communication interaction.
 - Safety-related functions have priority over all non-safety functions.
 - Analysis demonstrates that credible non-safety signal failures do not result in plant conditions that are outside the boundary of the safety analysis.
- (9) BTP 7-10 Guidance on Application of Regulatory Guide 1.97
The Equipment complies with this BTP for processing all instrumentation signals. However,

RG 1.97 Revision 4 has superseded Revisions 2 and 3, for which this BTP was written. Therefore, where there are conflicts, the Equipment meets the requirements of RG 1.97 Revision 4.

- (10) BTP 7-11 Guidance on Application and Qualifications of Isolation Devices
-endorses IEEE Std 472, ANSI Std C62.36, ANSI Std C62.41, ANSI Std C62.45
See compliance to RG 1.75. Isolation devices are qualified in compliance to these standards.
- (11) BTP 7-12 Guidance on Establishing and Maintaining Instrument Setpoints
The Equipment complies with this BTP. See compliance to RG 1.105. Section 6.5.4 defines the methodology used to combine all uncertainties to establish limiting safety-related system settings (LSSS) and Allowable Values defined in the plant technical specifications.
- (12) BTP 7-13 Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors
The methods used for periodically verifying the accuracy and response time of RTDs complies with this standard. The method is described in the US-APWR DCD Chapter 7.
- (13) BTP 7-14 Guidance on SW Reviews for Digital Computer Based I&C Systems
-endorses IEEE Std 730
The Equipment complies with this BTP. See compliance to RG 1.168 thru 1.173.
- (14) BTP HICB-16 Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52
This guidance was withdrawn. See compliance to RG 1.206.
- (15) BTP 7-17 Guidance on Self-Test and Surveillance Test Provisions
See compliance to GDC 21, 10CFR50.36, RG 1.22 and RG 1.118. Surveillance testing taken together with automatic self-testing provides a mechanism for detecting all failures.
- (16) BTP 7-18 Guidance on Use of Programmable Logic Controllers in Digital Computer Based I&C Systems
This Equipment is not a commercial-grade computer system; it was designed originally for nuclear safety-related applications in Japan. Since its development it has been deployed in numerous non-safety nuclear applications in Japan and will be deployed in nuclear safety-related applications in Japan in the near future. All of this operating experience in Japan is directly applicable to expected nuclear safety-related applications in the US. However, since this Equipment was not developed under a 10CFR50 Appendix B quality program, it has been re-evaluated to demonstrate that it is equivalent to a product that had been developed under a 10CFR50 Appendix B quality program and is therefore suitable for safety-related applications. This is referred to as the MELTAC Re-evaluation Program (MRP), which is described in MUAP-07005. The MRP is a non-recurring activity that applies only to the MELTAC past development design. The MRP and all future MELTAC life cycle activities, including production, and all application level life cycle activities are conducted under a 10 CFR 50 Appendix B Quality Assurance Program (QAP).
- (17) BTP 7-19 Guidance on Evaluation of Defense in Depth and Diversity in Digital Computer Based I&C Systems
The MHI safety-related digital I&C systems utilize the MELCO safety-related digital I&C

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

(18) BTP 7-21 Guidance on Digital Computer Real Time Performance

The real-time performance for this Equipment complies with this BTP. The method for determining response time performance for the digital safety-related systems (including the digital platform) is described in this Report. The response time performance for digital platform components is described in the MELTAC Platform Technical Report, MUAP-07005. Requirements for system response time for conformance with the plant design basis and the response time of actual plant systems is described in the US-APWR DCD Chapter 7 and MUAP-09021.

3.5 NRC Interim Staff Guidance

(1) DI&C-ISG-04, Digital Instrumentation and Control

This Equipment conforms to all requirements of this guidance including key requirements for:

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

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

3.6 NUREG-Series Publications (NRC Reports)

(1) NUREG-0737, Supplement 1 Clarification of TMI Action Plan Requirements

This Equipment is used for compliance with the following TMI Action Plan Requirements:

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

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

This Equipment fulfills all safety-related requirements of this NUREG for monitoring safety-related plant instrumentation and controlling safety-related plant components. Descriptions of specific plant systems are described in the US-APWR DCD Chapter 7.

(3) NUREG/CR-6303 Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems

The design of this Equipment is described in this Report. The assessment of diversity within this Equipment and between this Equipment and other I&C systems is described in the Diversity and Defense-in-Depth Topical Report, MUAP-07006. The Diversity and Defense-in-Depth Topical Report also describes the method of coping with common cause failure vulnerabilities.

- (4) NUREG/CR-6421 A Proposed Acceptance Process for Commercial-Off-the-Shelf (COTS) Software in Reactor Applications
. See compliance to BTP 7-18. The MRP described in MUAP-07005 complies with the acceptance process for Category A software in Section 4.3 of NUREG-6421.

3.7 IEEE Standards

- (1) IEEE 7-4.3.2 2003 Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations
This Equipment conforms to all requirements of this standard, as augmented by RG 1.152, including key requirements for:
 - Software quality and life cycle processes
 - Independent Verification and Validation
 - Communications independenceA detailed discussion of compliance to all aspects of IEEE7-4.3.2 is provided in Appendix B.
- (2) IEEE 323 2003 Qualifying Class 1E Equipment for Nuclear Power Generating Systems
This Equipment is qualified in compliance with this standard, as augmented by RG 1.89.
- (3) IEEE 338 1987 Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems
This Equipment conforms to this standard, as augmented by RG 1.22.
- (4) IEEE 344 1987 Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations
This Equipment conforms to this standard as augmented by RG 1.100.
- (5) IEEE 379 2000 Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems
This Equipment conforms to this standard as augmented by RG 1.53.
- (6) IEEE 383 1974 Type Test of Class 1E Electric Cables, Field Splices, and Connections for Nuclear Power Generating Stations
The cable and electrical connections used within this Equipment and between this Equipment conform to this standard, including requirements for flame retarding qualification requirements. Cables for interfaces to/from this equipment to other I&C systems and components are discussed in the US-APWR DCD Chapter 7.
- (7) IEEE 384 1992 Criteria for Independence of Class 1E Equipment and Circuits
This Equipment conforms to this standard as augmented by RG 1.75. All safety-related functions are implemented within multiple trains with physical separation and electrical independence between redundant safety trains and between safety and non-safety trains. Electrical independence is accomplished primarily through the use of fiber optic

technology. Independence of electrical circuits is accomplished with isolation modules and physical separation or barriers, such as conduits.

- (8) IEEE 420 1982 Design and Qualification of Class 1E Control Board, Panels and Racks. Standard enclosures for this Equipment conform to this standard. These enclosures are described in this Report.
- (9) IEEE 472 IEEE Guide for Surge Withstand Capability (SWC) Tests
As stated in BTP 7-11, this standard is currently intended for electrical protective relaying applications; it is not intended for digital systems. Therefore this Equipment complies with the surge withstand requirements of ANSI C62.41 and ANSI C62.45.
- (10) IEEE 494 1974 Method for identification of Documents Related to 1E Equipment.
The documentation for this Equipment conforms to this standard by having the term "Nuclear Safety Related" applied on the face of each document and drawing that is provided to the licensee. Generic documents and drawings used only for internal use by MHI do not contain this designation.
- (11) IEEE 497 2002 Accident Monitoring Instrumentation for Nuclear Power Generating Stations
See compliance for RG 1.97.
- (12) IEEE 603 1991 Safety Systems for Nuclear Power Generating Stations
1998 version is currently not endorsed by NRC
This Equipment conforms to this standard, as augmented by RG 1.153, including key requirements for:
 - Single failures
 - Completion of Protective Action
 - Quality
 - Qualification
 - Independence
 - Testability
 - Monitoring and Information
 - Bypasses

A detailed discussion of compliance to all aspects of IEEE603 is provided in Appendix A.
- (13) IEEE 730 1989 Software Quality Assurance Plans
- (14) IEEE 828 1990 IEEE Standard for Software Configuration Management Plans
- (15) IEEE 829 1983 Software Test Documentation
- (16) IEEE 830 1993 IEEE Recommended Practice for Software Requirements Specifications
- (17) IEEE 1008 1987 IEEE Standard for Software Unit Testing
- (18) IEEE 1012 1998 IEEE Standard for Software Verification and Validation Plans (2004 not yet endorsed by NRC)

-
- (19) IEEE 1016 1987 IEEE Recommended Practice for Software Design Descriptions
- (20) IEEE 1028 1997 IEEE Standard for Software Reviews and Audits
- (21) IEEE 1042 1987 IEEE Guide To Software Configuration Management
- (22) IEEE 1074 1995 IEEE Std for Developing Software Life Cycle Processes
1997 version not yet endorsed by NRC
The software design process and documentation for this Equipment conforms to the requirements of IEEE 730 thru 1074, above.

3.8 Other Industry Standards

- (1) ANS-10.4 1987 Guidelines for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry
The computer programs used to develop setpoints for this Equipment conform to this standard, as endorsed by RG 1.105.
- (2) ANSI C62.41 IEEE Recommended Practice on Surge Voltages in Low-Voltage AC Power Circuits
This Equipment complies with the sections of this standard endorsed by RG 1.180.
- (3) ANSI C62.45 IEEE Guide on Surge Testing for Equipment Connected to Low-Voltage AC Power Circuits
This Equipment complies with the sections of this standard endorsed by RG 1.180.
- (4) IEC 61000 Electromagnetic compatibility (EMC)
This Equipment complies with the following sections of this standard:
- IEC 61000-4-2: Testing and measurement techniques - Electrostatic discharge immunity tests. Basic EMC publication
 - IEC 61000-4-4: Testing and measurement techniques - Electrical fast transient/burst immunity test. Basic EMC publication
 - IEC 61000-4-5: Testing and measurement techniques - Surge immunity test
 - IEC 61000-4-12: Testing and measurement techniques - Oscillatory waves immunity test.
- (5) ISA-S67.04 1994 Setpoints for Nuclear Safety Related Instrumentation Used in Nuclear Power Plants
See compliance to RG 1.105. The methodology used to develop setpoints for this Equipment conforms to this standard, as endorsed by RG 1.105.
- (6) MIL-STD-461E Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment
This Equipment complies with this standard as referenced in RG 1.180. This standard replaces MIL-STD-461D and MIL-STD-462D.

4.0 SYSTEM DESCRIPTION

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

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

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

4.1 Overall I&C System Architecture

The MHI Overall I&C System is fully digital. It has been developed and applied in a step-by-step approach in Japanese PWR plants.

General specifications of the Overall I&C System are summarized below:

(1) Main control board

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

(2) Safety I&C

- Fully digital
- Consists of Mitsubishi Electric Corporation (MELCO) MELTAC platform
- Four train redundant Reactor Protection System
- Four train redundant ESF actuation system
- Four train redundant Safety Logic System for component control
- Four train redundant Safety-Related HSI System

(3) Non-safety I&C

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

(4) Data communication

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

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

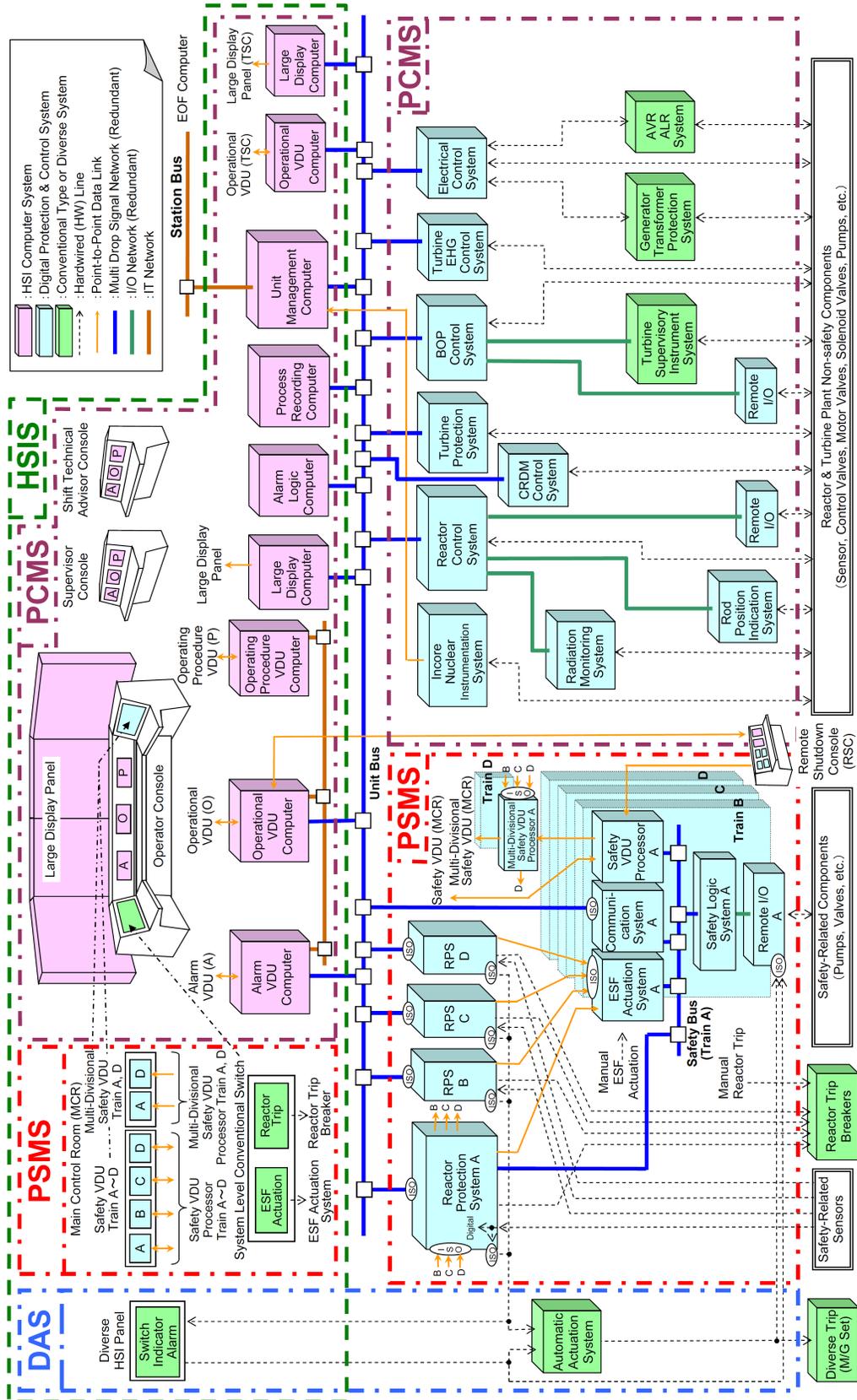


Figure 4.1-1 The Overall Architecture of the I&C System

DAS : Diverse Actuation System PSMS : Protection and Safety Monitoring System PCMS : Plant Control and Monitoring System HSI/S : Human System Interface System

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

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

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

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

a. **Human System Interface (HSI) System**

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

Figure 4.1-2 Deleted

Figure 4.1-3 Deleted

(1) Operator Console

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

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

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

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

(2) Large Display Panel

The Large Display Panel includes sufficient Spatially Dedicated Continuously Visible (SDCV) indications and alarms, so that the total status of the plant can be easily accessed without requesting VDU screens on the Operator Console. Important information for normal

operation and important information for emergency or accident conditions are displayed on the Large Display Panel. Easy and reliable comprehension for all operating crew members is achieved from the information on this panel by continuously displaying high level plant conditions.

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

(3) Supervisor Console

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

(4) Shift Technical Advisor Console

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

(5) Diverse HSI Panel

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

(6) Process Recording Computer (PRC)

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

(7) Alarm Logic Processor

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

(8) Unit Management Computer (UMC)

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

(9) Operational VDU Processor

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

(10) Alarm VDU Processor

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

(11) Operating Procedure VDU Processor

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

(12) Large Display Processor

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

(13) Safety VDU Processors

The safety VDU consists of the safety VDU panel and the safety VDU Processor. The safety VDU Processors manage the displays on the safety VDU panels located on the Operator Console and the Remote Shutdown Console. They also receive operator commands such as screen navigation and software control from the safety VDU panels. There are two types of the safety VDUs as described in Figure4.1-1.

(a) Safety VDU

The safety VDU can control and monitor all safety-related functions of each train.

(b) Multidivisional Safety VDU

The multidivisional safety VDU can monitor critical safety functions for the safe shutdown of all four trains.

There is one or two safety VDU Processor for each safety train, each located in separate fire area.

(14) Remote Shutdown Console (RSC)

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

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

(15) Technical Support Center (TSC) Computers

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

(16) Emergency Operations Facility (EOF) Computer

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

(17) Data Management Console (DMC)

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

(18) MELTAC Engineering Tool

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

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

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

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

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

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

b. Protection and Safety Monitoring System (PSMS)

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

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

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

(1) Reactor Protection System (RPS)

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

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

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

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

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

(2) ESF Actuation System (ESFAS)

The ESF actuation system has up to four redundant trains, with each train located in a separate I&C equipment room. The number of trains corresponds with the number of ESF system trains in the plant.

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

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

(3) Safety Logic System (SLS)

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

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

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

This is a microprocessor based system that achieves high reliability through redundancy within each train and microprocessor self-diagnosis, including data communications. The system also includes features to allow periodic testing of functions that are not

automatically tested by the self-diagnosis, such as final actuation of safety-related components. Manual periodic tests can be conducted with the plant on-line and without jeopardy of spurious component actuation due to single failures during testing.

(4) Safety-Related HSI System

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

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

(5) Reactor Trip Breakers

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

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

c. Plant Control and Monitoring System (PCMS)

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

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

(1) Reactor Control System

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

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

(2) Radiation Monitoring System

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

(3) Rod Position Indication System

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

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

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

(5) In-Core Neutron Instrumentation System

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

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

(6) Turbine Protection System

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

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

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

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

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

(8) Balance of Plant Control System

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

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

(9) Turbine Supervisory Instrument System

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

(10) Electrical Control System

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

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

(11) Generator Transformer Protection System

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

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

The AVR/ALR System provides regulation of generator voltage.

d. Diverse Actuation System

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

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

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

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

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

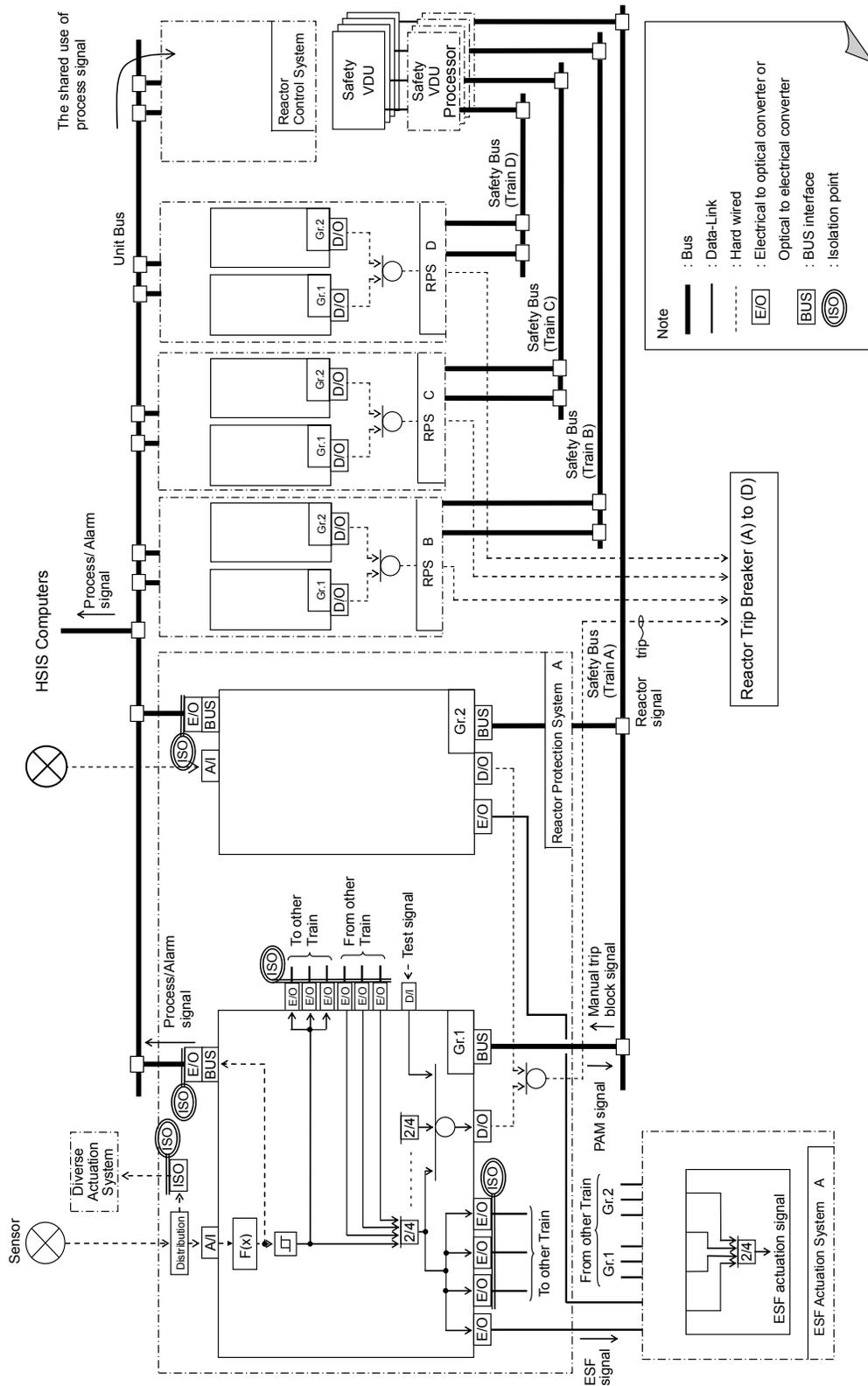


Figure 4.1-4 Configurations of the Reactor Protection System

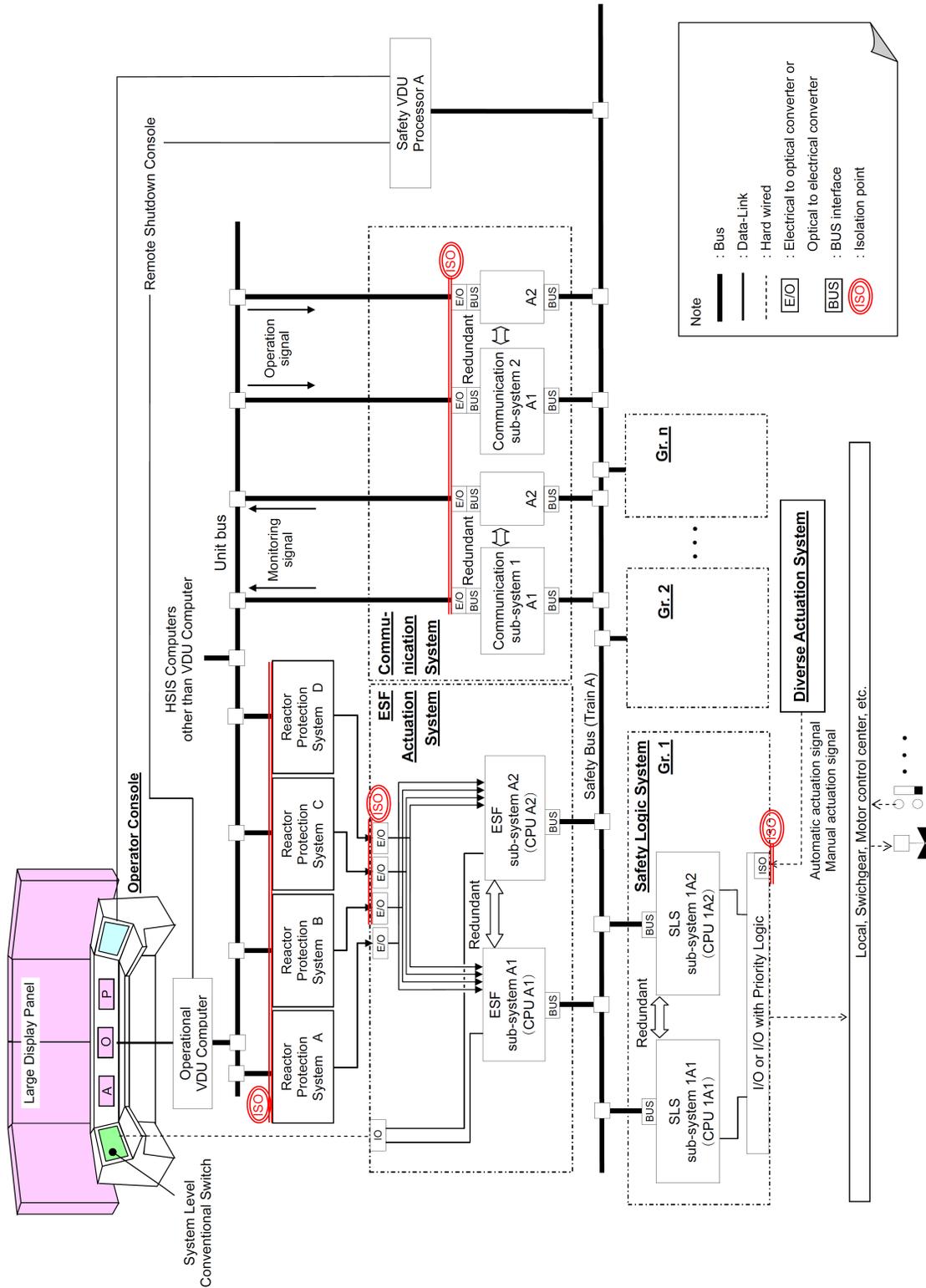


Figure 4.1-5 Configurations of the ESFAS, SLS, and Safety-Related HSI

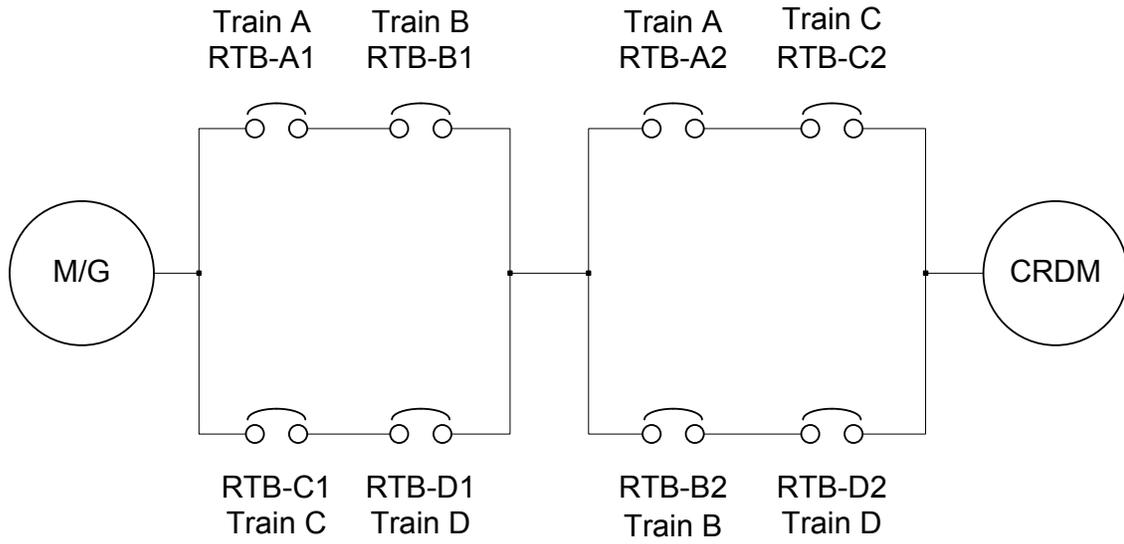


Figure 4.1-6 Configurations of the Reactor Trip Breakers

4.2 Detailed Description of Safety-Related Systems

4.2.1 Reactor Protection System (RPS)

a. Reactor Trip Function in RPS

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

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

- Sensors and manual inputs
- Reactor Trip Breakers

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

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

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

The PRA safety goals, the Single Failure Criterion, and GDC24 are met with only three trains in service. Therefore, these requirements are met even when one RPS train and its corresponding RTA train are bypassed. Therefore, bypass of one complete RPS/RTA train is permitted for a limited time period consistent with the reliability of the remaining three trains. Interlocks between RPS trains prevent bypassing two RPS trains or two RTA trains.

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

b. Engineered Safety Features Actuation Function in RPS

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

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

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

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

- Sensors
- Engineered Safety Features Actuation System

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

4.2.2 ESF Actuation System (ESFAS)

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

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

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

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

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

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

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

The ESF actuation system also provides automatic load sequencing for the Class 1E GTGs to accommodate the Loss of Offsite Power (LOOP) accident. Each ESFAS train monitors the loss of power condition for its respective train. Upon detecting a loss of power, the ESFAS starts the Class 1E GTG for its train and disconnects the loads for its train from the electrical

bus. Once the Class 1E GTG is capable of accepting loads, the ESFAS sequences the loads for its train back onto the electrical bus in an order appropriate for the current train level ESF actuation signal(s). The ESFAS sequencing logic accommodates ESF actuation signals occurring prior to or during a loading sequence. The ESFAS load sequencing function is independent for each train.

4.2.3 Safety Logic System

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

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

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

To enhance reliability, each SLS controller consists of a duplex architecture using dual redundant CPUs operating in a redundant parallel configuration. In the Digital Platform TR, MUAP-07005, this is referred to as a redundant parallel controller configuration. Each controller of the duplex architecture receives ESF actuation signals and Load Sequencing signals from the corresponding duplex controller of the ESFAS. The SLS also includes I/O modules mounted in I/O chassis. These I/O chassis can be located within the same cabinet as the controllers or remotely in separate cabinets that are distributed throughout the plant to reduce the length of cable from the process component or instrument to the I/O chassis. Signals from each SLS controller in the duplex architecture are combined in the output modules using 1-out-of-2 voting logic for control of plant components to the desired safety state.

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

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

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

The primary functions performed by the SLS are described below:

a. Control of ESF Components

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

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

The SLS also controls ESF components based on manual component level controls from operational VDUs and safety VDUs.

b. Control of Safe Shutdown Components

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

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

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

c. Control of Interlocks Important to Safety

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

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

4.2.4 Safety-Related HSI System

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

a. Control of Reactor Trip Switchgear

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

b. Control of ESF Components

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

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

c. Post Accident Monitoring (PAM)

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

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

d. Safe Shutdown from Outside the Main Control Room

The Remote Shutdown Console, located outside the Main Control Room fire zone, is installed so that safe shutdown can be achieved in the case that the operators can not stay within the Main Control Room.

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

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

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

Transfer Switches near the MCR is administratively controlled through closed areas with key access.

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

4.2.5 Plant Control and Monitoring System

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

a. Instrumentation Shared with the Protection and Safety Monitoring System

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

The SSA ensures the PCMS does not take erroneous control actions based on a single instrument channel failure or single RPS train failure. As such, a single failure will not cause the PCMS to take erroneous control actions that challenge the PSMS, while the PSMS is in a degraded operability state due to the failed instrument channel or failed RPS train. This signal selection algorithm within the PCMS is one design feature that contributes to allowing the RPS to have one instrument channel inoperable or bypassed at all times while still complying with GDC24 and IEEE 603-1991.

b. Information Systems Important to Safety

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

(1) Post Accident Monitoring (PAM)

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

(2) Bypassed or Inoperable Status Indication (BISI)

If a safety-related function of the PSMS is bypassed or inoperable at the train level, this is continuously indicated on the Large Display Panel. Other bypassed or inoperable conditions that do not result in inoperability of safety-related functions at the train level are indicated on operational VDUs but not on the Large Display Panel. For example, if one redundant subsystem fails within an ESFAS or RPS controller the safety-related function of the controller is still maintained for that train, so this inoperable condition is only indicated on operational VDUs. Alternately, if an instrument input to a train of the RPS is bypassed or inoperable, this is continuously indicated on the Large Display Panel because that RPS train can no longer perform its safety-related function for that parameter.

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

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

(3) Plant Alarms

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

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

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

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

The main features of the alarm system are as follows;

- Adequate display to acknowledge and recognize alarm information

-
- Application of alarm prioritization to avoid alarm avalanche
 - Request functions from alarm display to relevant operation display and alarm response procedures.

These functions help operators to identify and diagnose transients.

(4) Safety Parameter Display System (SPDS)

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

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

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

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

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

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

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

- **Electrical independence**
Fiber optic interfaces between the PSMS and PCMS prevent propagation of electrical faults between trains. The electrical independence features are shown in Fig. 4.2-2.
- **Data processing independence**
The PSMS employs communication processors for the PCMS that are separate from the processors that perform safety-related logic functions. The safety-related processors and communication processors communicate via 2-port memory. This ensures there is no potential for communications functions, such as handshaking, to disrupt deterministic safety-related function processing. The data processing independence features are shown in Figure. 4.2-2.
- **No ability to transfer unpredicted data**
There is no file transfer capability in the PSMS. Only predefined communication data sets are used between the PSMS and PCMS. Therefore any unknown data is rejected by the PSMS.
- **No ability to alter safety-related software**
The software in the PSMS cannot be changed through the non-safety communication network, which is called the unit bus, or from any communication interface that is connected or can be connected to the PSMS. The PSMS software is changeable only when the CPU module that contains the memory devices is removed from the MELTAC controller. The PSMS basic software is changeable only by removing and replacing the memory device that contains the software. The PSMS application software is changeable

only by removing the controller’s CPU module from its chassis and placing it in a dedicated re-programming chassis.

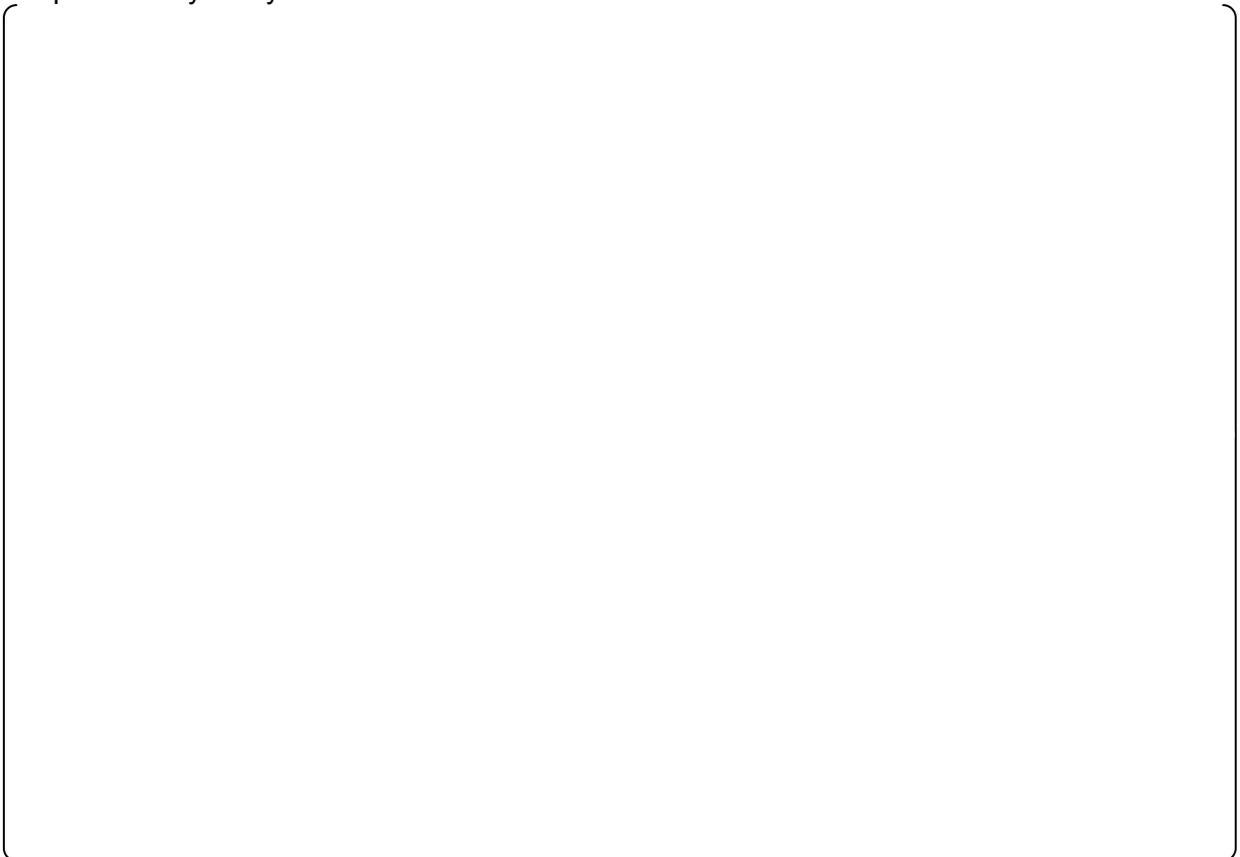
- Acceptable safety function performance

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



- Failures of non-safety systems are bounded by the safety analysis

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



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

4.2.6 Diverse Actuation System

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

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

Within the DAS manual initiation is provided for all critical functions at the train level (e.g., reactivity level, core heat removal, reactor coolant inventory and containment isolation). Automatic actuation is also provided for functions where time for manual operator action is inadequate.

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

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

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

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

4.2.7 Digital Data Communication

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

- The Unit bus provides bi-directional communication between safety-related and non-safety systems for only non-safety functions. The safety-related system and non-safety system are functionally isolated by dedicated communication processors in each safety-related system controller, and priority logic within the safety train that ensure safety-related functions have priority over all non-safety functions. Unit bus uses optical fiber to achieve electrical independence of each train. Physical separation between safety-related and non-safety system is accomplished by locating the safety and non-safety trains in different areas. The Unit bus uses the Control Network digital communication technology described in the Platform Technical Report, MUAP-07005 Section 4.3.2.
- Communications between different trains are one way data link communication between RPS trains, from RPS to ESFAS and safety VDU trains. Functional separation is achieved by communication controllers that are separate from functional processors and voting logic that processes the data from the different trains. Each data link uses optical fiber to achieve electrical independence of each train. Physical separation between safety trains is achieved by locating in different areas. These interfaces are the data link digital data communication technology described in the MELTAC Platform Technical Report, MUAP-07005 Section 4.3.3.
- Bi-directional communications between controllers in one(1) safety train are performed by the Safety Bus. The Safety Bus provides deterministic cyclical data communication. Functional independence is provided by separate communication processors within each controller. Fiber optic cable is provided to enhance EMI susceptibility. The Safety Bus uses the Control Network digital communication technology described in the MELTAC Platform Technical Report, MUAP-07005 Section 4.3.2.
- Bidirectional communication between controllers and their respective I/O modules is provided by the I/O Bus described in the MELTAC Platform Technical Report, MUAP-07005 Section 4.1.
- Bidirectional communication between the PSMS controllers and the MELTAC engineering tool is provided by the Maintenance Network described in the MELTAC Platform Technical Report, MUAP-07005 Section 4.3.4. The PSMS controllers are normally disconnected from the Maintenance Network. Temporary connections are made for equipment trouble shooting and periodic surveillance. Temporary connections are managed by administrative controls and plant technical specifications.

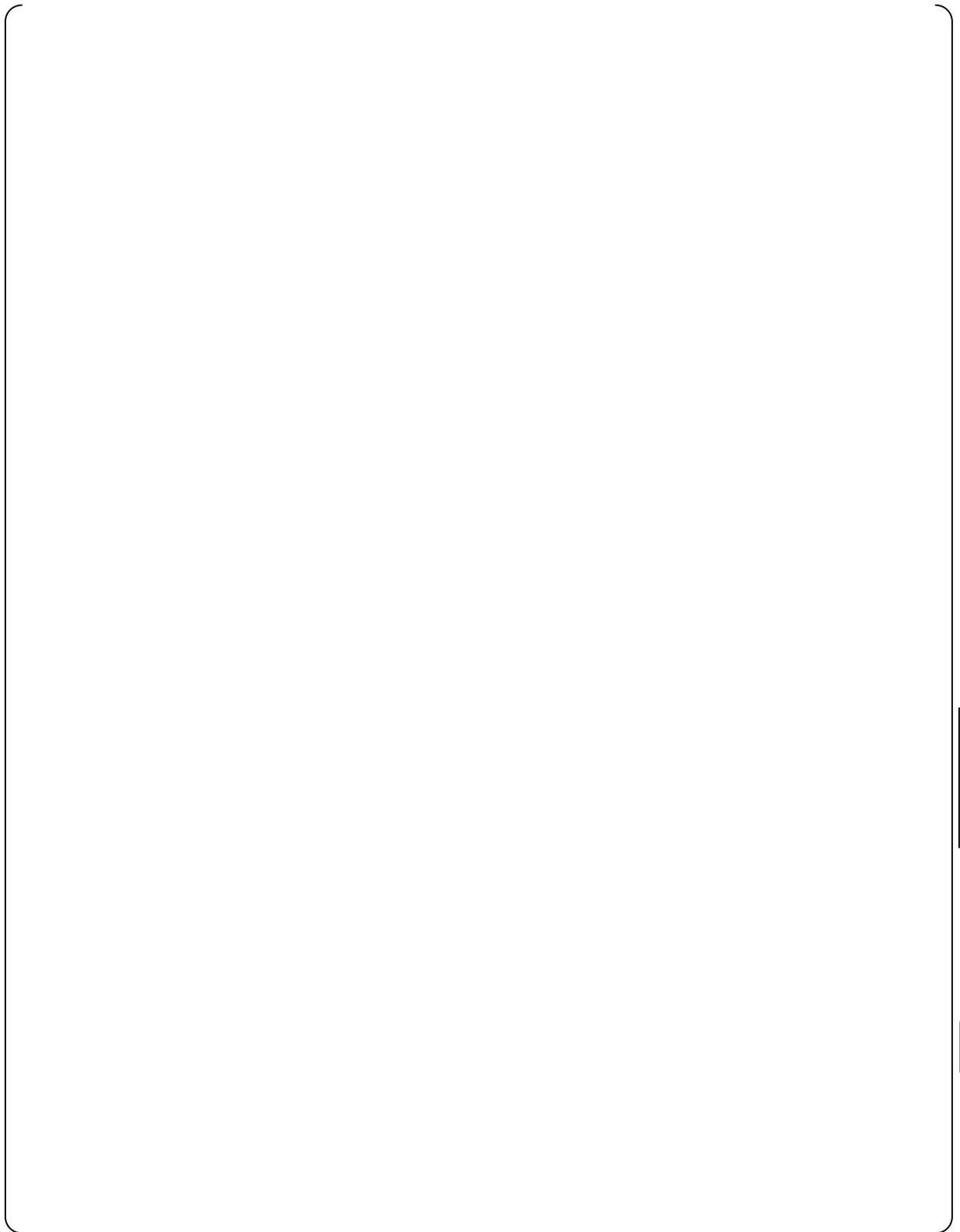


Figure 4.2-1 Configuration of RSC/MCR Transfer System

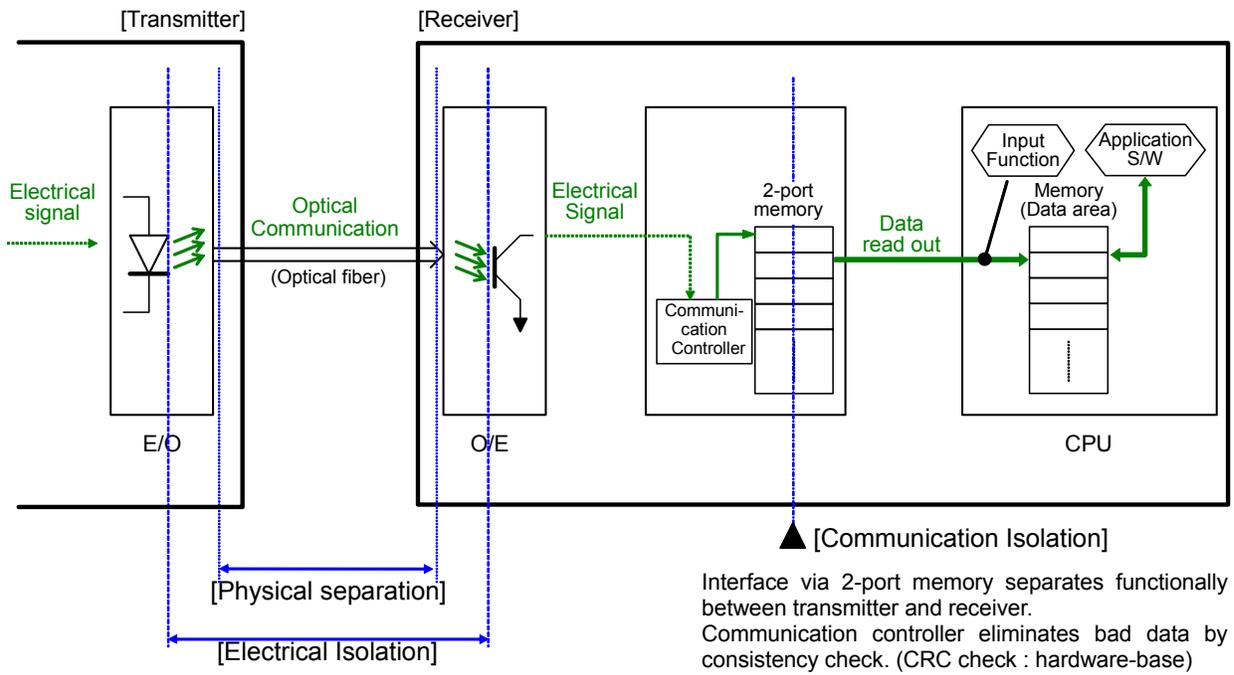


Figure 4.2-2 Electrical Independence Features between PCMS and PSMS



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



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



Figure 4.2-5 Overlap Testability for DAS

4.3 PSMS Self-diagnostic Features

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

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

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

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

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

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

The continuous automatic CHANNEL CHECK, which is also a technical specification surveillance, is conducted by the PCMS, based on signals that are processed by the

RPS controllers. This test confirms the operability of the RPS controllers through automated testing that is diverse from the MELTAC self-diagnostic features. If a failure is detected that should have been detected by the MELTAC self-diagnostic features, a failure of the MELTAC self-diagnostic features is also identified. The operability of the automatic CHANNEL CHECK is confirmed through periodic manual CHANNEL CALIBRATION.

4.4 PSMS Manual Testing and Calibration Features

The integrity of safety-related function of the PSMS is continuously checked by their self-diagnostic features. The continuous PSMS self-diagnostic features allow elimination of most manual surveillances required for Technical Specification compliance.

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

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

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

4.4.1 Manual Testing

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

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

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

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

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

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

[]

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

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

[]

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

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

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

confirmed by reading analog or binary values on any VDU driven by the signal processed by the PSMS.

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

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

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

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

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

- Final Actuation Outputs (TRIP ACTUATION DEVICE OPERATIONAL TEST)

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

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

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

- Memory Integrity Check (CHANNEL OPERATIONAL TEST – Digital and ACTUATION LOGIC TEST – Digital)

This function is used during periodic surveillance tests to confirm that the software in the controller is the same as the off-line version, and therefore has not changed. This test confirms the functional integrity of PSMS software applications without the need to perform functional logic tests. The Memory Integrity Check is conducted with the train for the controller to be tested in a bypass condition.

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

This test ensures the integrity of the software credited to execute system safety-related functions, including correct setpoints, constants and logic functions. This test also ensures the integrity of the software credited to execute self-diagnostic functions. The Memory Integrity Check overlaps with platform self-diagnostic tests, automated cross-channel tests and manual tests described above and as shown in Figure 4.4-4.

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

4.4.2 Manual Calibration (CHANNEL CALIBRATION)

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

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

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

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

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

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

4.4.3 Response Time Test

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

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

4.5 PSMS On-line Maintenance

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

Failures detected by platform self-diagnosis are automatically diagnosed to the replaceable module level. Alarms are provided on operational VDUs and failed module identification is provided on the engineering tool. Alarms are provided for failures detected by self-diagnosis in all processor configurations, single or redundant. Failed processor modules in a Redundant Parallel Controller configuration and failed I/O modules may cause actuation or failure of components in a single train, depending on the application logic.

I/O modules can be replaced while the PSMS controllers are powered. Processor modules (e.g., CPU and digital communication modules), require power to be removed from the chassis, prior to module replacement. For failed processor modules in controllers configured for parallel or standby redundancy, the controllers will recover to their normal redundant configuration with no plant impact beyond the initial failure, as discussed above. For failed processor modules in single controller configurations, the plant level effects of the failure must be considered, including recognition that the controller must be powered down for module replacement.

Replacement of I/O modules must consider that some modules have more than one input or output. Therefore, if the initial failure was limited to a single channel on the module, removal of the failed module may impact more channels and therefore more plant interfaces. Failures and module replacement are considered in the assignment of plant process I/O to I/O modules during the system design, to minimize plant impact during module failure or maintenance.

The plant level of effects of controller failures (including I/O modules) are described in the US-APWR DCD Chapter 7 and MUAP-09020.

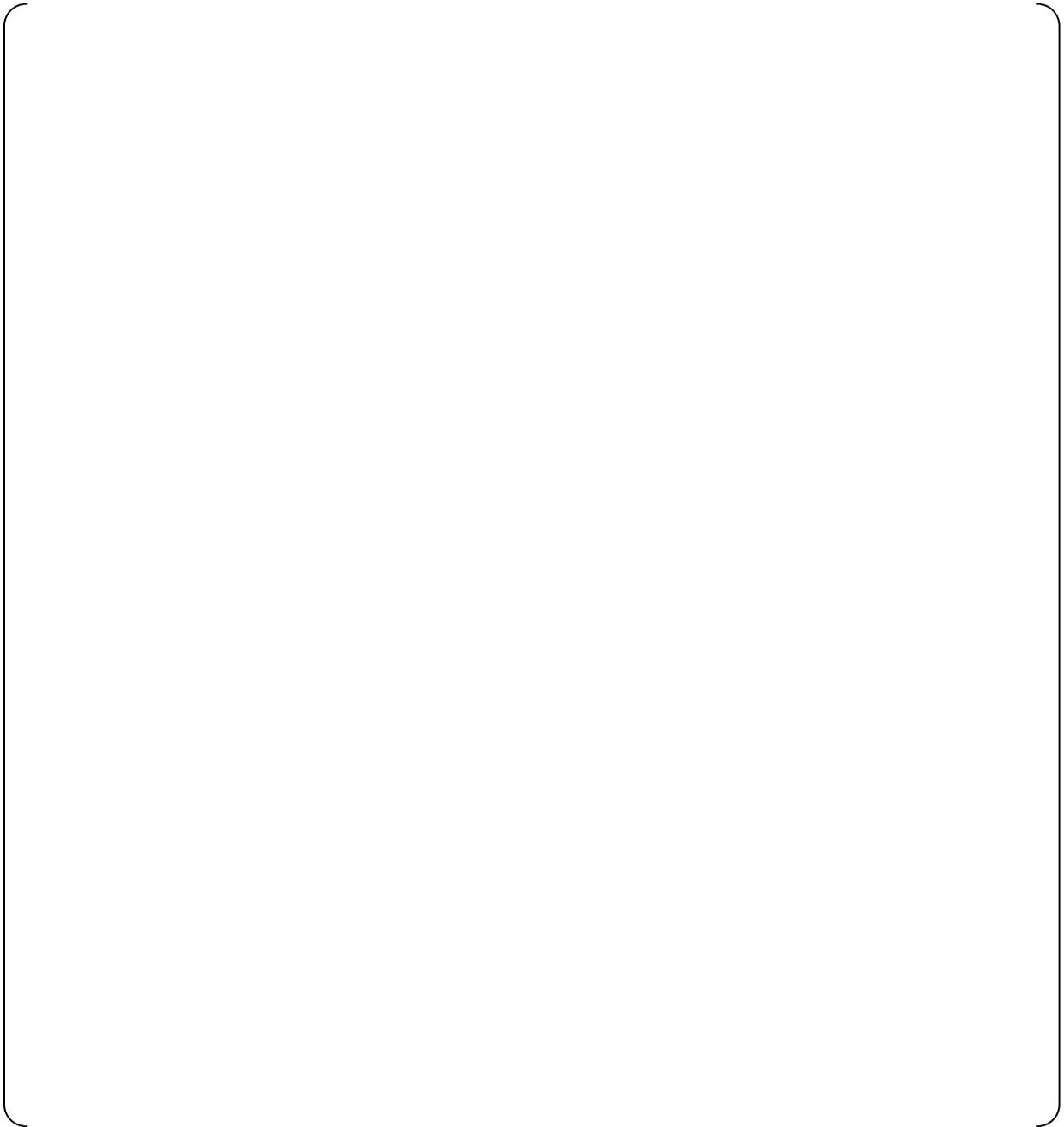


Figure 4.4-1 Overlap Testability for Reactor Trip

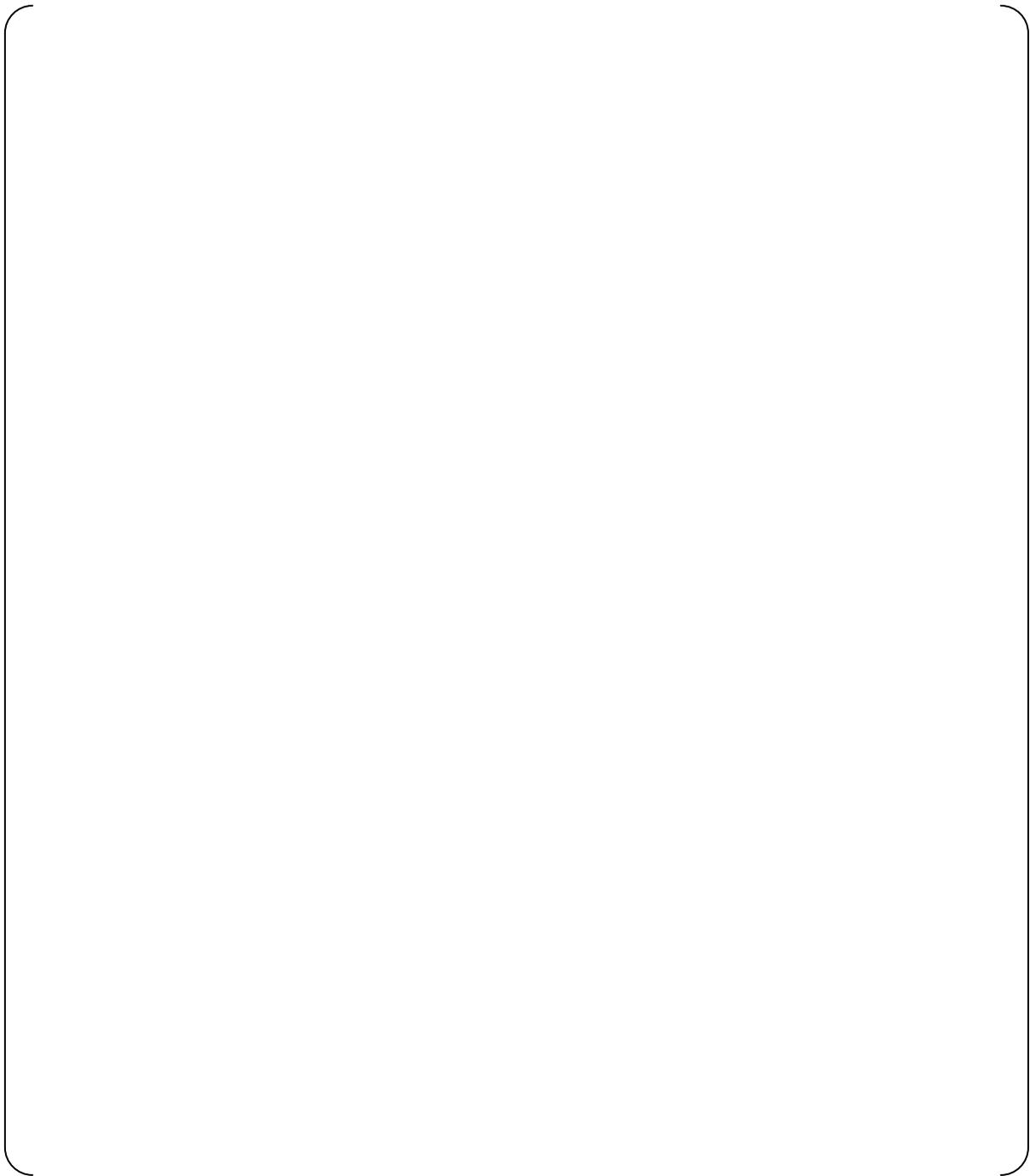


Figure 4.4-2 Overlap Testability for ESF Actuation



Figure 4.4-3 Overlap Testability for Safety VDU



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

5.0 DESIGN BASIS

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

5.1 Key Technical Issue

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

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

5.1.1 Multi-Channel Operator Station

There is two-way communication between non-safety operational VDUs and the PCMS and between the non-safety operational VDUs and all trains of the PSMS. To ensure independence between redundant safety trains and between the non-safety and safety-related systems the following independence measures described in Section 4.2.5, above, are applied.

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

5.1.2 HSI to Accommodate Reduced Operator Staffing

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

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

5.1.3 Operation under Degraded Conditions

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

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

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

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

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

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

5.1.4 Integrated RPS & ESFAS with Functional Diversity

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

Instead of separating RPS and ESFAS, functional diversity is provided within the integrated RPS/ ESFAS through two separate subsystems in each train. For each DBA each subsystem processes diverse sensor inputs that can each detect the DBA and initiate protective actions.

PRAs done for the MHI digital I&C design are expected to show significant benefit for this functional diversity; this is confirmed on a plant specific basis.

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

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

5.1.6 This section intentionally left blank

5.1.7 Output Module for PSMS and DAS

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

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

Figure 5.1-1 shows the signal interface between output module and PSMS and DAS.

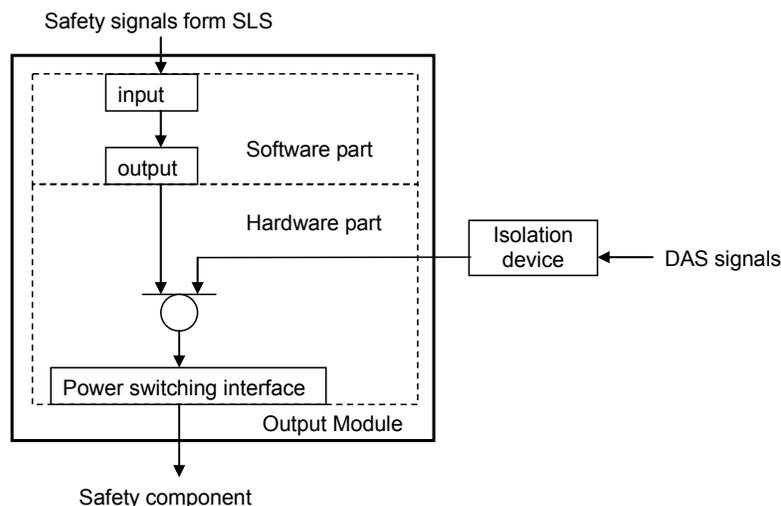


Figure 5.1-1 Signal Interface of Output Module

5.1.8 Control System Failure Mode

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

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

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



5.1.9 Credit for Self-Diagnosis for Technical Specification Surveillance

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

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

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

5.1.10 Unrestricted Bypass of One Safety-Related Instrument Channel

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

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

5.1.11 Minimum Inventory of HSI

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

5.1.12 Computer Based Procedures

Computer based procedure allows operators to access relevant display formats which are hyper linked from the procedure and shown on the operational VDU. Operator accesses and operates the required control switch quickly from the linked display formats on the operational VDU, if necessary.

5.1.13 Priority Logic

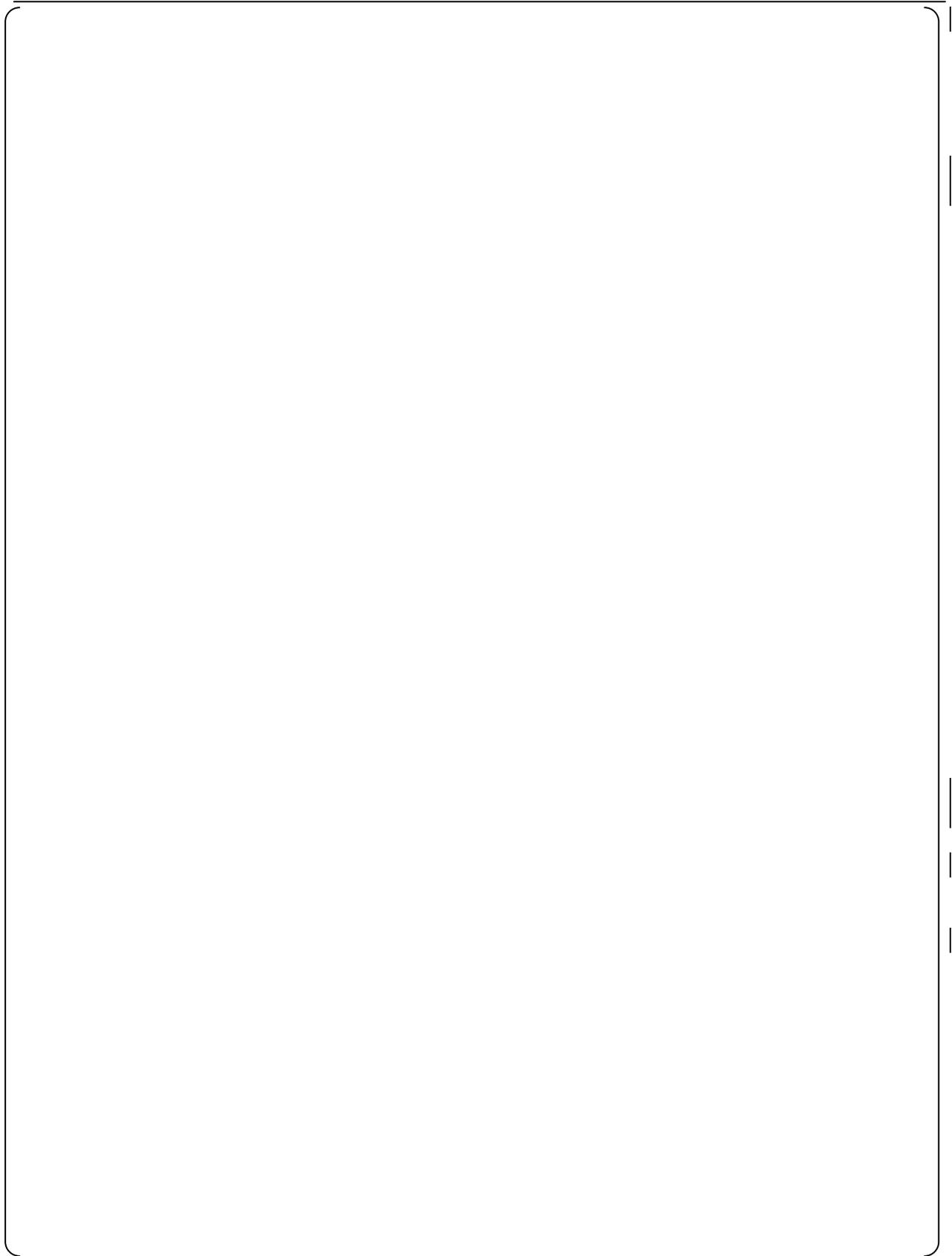






Figure 5.1-3 Priority Between Commands from Safety VDU and Operational VDU

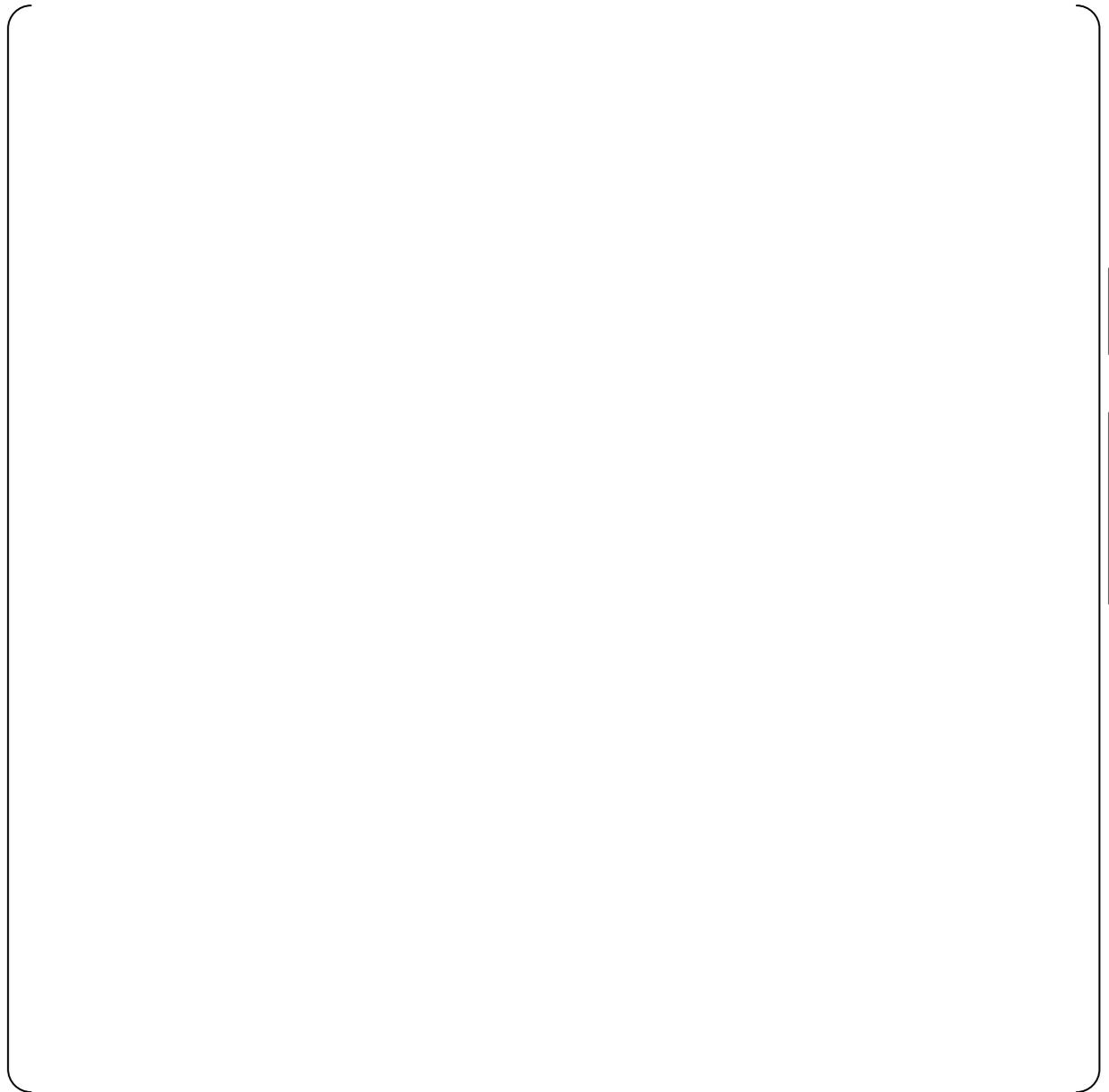


Figure 5.1-4 Priority for Manual and Automatic Signals of Safety and Non-Safety Demand



Figure 5.1-5 State-based Priority in PIF



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

5.2 This section intentionally left blank

Figure 5.2-1 Deleted

Figure 5.2-2 Deleted

Figure 5.2-3 Deleted

Figure 5.2-4 Deleted

6.0 DESIGN PROCESS

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

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

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

6.1 This section intentionally left blank

Figure 6.1-1 Deleted

6.2 This section intentionally left blank

Figure 6.2-1 Deleted

6.3 This section intentionally left blank

6.4 This section intentionally left blank

6.5 Analysis Method

6.5.1 FMEA Method

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

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

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

This section describes the FMEA method.

Safety-related functions are designed with multiple trains. Each train is independent from the other trains and from the non-safety trains. Independence ensures that credible single failures cannot propagate between trains within the safety-related system or between safety-related and non-safety trains. Therefore credible single failures can not prevent proper protective action at the system level. The credible single failures considered in the safety-related and non-safety trains are described in the FMEA for each system. The FMEA follows the guidance of IEEE379, which is endorsed by RG1.53.

Component

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

Failure Mode

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

Method of Failure Detection

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

Local Failure Effect

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

Effect on Protective Function or Plant

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

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

Table 6.5-1 Deleted

The FMEA for safety-related I&C system is provided in the US-APWR DCD Chapter 7.

6.5.2 Reliability Analysis Method

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

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

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

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

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

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

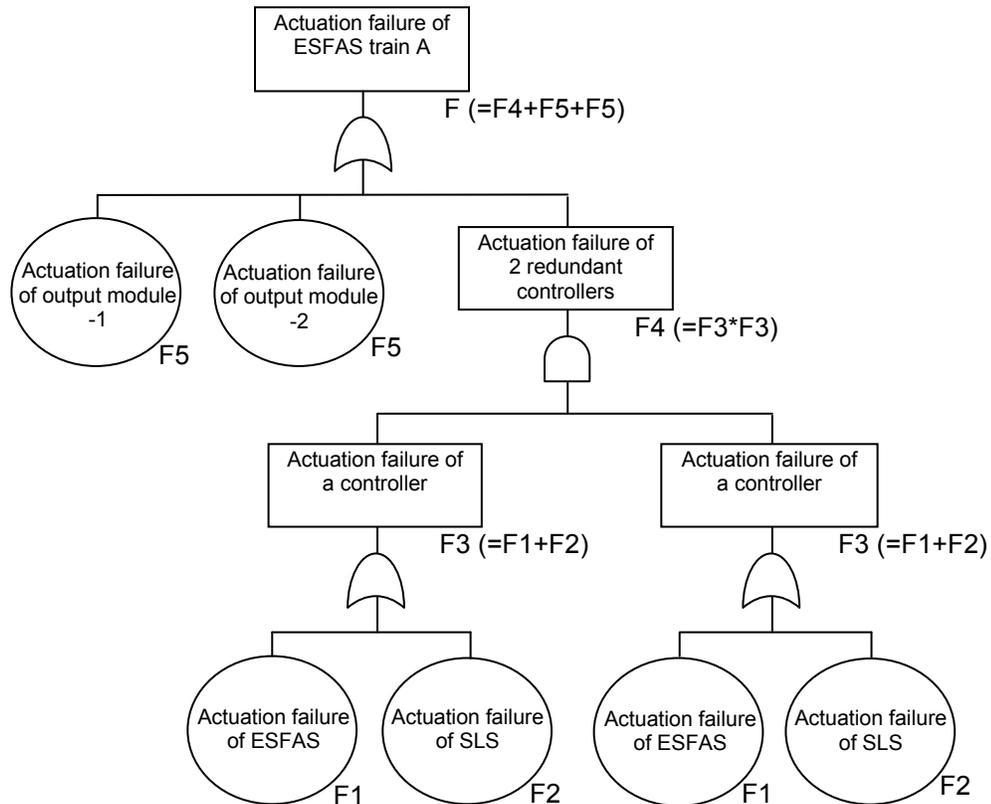


Figure 6.5-1 Typical FTA for Failure of ESFAS Actuation

6.5.3 Response Time Analysis Method

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

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



Figure 6.5-2 Breakdown Response Time for Reactor Trip

6.5.4 Accuracy Analysis Method

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

- Sensor
- Analog input module

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

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

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

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

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

where

A = resultant uncertainty for one component

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

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

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



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

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



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

6.5.5 Heat Load Analysis Method

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

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

6.5.6 Seismic Analysis Method

The seismic analysis method for the PSMS is based on Regulatory Guide 1.100, which endorses IEEE 344-1987.

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

type tests bound the in plant conditions to which the MELTAC components will actually be exposed.

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

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

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

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

(2) Qualification of non-MELTAC enclosures

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

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

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

Seismic analysis is described in the US-APWR DCD Chapter 3.

6.5.7 EMI Analysis Method

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

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

EMI qualification analysis also confirms that the characteristics of the EMI environment for the type test bounds the EMI environment of the plant.

6.5.8 Fire Protection Analysis

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

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

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

Figure 6.5-4 shows this fire protection configuration of DAS.

Fire protection and fire protection program are described in DCD Chapter 9.



Figure 6.5-4 Configuration of Fire Protection for Diverse Actuation System

7.0 This section intentionally left blank

8.0 REFERENCES

In this section, references referred in this report except for applicable codes and standards and regulatory guidance in section 3 are enumerated.

1. Safety System Digital Platform -MELTAC-, MUAP-07005-P Rev.7 (Proprietary) and MUAP-07005-NP Rev.7 (Non-Proprietary), April 2011
2. Defense-in-Depth and Diversity, MUAP-07006-P-A Rev.2 (Proprietary) and MUAP-07006-NP-A Rev.2 (Non-Proprietary), September 2009
3. HSI System Description and HFE Process, MUAP-07007-P Rev.3 (Proprietary) and MUAP-07007-NP Rev.3 (Non-Proprietary), October 2009
4. Quality Assurance Program (QAP) Description for Design Certification of US-APWR, PQD-HD-19005 Rev.4, April 2011
5. Methodologies for the Determination of Setpoints for Nuclear Safety-Related Instrumentation, ISA-RP67.04.02-2000
6. Deleted
7. System 80+ Design Certification Document (DCD).
8. Design Control Document for the US-APWR, Rev.3, March 2011.
9. US-APWR Instrument Set point Methodology, MUAP-09022-P Rev.2 (Proprietary) and MUAP-09022-NP Rev.2 (Non-Proprietary), May 2011.
10. US-APWR Software Program Manual, MUAP-07017-P Rev.4 (Proprietary) and MUAP-07017-NP Rev.4 (Non-Proprietary), May 2011.
11. Defense in Depth and Diversity Coping Analysis, MUAP-07014-P Rev.3 (Proprietary) and MUAP-07014-NP Rev.3 (Non-Proprietary), May 2011.
12. Response Time of Safety I&C System, MUAP-09021-P Rev.3 (Proprietary) and MUAP-09021-NP Rev.3 (Non-Proprietary), May 2011.
13. US-APWR Functional Assignment Analysis for Safety Logic System, MUAP-09020-P Rev.2 (Proprietary) and MUAP-09020-NP Rev.2 (Non-Proprietary), May 2011.

Appendix A Conformance to IEEE 603-1991

This appendix describes conformance of the PSMS to the requirements of IEEE 603. The section numbers follow the sections in IEEE603. All sections pertain to the 1991 version of this standard unless specifically noted.

A.1. Scope

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

A.2. Definitions

The definitions are applicable to the PSMS.

A.3. References

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

A.4. Safety System Designation

A.4.1 Design Basis Events

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

A.4.2 Safety Functions and Corresponding Protective Actions

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

A.4.3 Permissive Conditions for Each Operating Bypass Capability

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

report. Initiation of manual blocks may be by either the operational VDUs or safety VDUs. In either case the PSMS provides the necessary safety permissive and automatic removal.

A.4.4 Variables Required to be Monitored for Protective Action

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

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

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

Table A.4.4-1 Deleted.

Table A.4.4-2 Deleted.

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

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

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

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

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

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

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

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

A.4.6 Spatially Dependent Variables

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

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

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

A.4.7 Range of Conditions for Safety System Performance

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

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

A.4.8 Functional Degradation of Safety Functions

The PSMS is located in plant areas that provide protection from accident related hazards such as missiles, pipe breaks and flooding. The redundant trains of the PSMS are isolated from

each other and isolated from non-safety systems. Isolation ensures functional and communications independence and independence for fires and electrical faults. The design life of PSMS components is maximized when operated continuously in a controlled ventilation environment. The PSMS will operate reliably for extended periods with loss of ventilation.

A.4.9 Reliability

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

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

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

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

A.4.11 Equipment Protective Provisions

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

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

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

- Reactor trip circuits are designed to fail in the tripped state.
- Engineered safety features actuated components are designed to fail into a de-energized state or fail as-is. The de-energized state applies to failures that result in complete loss of component control. The as-is state is selected for failures that impair control but do not result in complete loss of component control. These states has been demonstrated to be

acceptable if conditions such as disconnection, loss of power source, or postulated adverse environments are experienced.

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

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

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

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

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

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

A.4.12 Other Special Design Basis

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

A.5. Safety System Criteria

A.5.1 Single Failure Criterion

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

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

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

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

causing a reactor trip. The 2-out-of-4 actuation logic for reactor trip requires trip signals from 2-out-of-4 trains.

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

A.5.2 Completion of Protective Action

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

A.5.3 Quality

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

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

A.5.4 Equipment Qualification

Section 5.2 describes the environmental and seismic qualification of the PSMS.

A.5.5 System Integrity

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

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

A.5.6 Independence

A.5.6.1 Between Redundant Portions of a Safety System

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

demonstrate the adequacy of the isolation method. Separate power feeds energize each redundant protection train.

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

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

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

ANSI/ISA S67.02-1980 endorsed by RG1.151 describes that a single process pipe tap to connect process signals to redundant instruments shall not be used. However, the latest version of the ANSI, ANSI/ISA S67.02.01-1999 describes that if a single process connection cannot be avoided, justification shall be provided to permit its use. The common instrument tap on reactor coolant flow measurement of the US-APWR is justified as follows.

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

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

A.5.6.3 Between Safety Systems and Other Systems

A.5.6.3.1 Interconnected Equipment

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

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

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

A.5.6.3.2 Equipment in Proximity

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

A.5.6.3.3 The Effects of a Single Random Failure

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

A.5.6.4 Detailed Independence Criteria

IEEE 384-1981, Regulatory Guide 1.75

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

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

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

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

A.5.7 Capability for Test and Calibration

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

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

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



A.5.8 Information Displays

A.5.8.1 Displays for Manually Controlled Actions

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

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

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

The operational VDUs provide the following HSI functions:

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

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

A.5.8.2 System Status Indication

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

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

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

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

A.5.8.3 Indication of Bypasses

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

SDCV indications for each train are automatically provided for inoperable or bypassed conditions that adversely affect the function of the train. SDCV indications can also be manually actuated for conditions that are not automatically monitored. For example, for

unmonitored components, such as hand-wheel valves, the component's status is manually entered in the PCMS data base. The component status is displayed on operational VDU displays. In addition, if that status adversely affects the operability of the train, the train level SDCV indication is automatically activated. The train level SDCV indication can also be manually actuated directly for other unexpected conditions that may have no manual data entry capability in the PCMS data base.

A.5.8.4 Location of Displays

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

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

A.5.9 Control of Access

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

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

A.5.10 Repair

The PSMS facilitates the recognition, location, replacement, repair and adjustment of malfunctioning components or modules. The built-in diagnostics, along with the operational VDU alarms and MELTAC engineering tool provide a mechanism for rapidly identifying and locating malfunctioning assemblies.

Channel bypass permits replacement of malfunctioning sensors or PSMS components, without jeopardizing plant availability, and while still meeting the single failure criterion.

A.5.11 Identification

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

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

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

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

A.5.12 Auxiliary Features

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

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

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

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

A.5.13 Multi-Unit Stations

There is no sharing of PSMS components between units.

A.5.14 Human Factors

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

A.5.15 Reliability

The PSMS reliability is used in the Probabilistic Risk Assessment (PRA). That analysis is described in the US-APWR DCD Chapter 19, and MUAP-07030. The component level reliability which is the basis for the PRA analysis is described in the MELTAC Platform

Technical Report, MUAP-07005. The system level reliability method which is the basis for the PRA analysis is described in Section 6.5.2.

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

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

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

For each design basis accident addressed in the plant safety analysis, two diverse parameters are used to detect the event and initiate protective actions. These diverse parameters are processed in two separate Controller Groups within each train of the RPS. The Table 7.2-5 described in DCD Chapter7 shows examples of this diversity.

Table A.5.16-1 Deleted.

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

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

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

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

A.6.1 Automatic Control

The PSMS is designed to automatically initiate reactor trip and actuate the engineered safety features necessary to mitigate the effects of anticipated operational occurrences and design basis accidents. The PSMS automatically initiates appropriate safety functions whenever a variable measured by the PSMS reaches a trip or actuation setpoint. The earliest operator

actions are not required for certain time period defined in the safety analysis. Any exception to this is described in the US-APWR DCD Subsections 7.5.1.5.

A.6.2 Manual Control

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

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

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

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

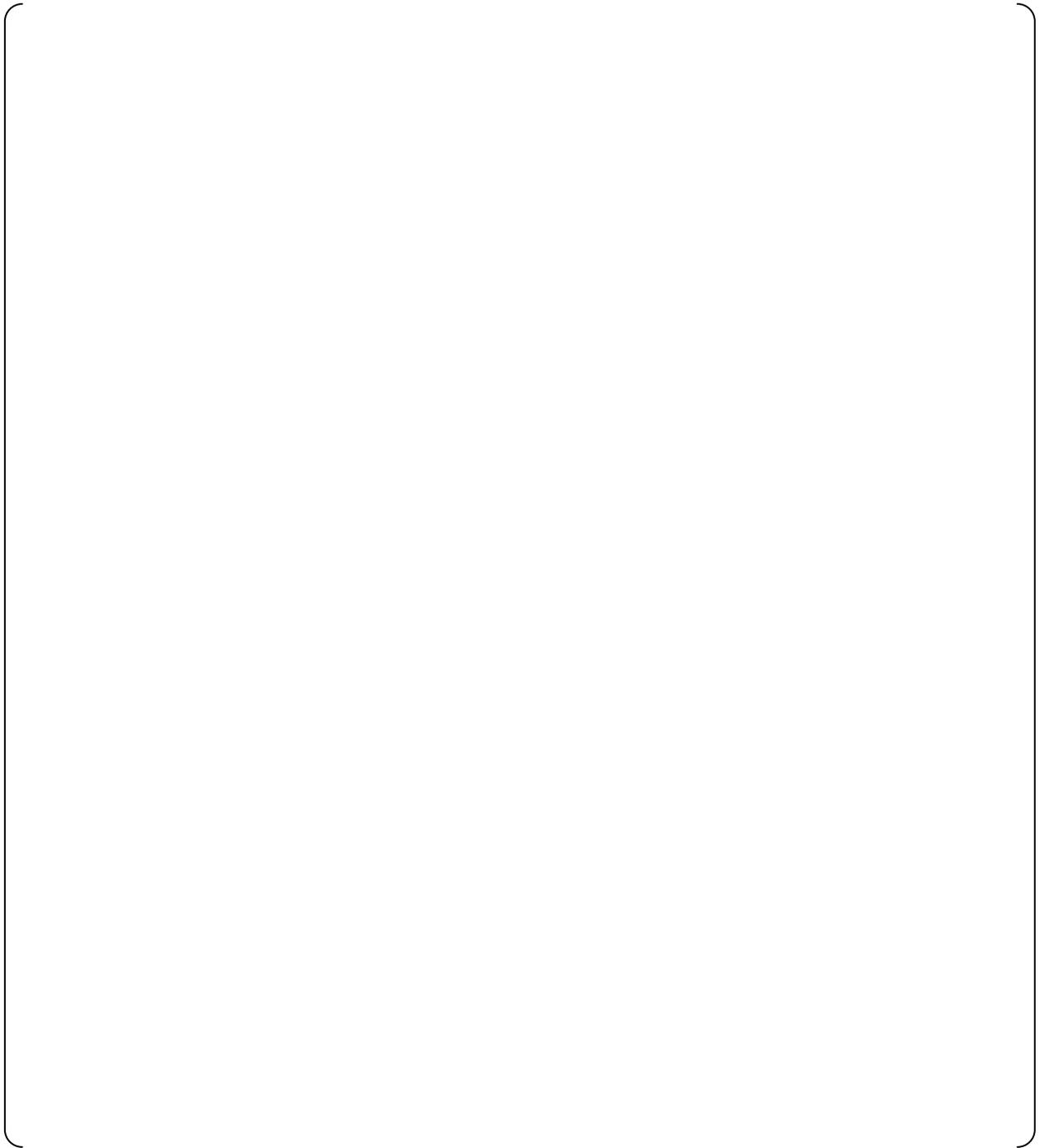


Figure A.6.2-1 Manual Control

A.6.3 Interaction between the Sense and Command features and other Systems

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

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

A.6.4 Derivation of System Inputs

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

A.6.5 Capability for Testing and Calibration

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

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

A.6.6 Operating Bypasses

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

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

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

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

A.6.7 Maintenance Bypass

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

a. Input Channel Bypass

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

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

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

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

b. Train Level RPS Bypass

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

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

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

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

A.6.8 Setpoint

A.6.8.1 Setpoint Uncertainties

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

- Safety limit
- Allowable value
- Nominal trip setpoint

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

The allowable value is the Technical Specification value and is obtained by subtracting the unmeasurable channel uncertainties from the safety limit. The method used for combining all process measurement effects to determine the unmeasurable process measurement uncertainty is described in Section 6.5.4.

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

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

A.6.8.2 Multiple Setpoints

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

Other trip setpoints are manually enabled or disabled based on administrative controls. To manually disable a setpoint a permissive interlock must be reached. This interlock can be

based on the same process parameter or an alternate process parameter. If the interlock permissive condition is no longer satisfied the manually disabled setpoint is reenabled.

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

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

A.7. Executive Features - Functional and Design Requirements

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

A.7.1 Automatic Control

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

A.7.2 Manual Control

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

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

Plant components with Execute Feature Manual Controls are described in the US-APWR DCD Section 7.1 and Table 7.1-1.

A.7.3 Completion of Protective Action

[]

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

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

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

A.7.4 Operating Bypass

There are no Operating Bypasses in the Execute Features.

A.7.5 Maintenance Bypass

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

A.8. Power Source Requirements

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

Appendix B Conformance to IEEE 7-4.3.2 -2003

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

B.1. Scope

This conformance section addresses the computer portions of the PSMS.

B.2. References

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

B.3. Definitions and abbreviations

The definitions are applicable to the PSMS.

B.4. Safety System Design Basis

No requirements beyond IEEE Std 603-1998 are necessary.

B.5. Safety System Criteria

B.5.1 Single Failure Criterion

No requirements beyond IEEE Std 603-1998 are necessary.

B.5.2 Completion of Protective Action

No requirements beyond IEEE Std 603-1998 are necessary.

B.5.3 Quality

B.5.3.1 Software Development

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

B.5.3.1.1 Software quality metrics

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

B.5.3.2 Software tools

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

B.5.3.3 Verification and Validation

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

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

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

B.5.3.5 Software configuration management

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

B.5.3.6 Software project risk management

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

B.5.4 Equipment Qualification

B.5.4.1 Computer system testing

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

B.5.4.2 Qualification of existing commercial computers

There are no commercial computers in the PSMS.

B.5.5 System Integrity

B.5.5.1 Design for computer integrity

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

B.5.5.2 Design for test and calibration

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

B.5.5.3 Fault detection and self-diagnostics

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

B.5.6 Independence

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

a. Electrical independence

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

b. Data processing independence

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

c. No ability to transfer unpredicted data

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

d. No ability to alter safety software

The software in the PSMS cannot be changed through the communication interface between PSMS trains or the communication interface for the PCMS or the communication interface for the MELTAC engineering tools. The PSMS application software is changeable only through a hardwired connection to the software memory device, which can only be made when the CPU module is removed from the MELTAC controller. The PSMS basic software can only be changed by physically replacing the software memory device, which can only be done when the CPU module is removed from the MELTAC controller.

e. Deleted

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

f. Acceptable safety function performance

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

g. Failures of non-safety systems are bounded by the safety analysis

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

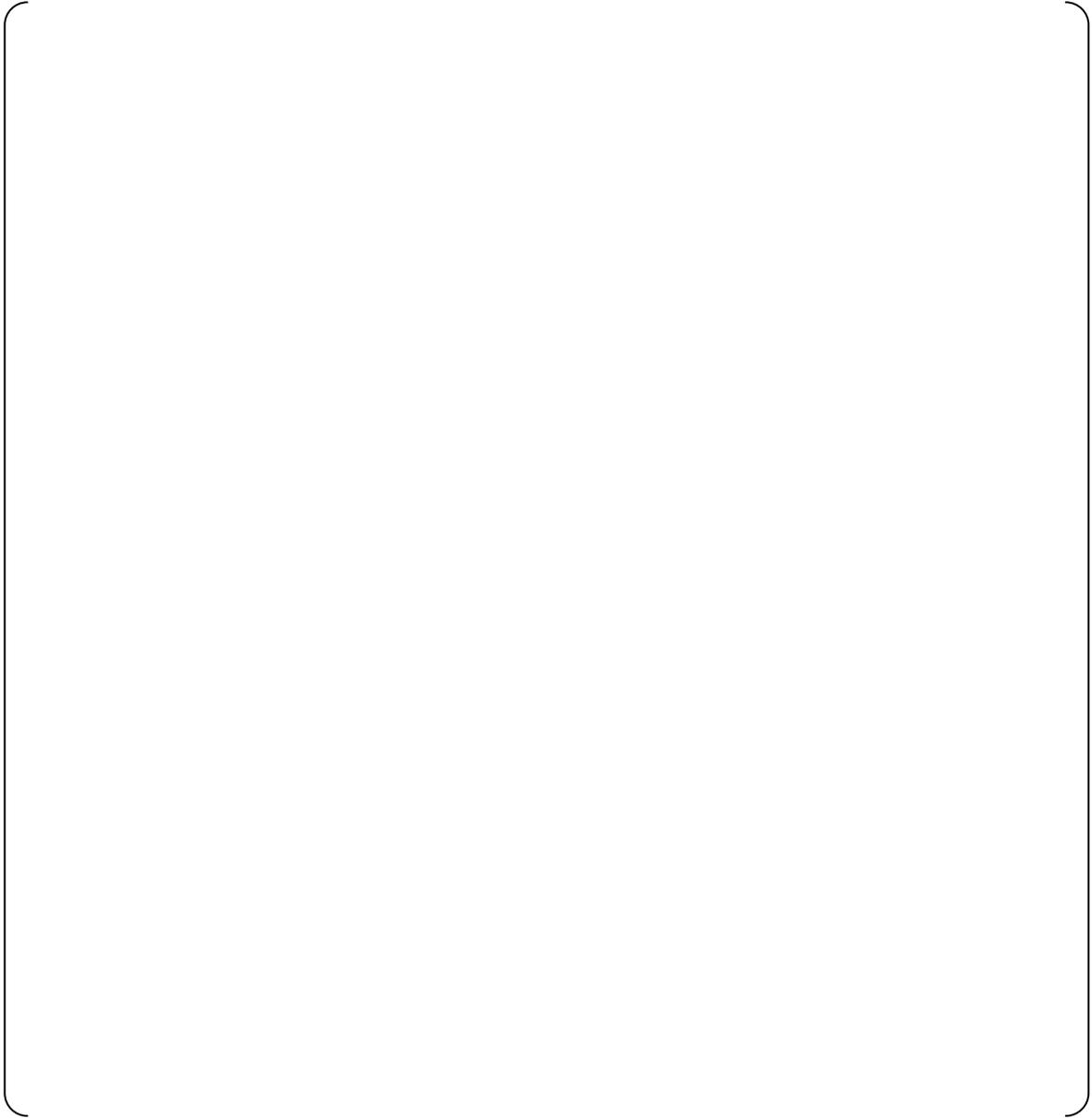


Figure B.5.6-1 Software Isolation (Non-Safety VDU / Safety-related System)

B.5.7 Capability for Test and Calibration

No requirements beyond IEEE Std 603-1998 are necessary.

B.5.8 Information Displays

No requirements beyond IEEE Std 603-1998 are necessary.

B.5.9 Control of Access

No requirements beyond IEEE Std 603-1998 are necessary.

B.5.10 Repair

No requirements beyond IEEE Std 603-1998 are necessary.

B.5.11 Identification

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

B.5.12 Auxiliary Features

No requirements beyond IEEE Std 603-1998 are necessary.

B.5.13 Multi-Unit Stations

No requirements beyond IEEE Std 603-1998 are necessary.

B.5.14 Human Factors

No requirements beyond IEEE Std 603-1998 are necessary.

B.5.15 Reliability

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

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

No requirements beyond IEEE Std 603-1998 are necessary.

B.7. Executive Features - Functional and Design Requirements

No requirements beyond IEEE Std 603-1998 are necessary.

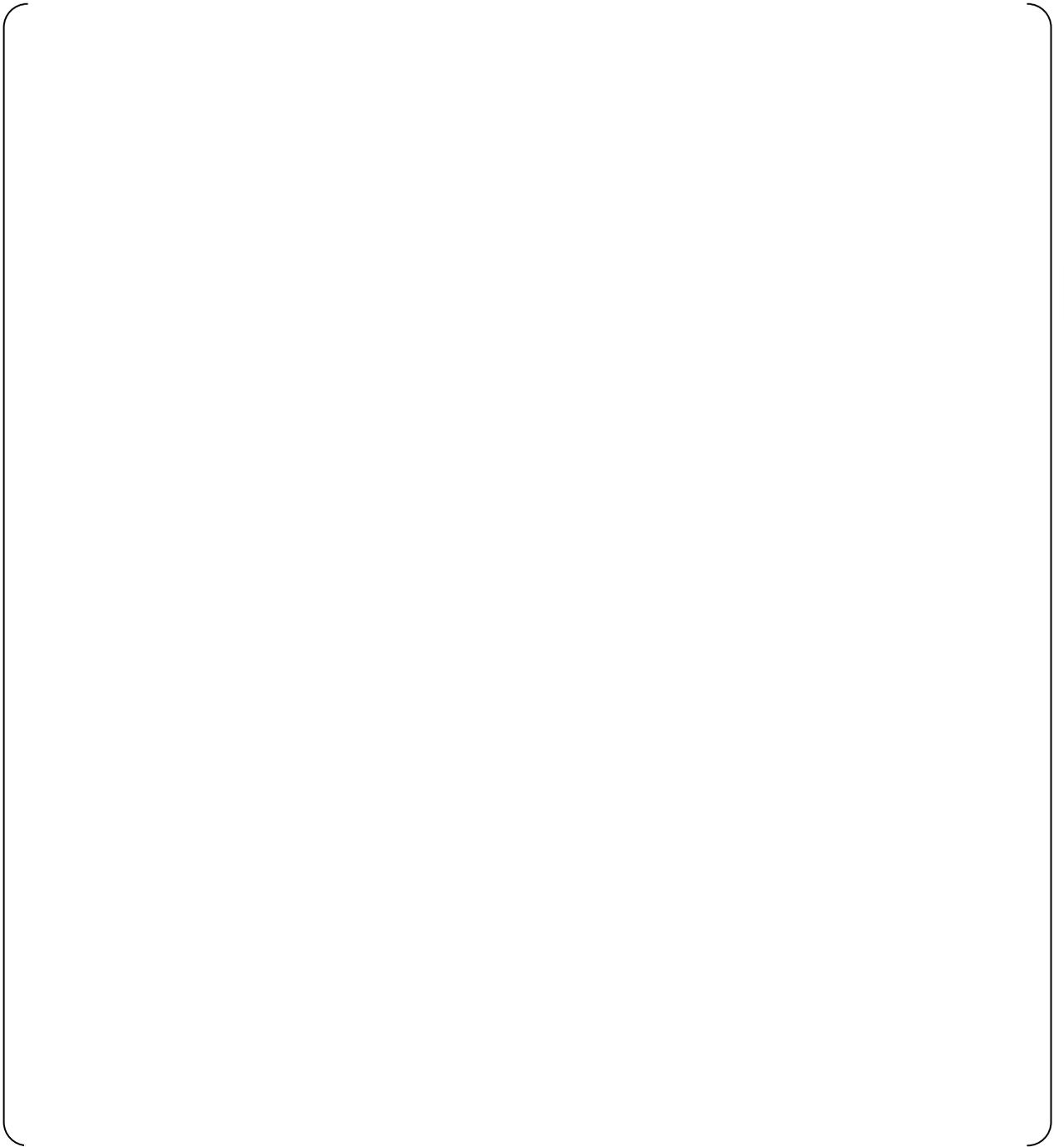
B.8. Power Source Requirements

No requirements beyond IEEE Std 603-1998 are necessary.

Appendix C Prevention of Multiple Spurious Commands and Probability Assessment

C.1. Prevention of Multiple Spurious Commands





C.2. Probability Assessment

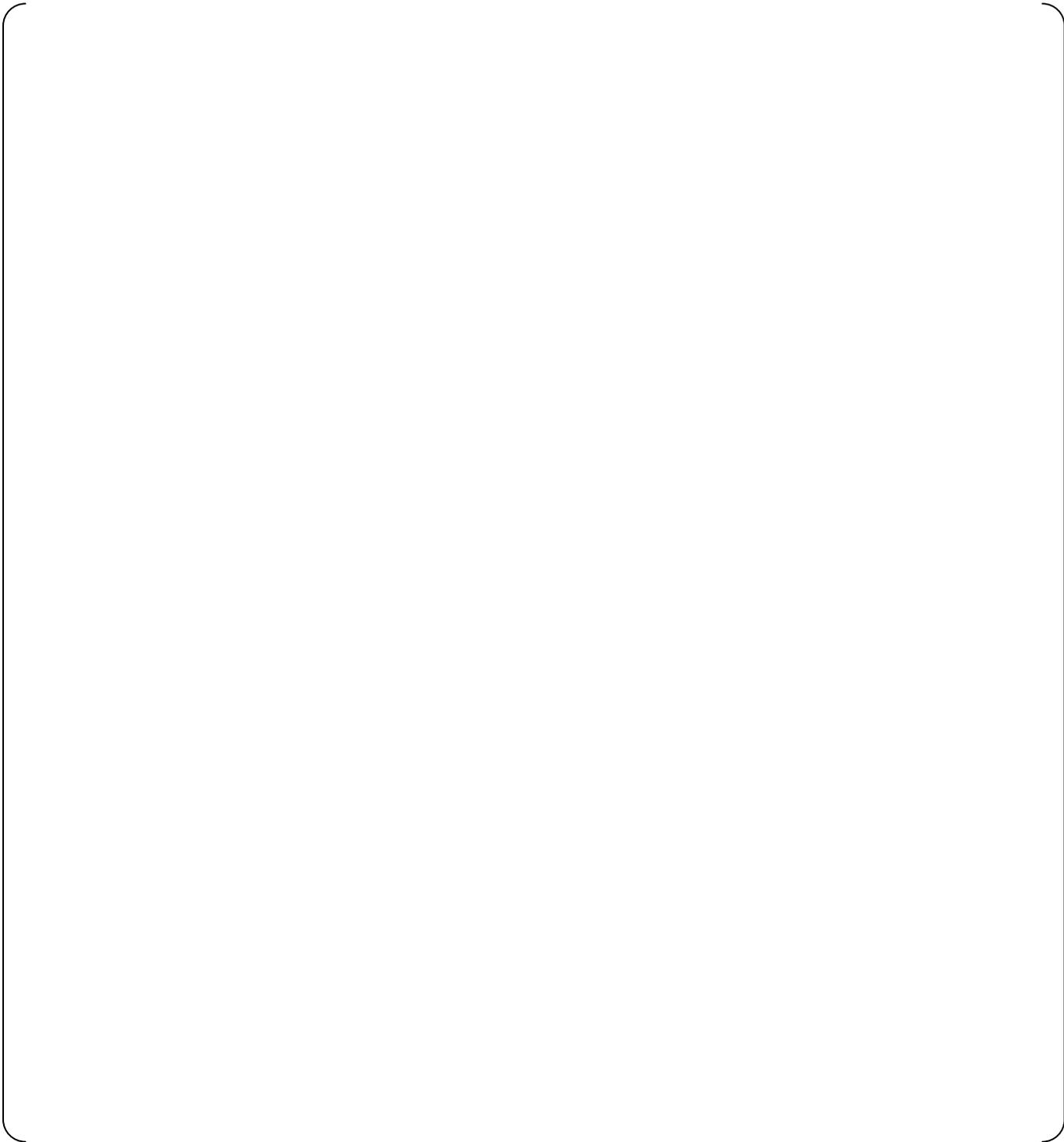
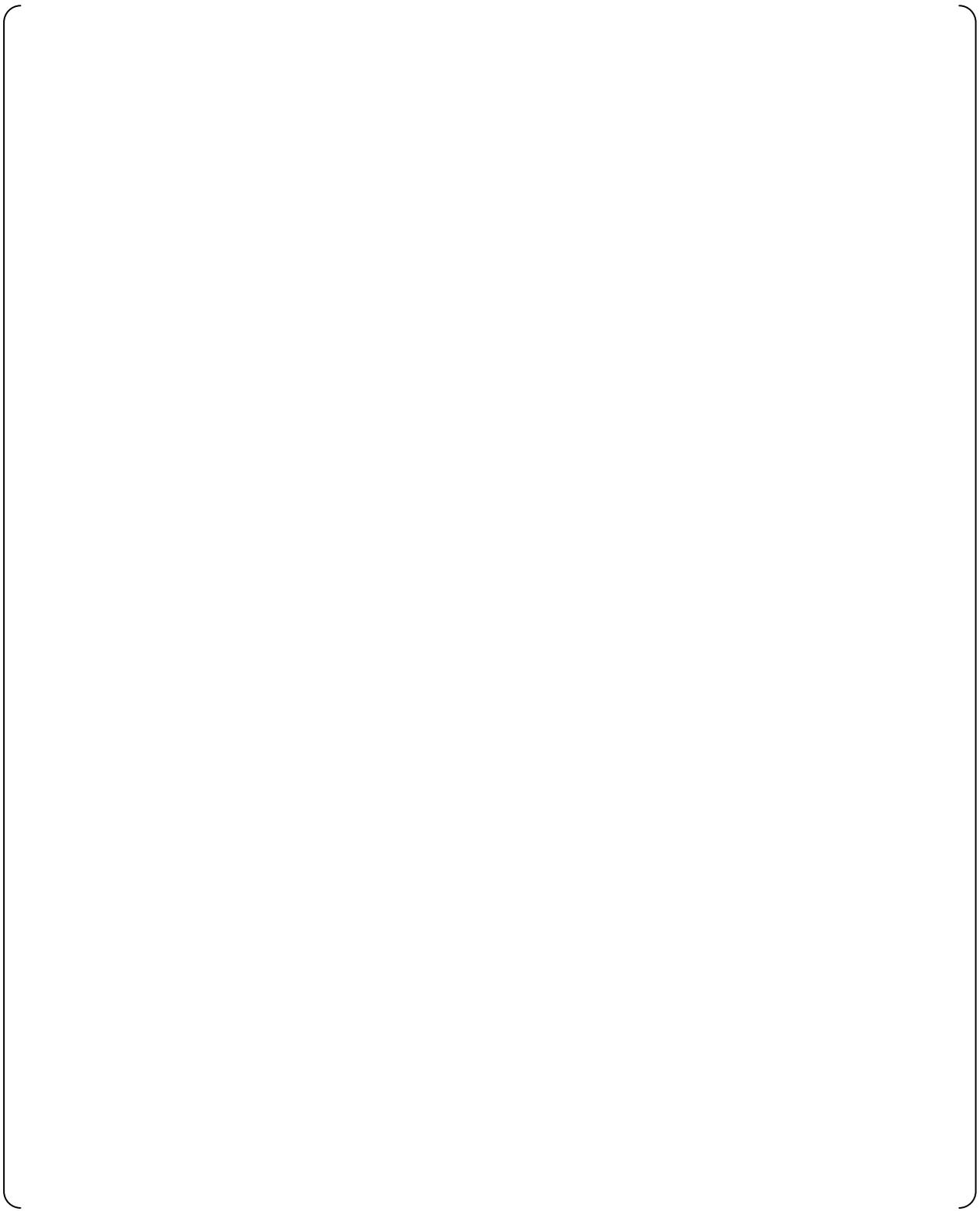
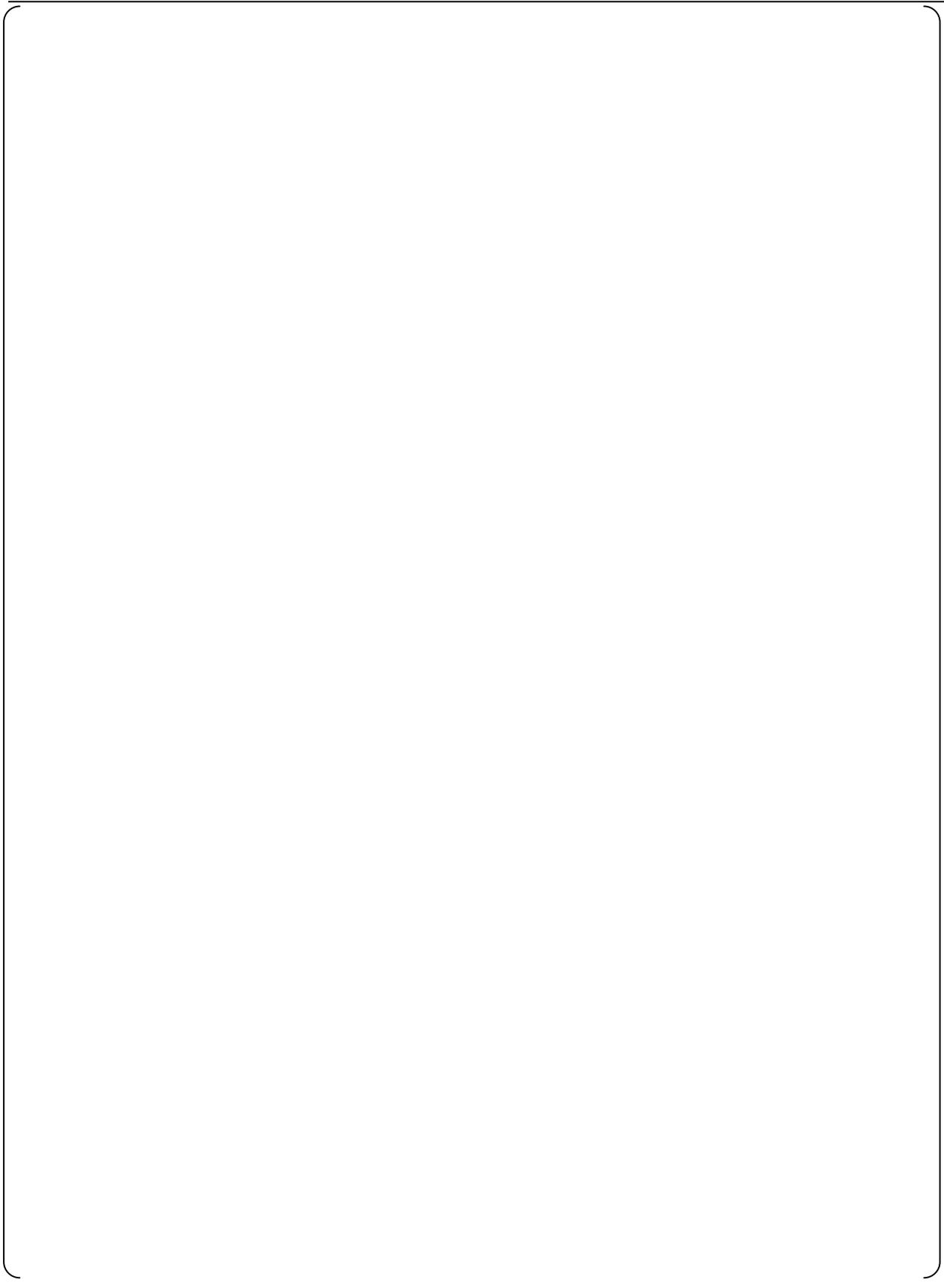
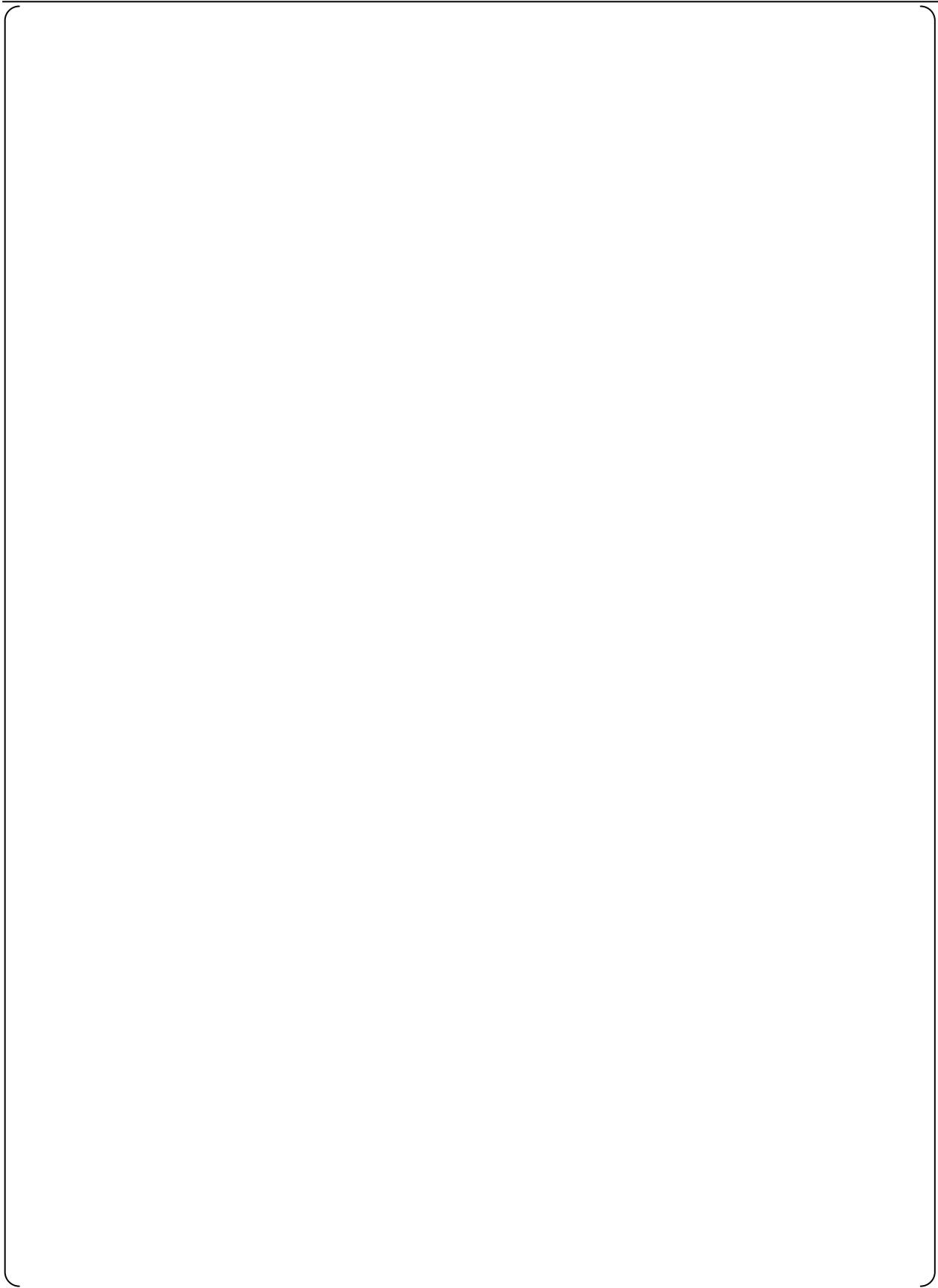


Figure C.2-1 Probability Assessment Flow

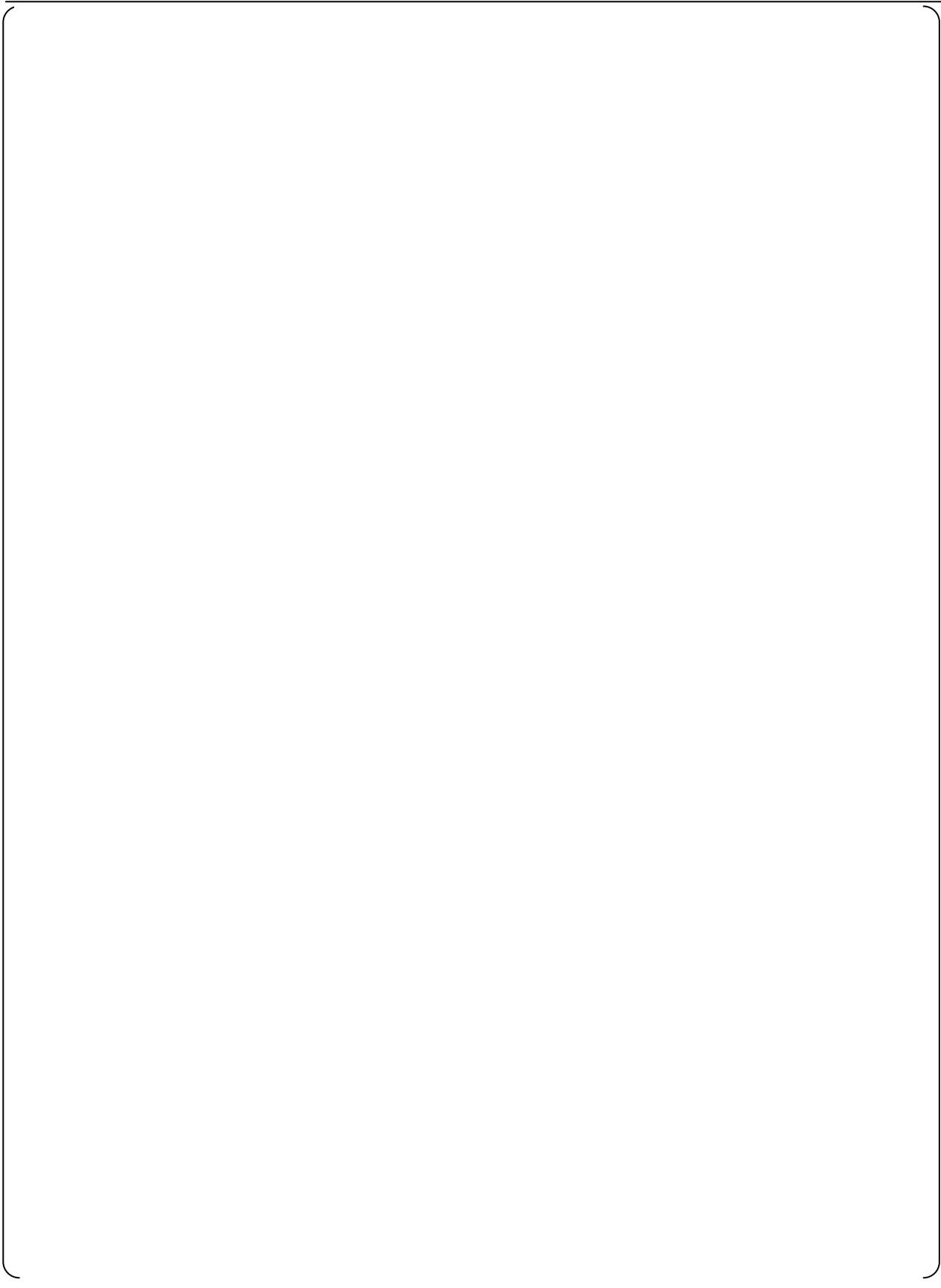
**Appendix D Analysis of Operational VDU (O-VDU) and
PCMS Spurious Commands**

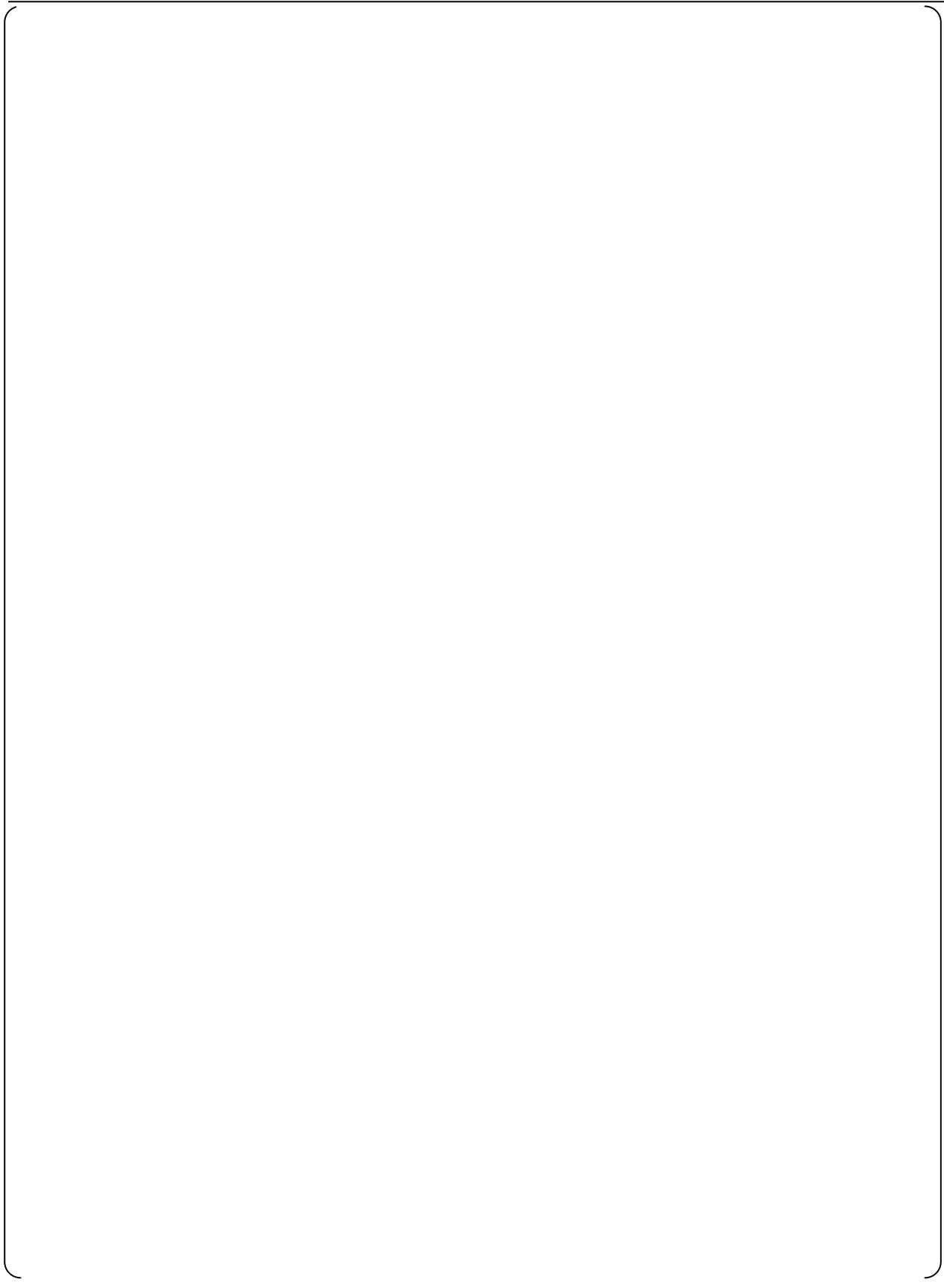


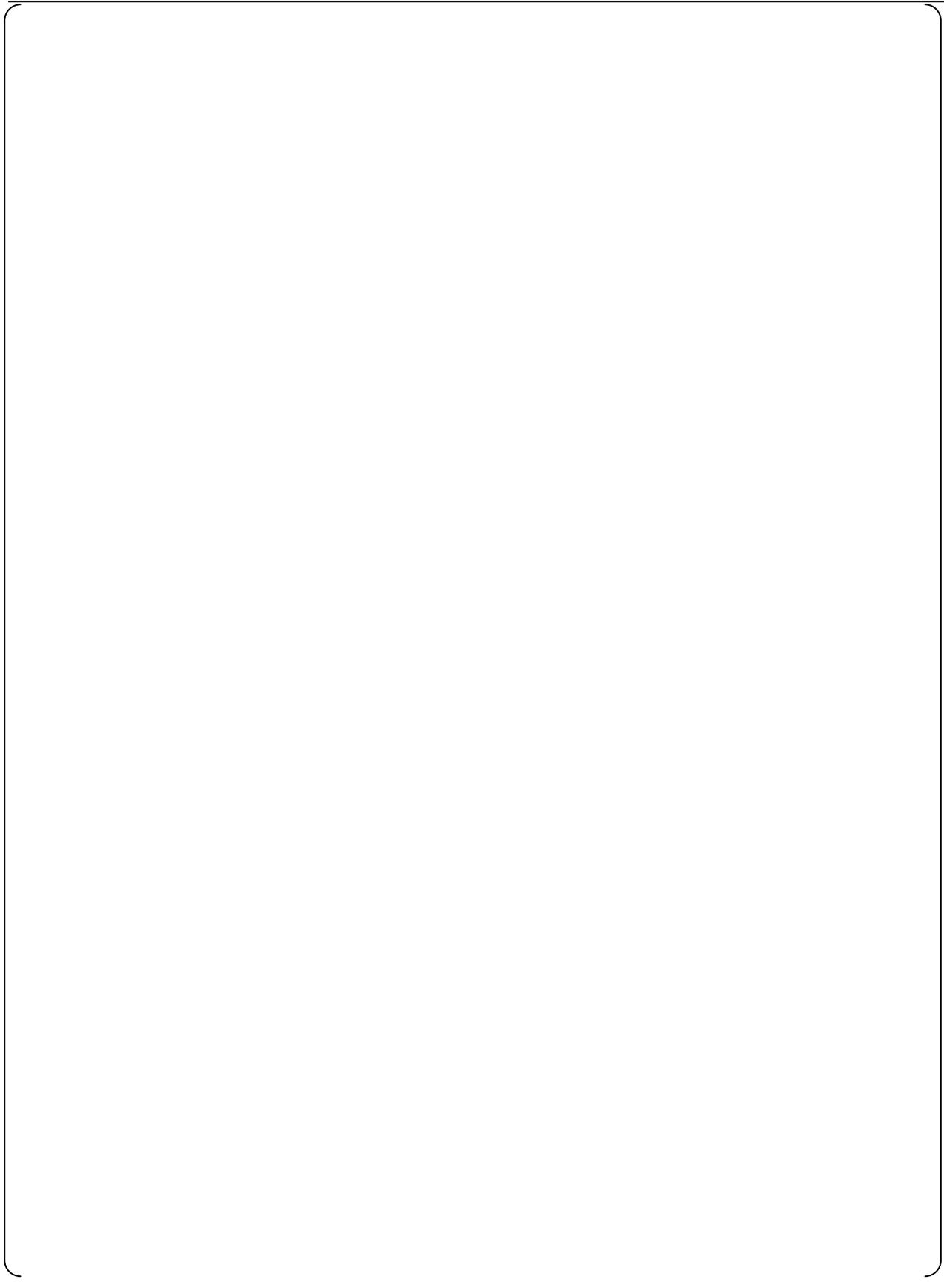


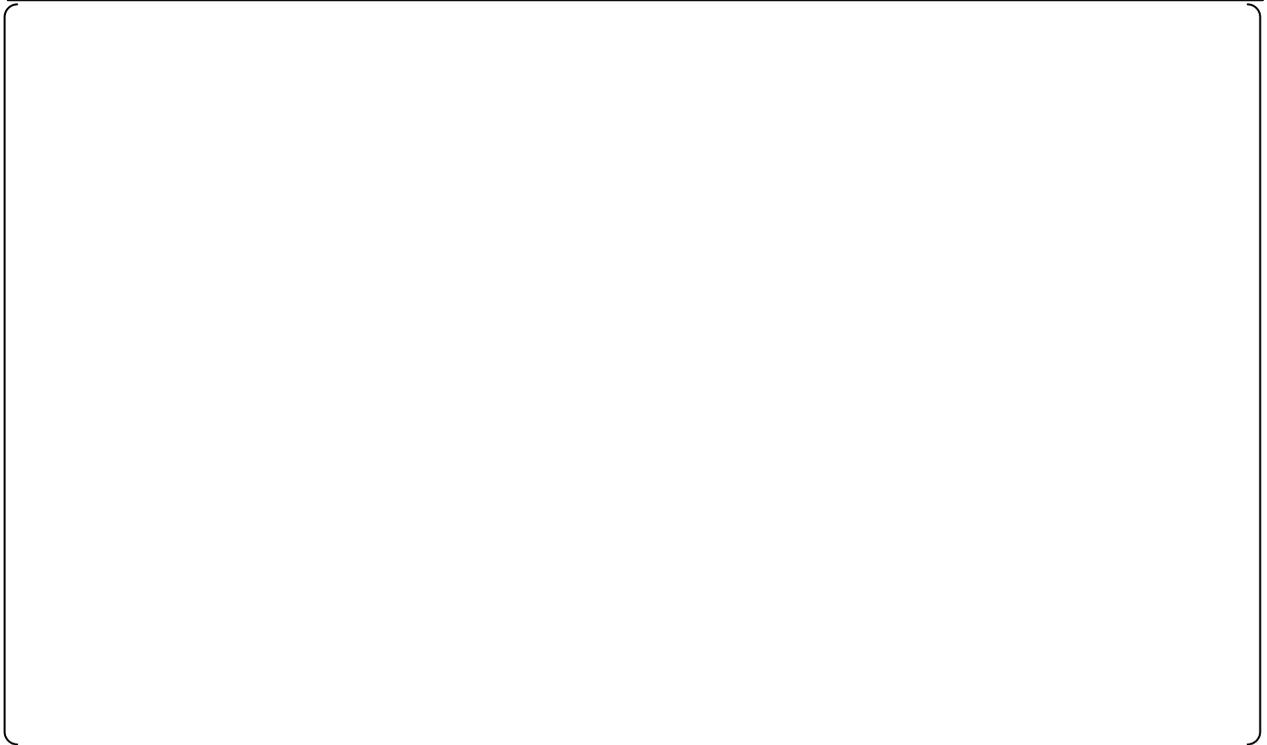










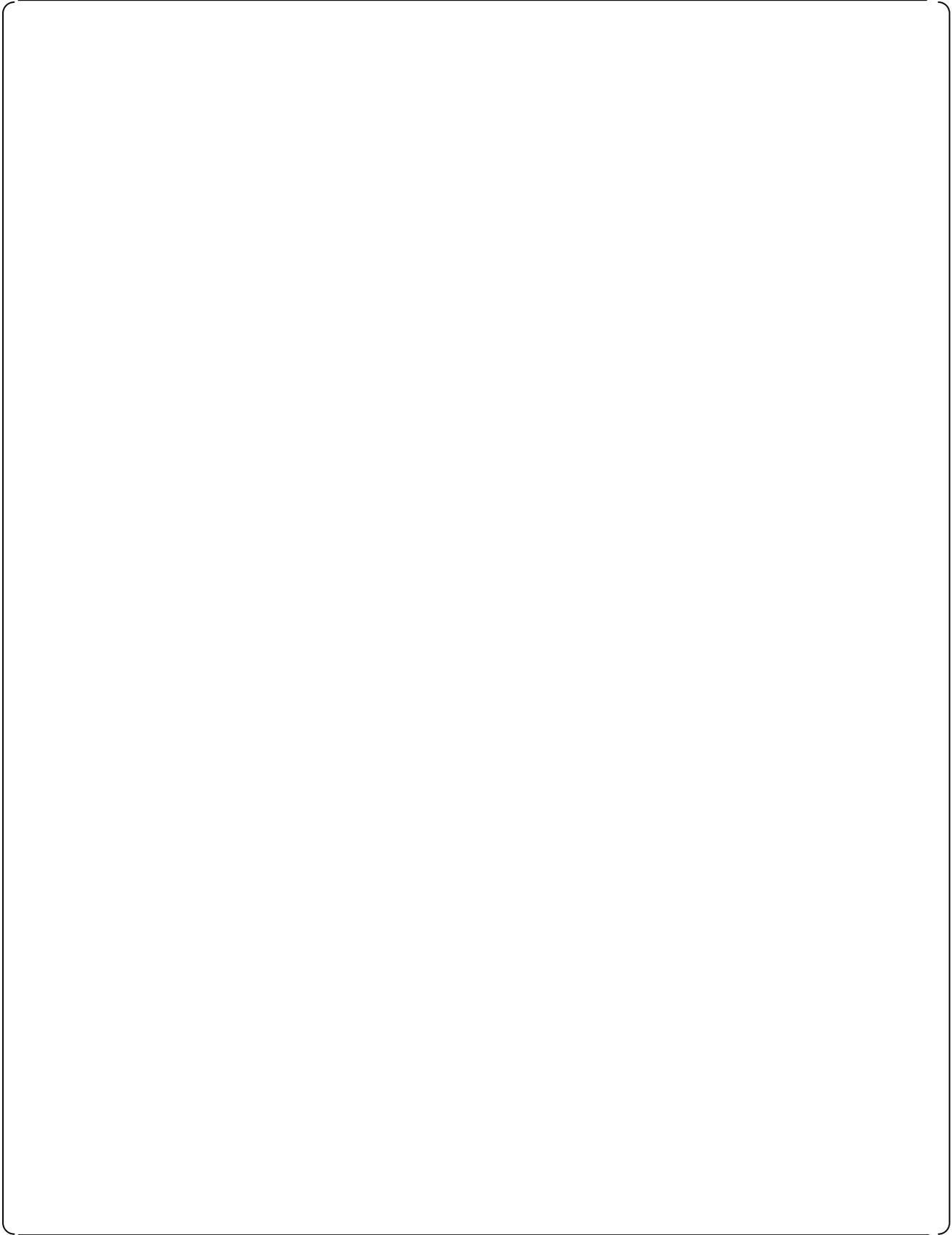


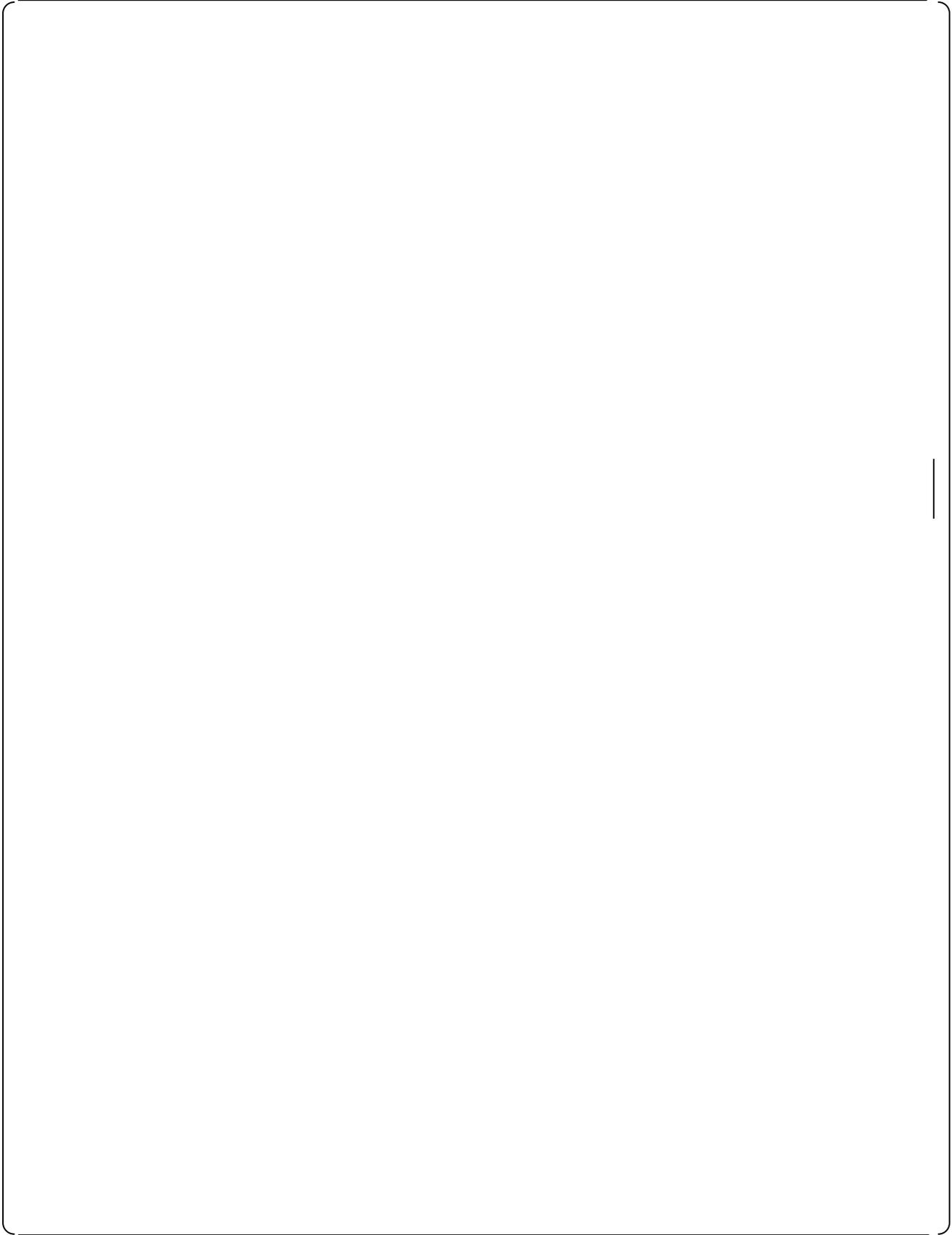
Appendix E Conformance to ISG-04

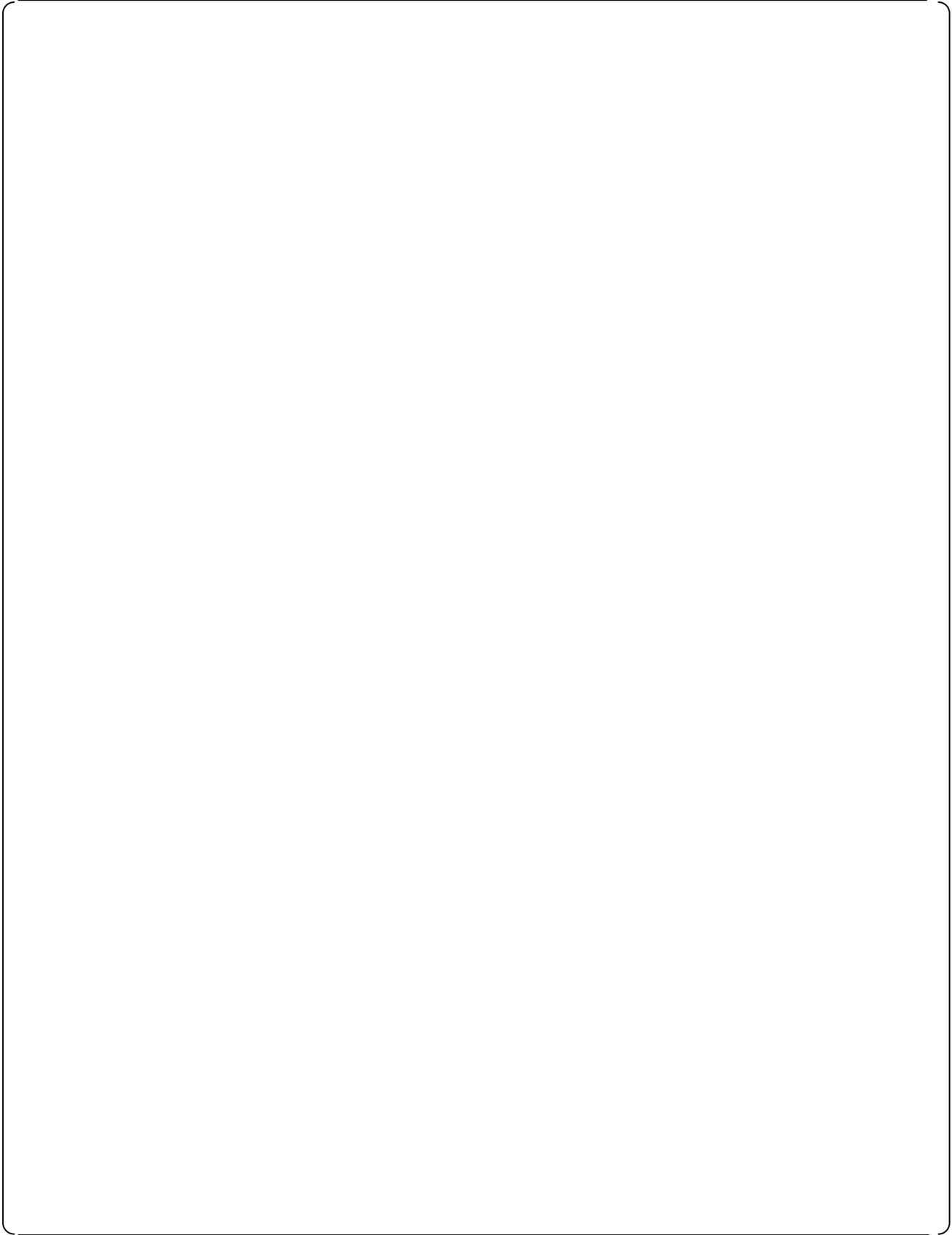
This Appendix E describes conformance of the interdivisional communication design in the US-APWR PSMS to Staff Positions of DI&C-ISG-04. The section numbers in this Appendix E follow the section numbers in DI&C-ISG-04. All sections pertain to DI&C-ISG-04 "Task Working Group#4: Highly-Integrated Control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

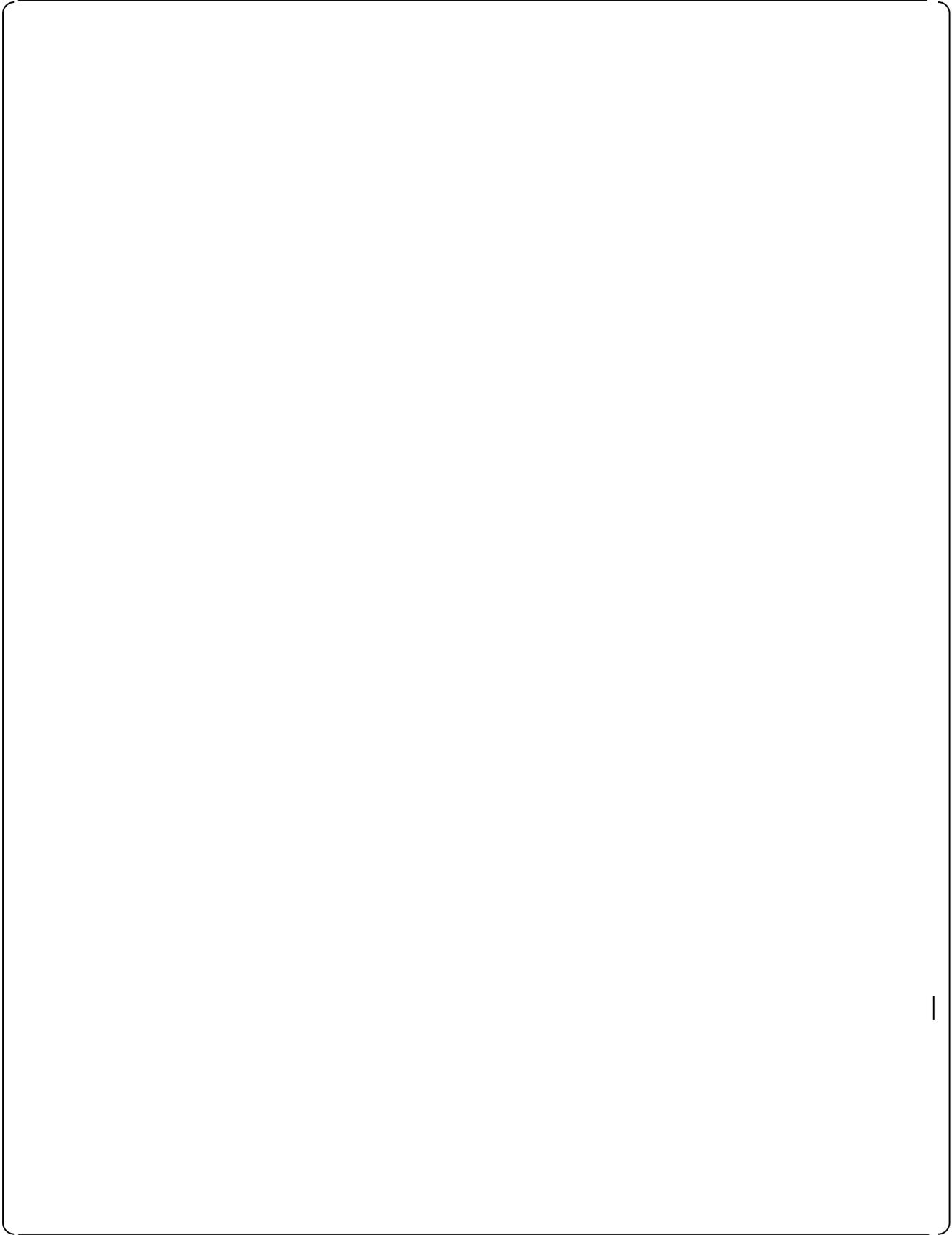
The following two types of interdivisional communication designs are applied to the US-APWR safety-related I&C architecture, and the conformance analyses are separately performed to both of the following two application types.

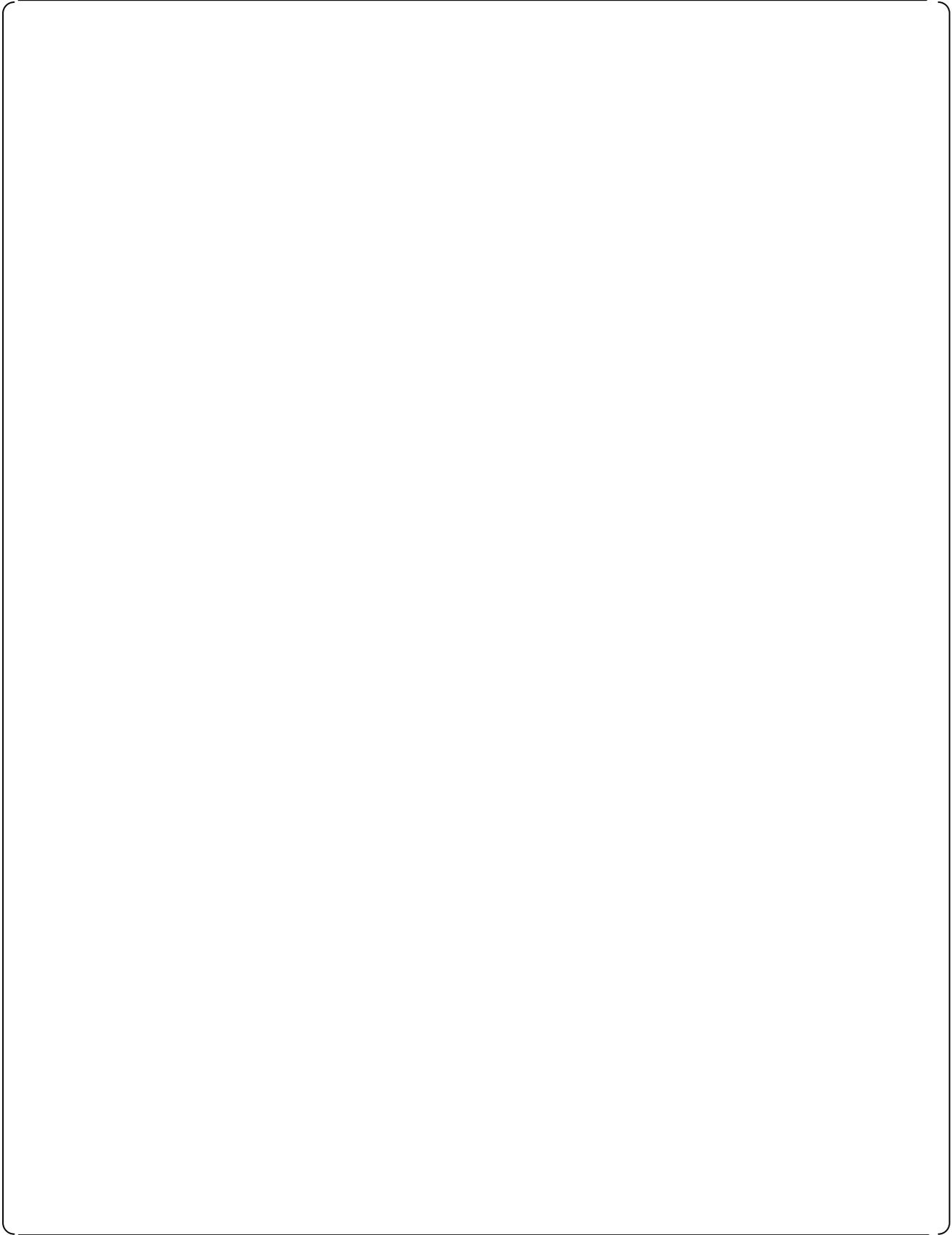


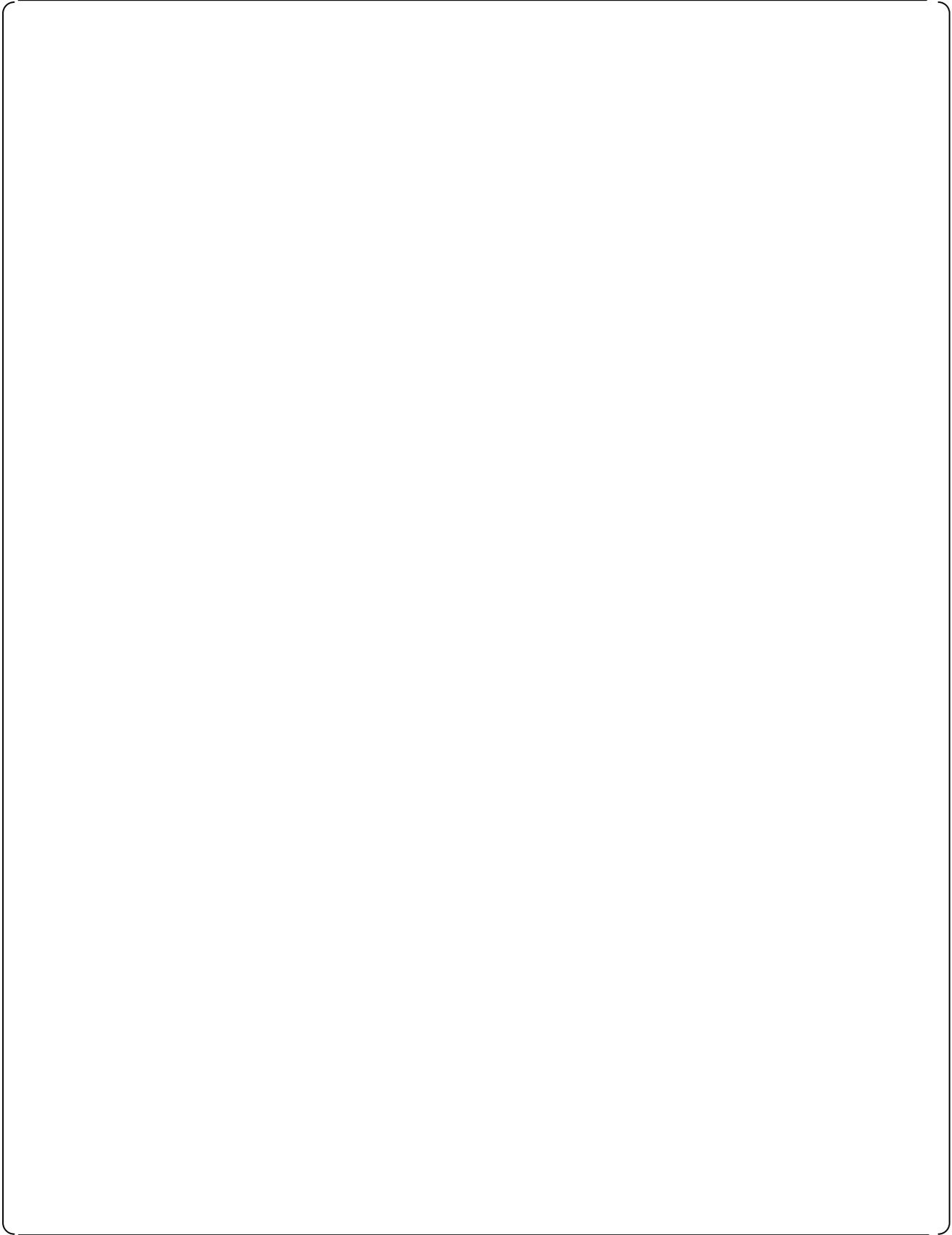


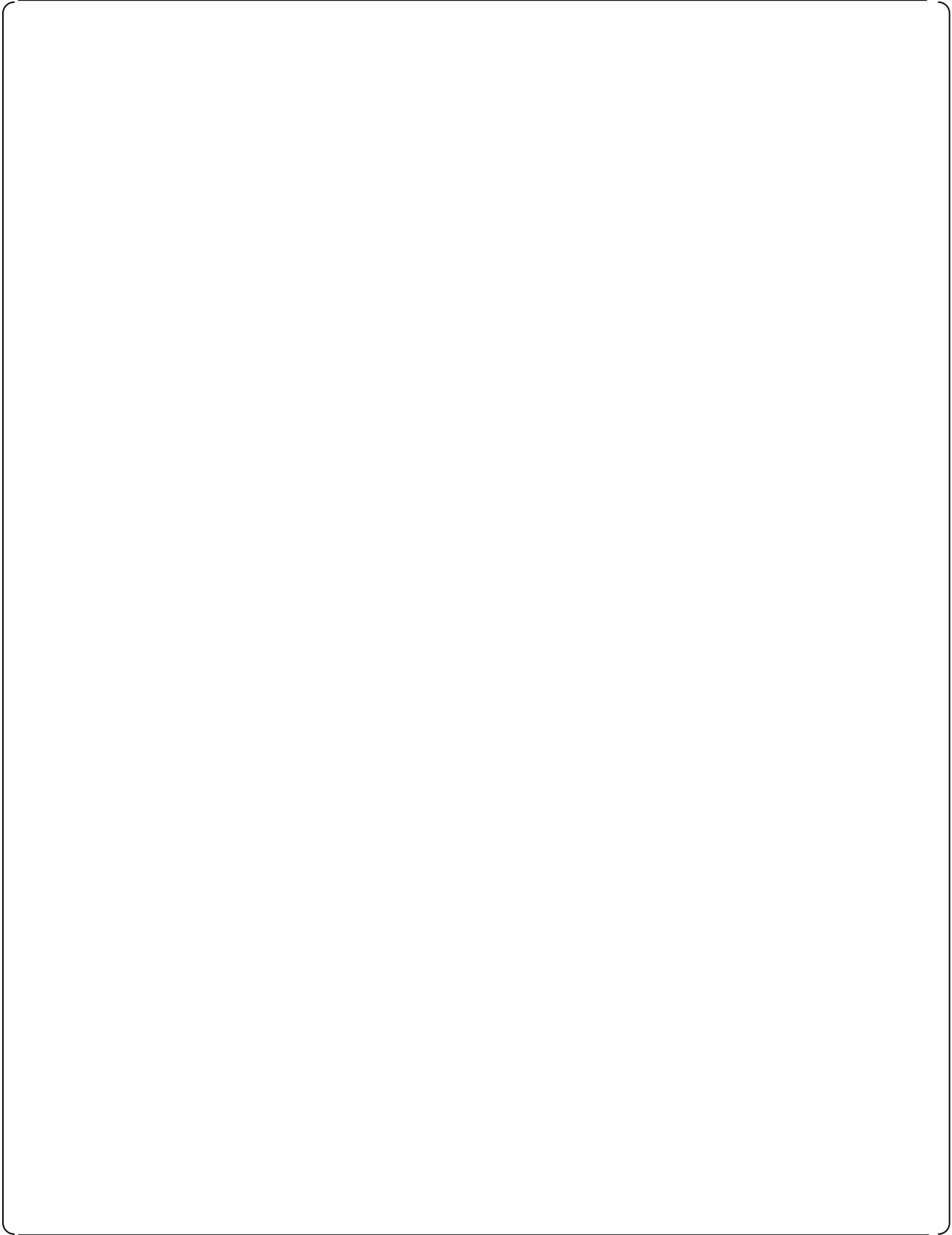


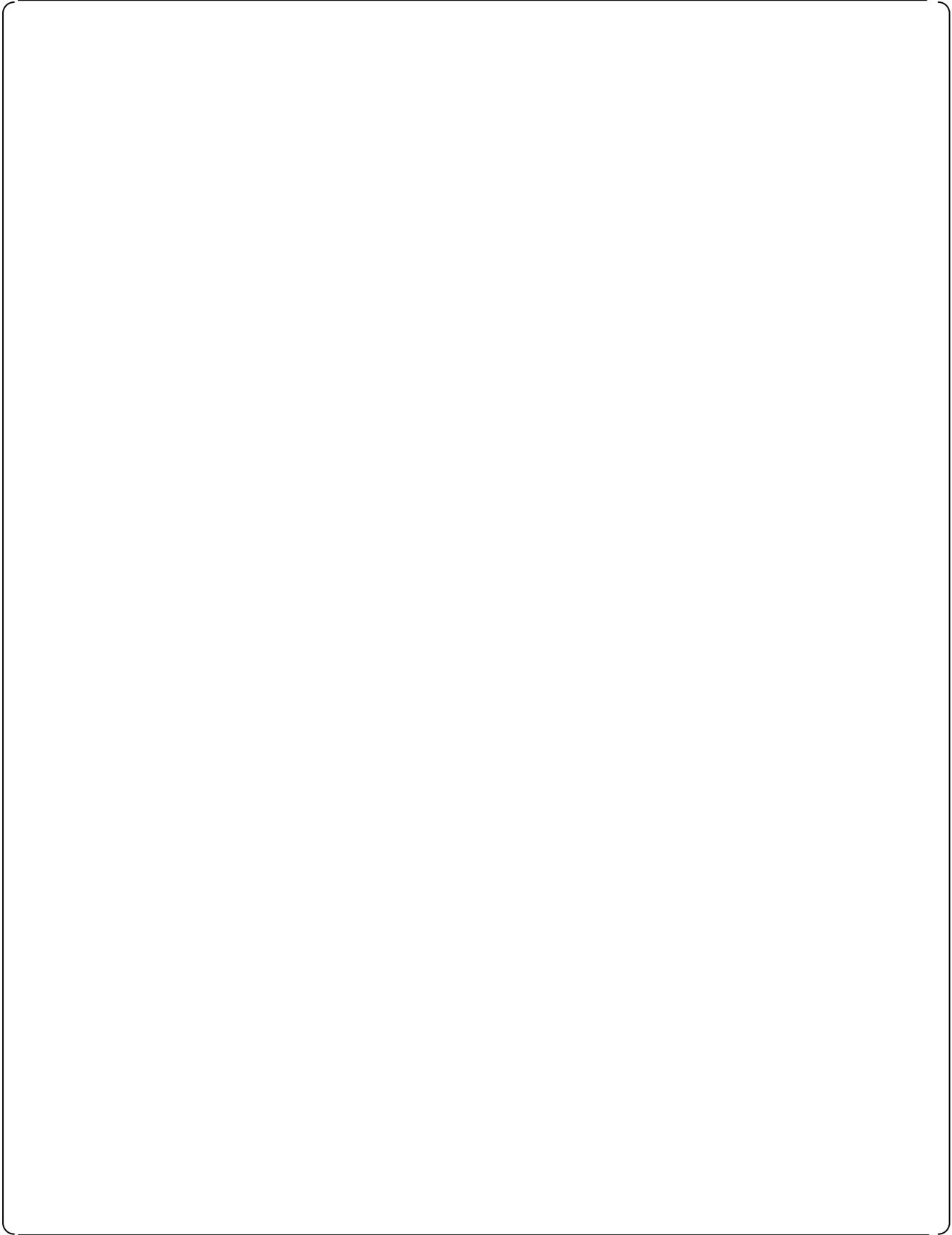


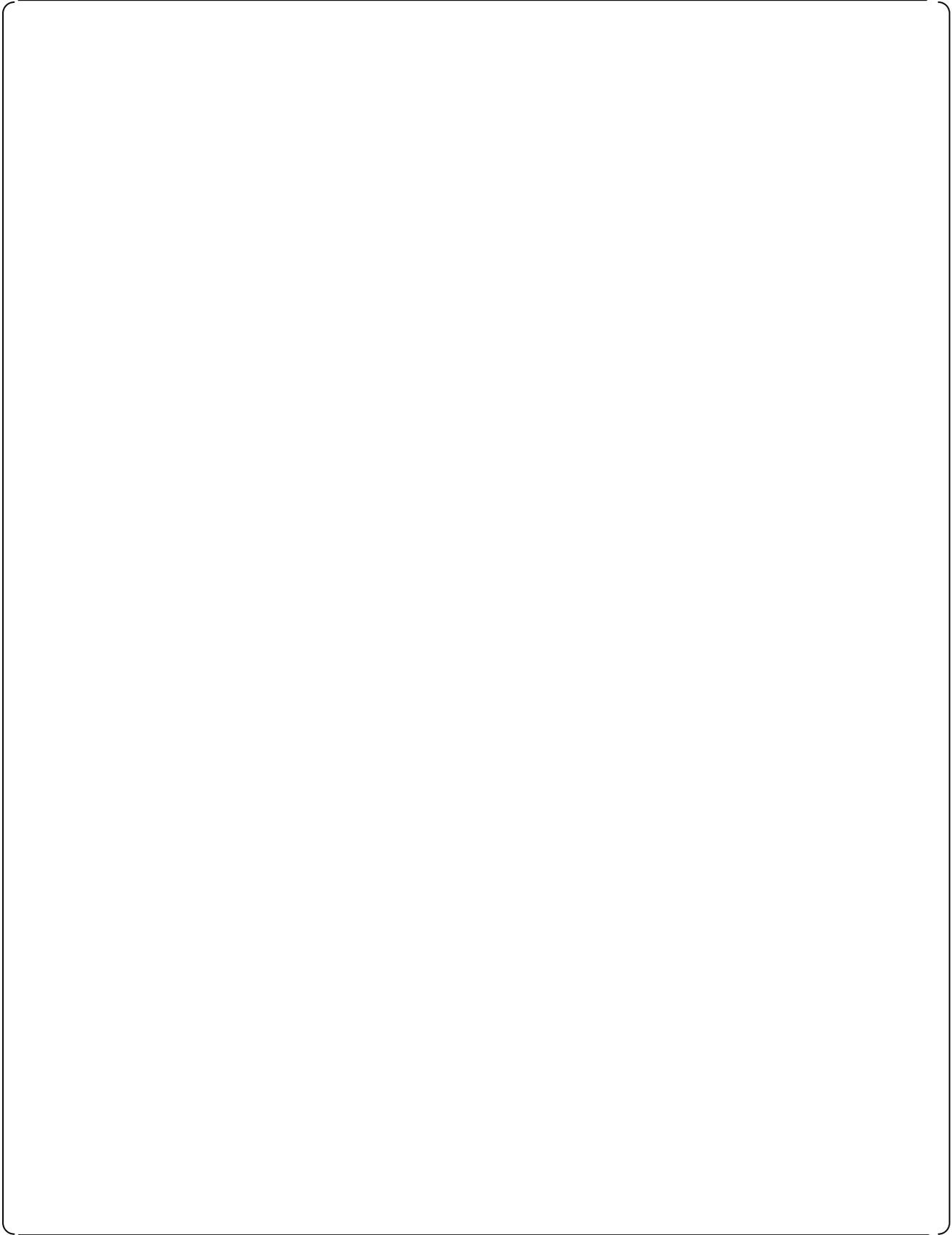


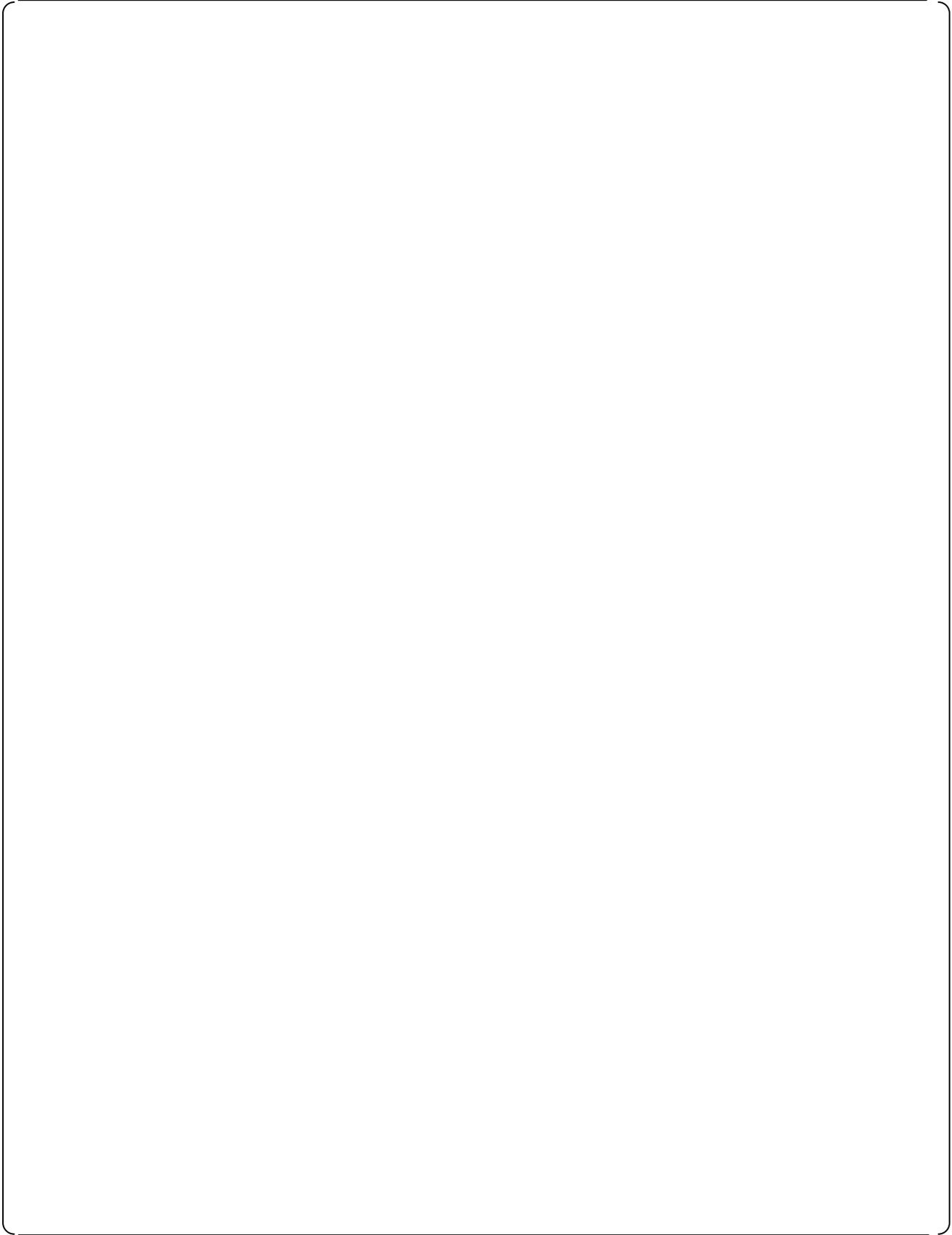


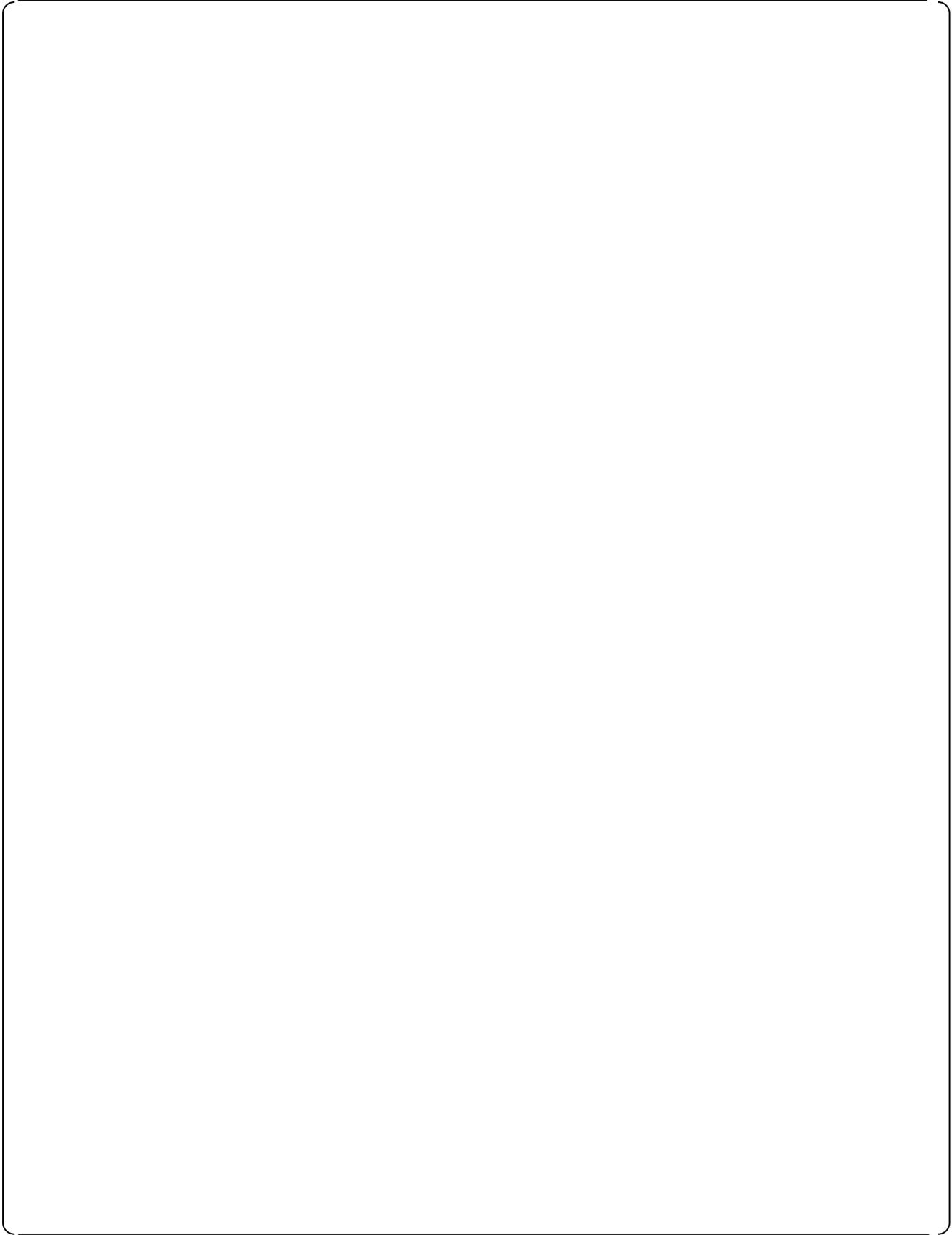


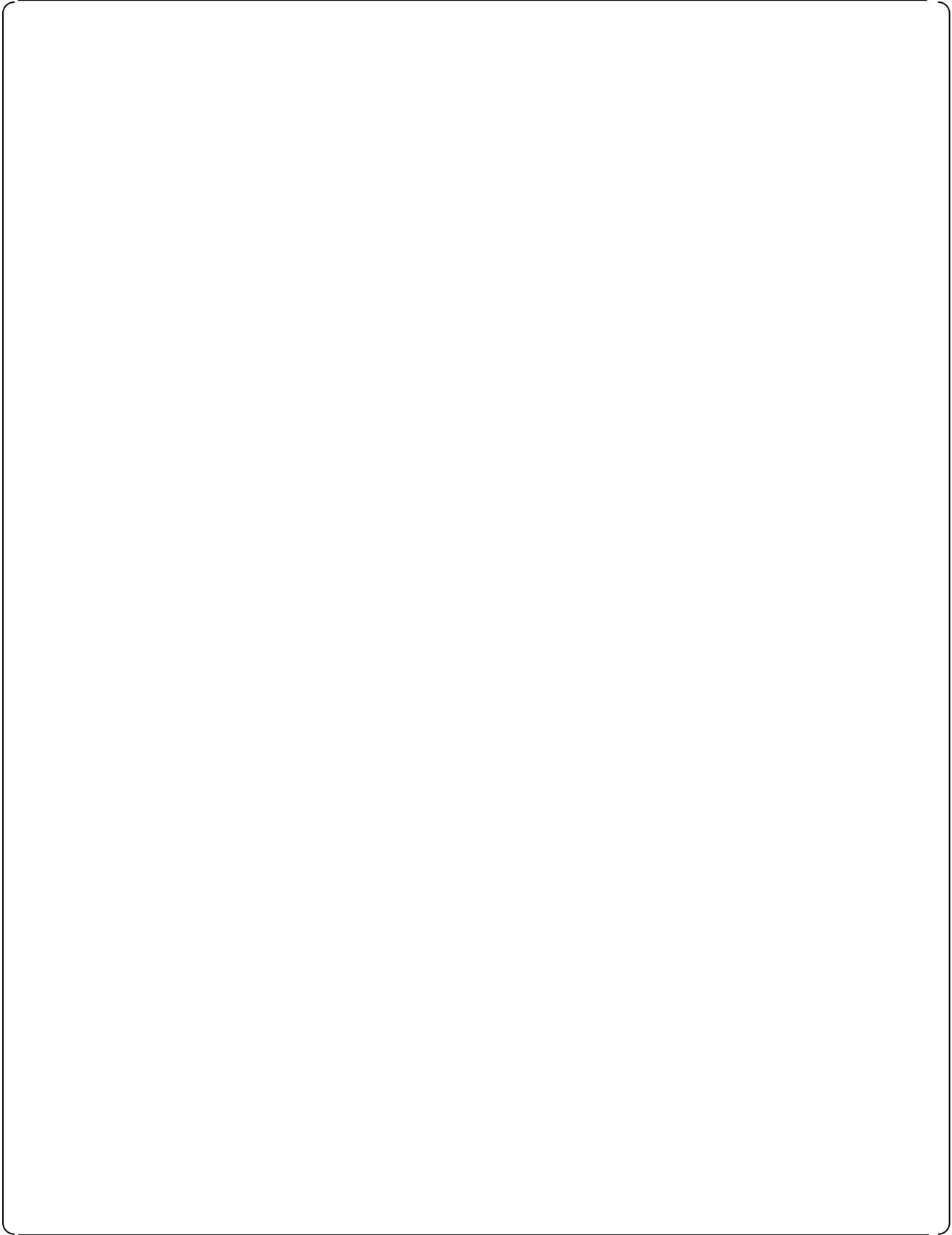


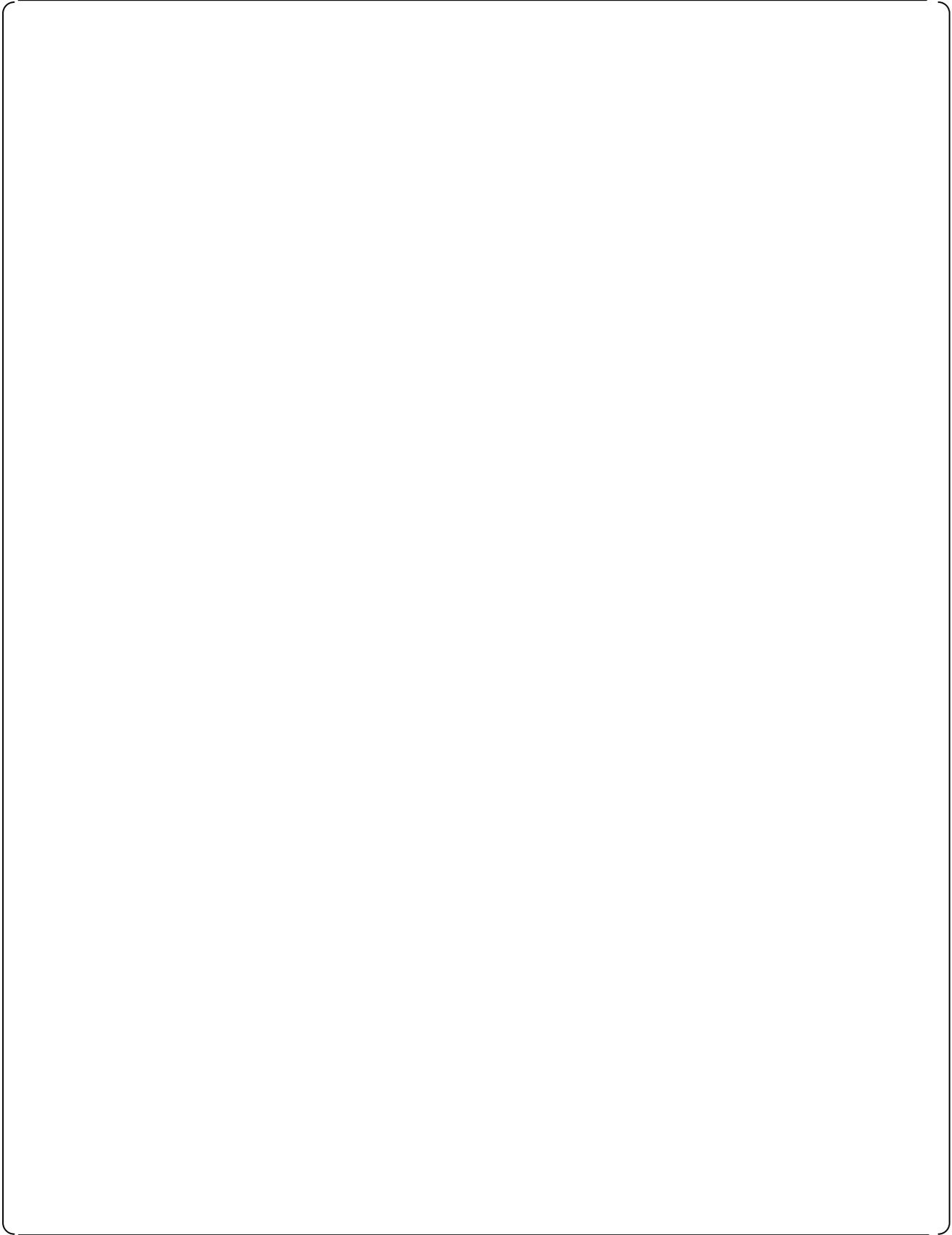


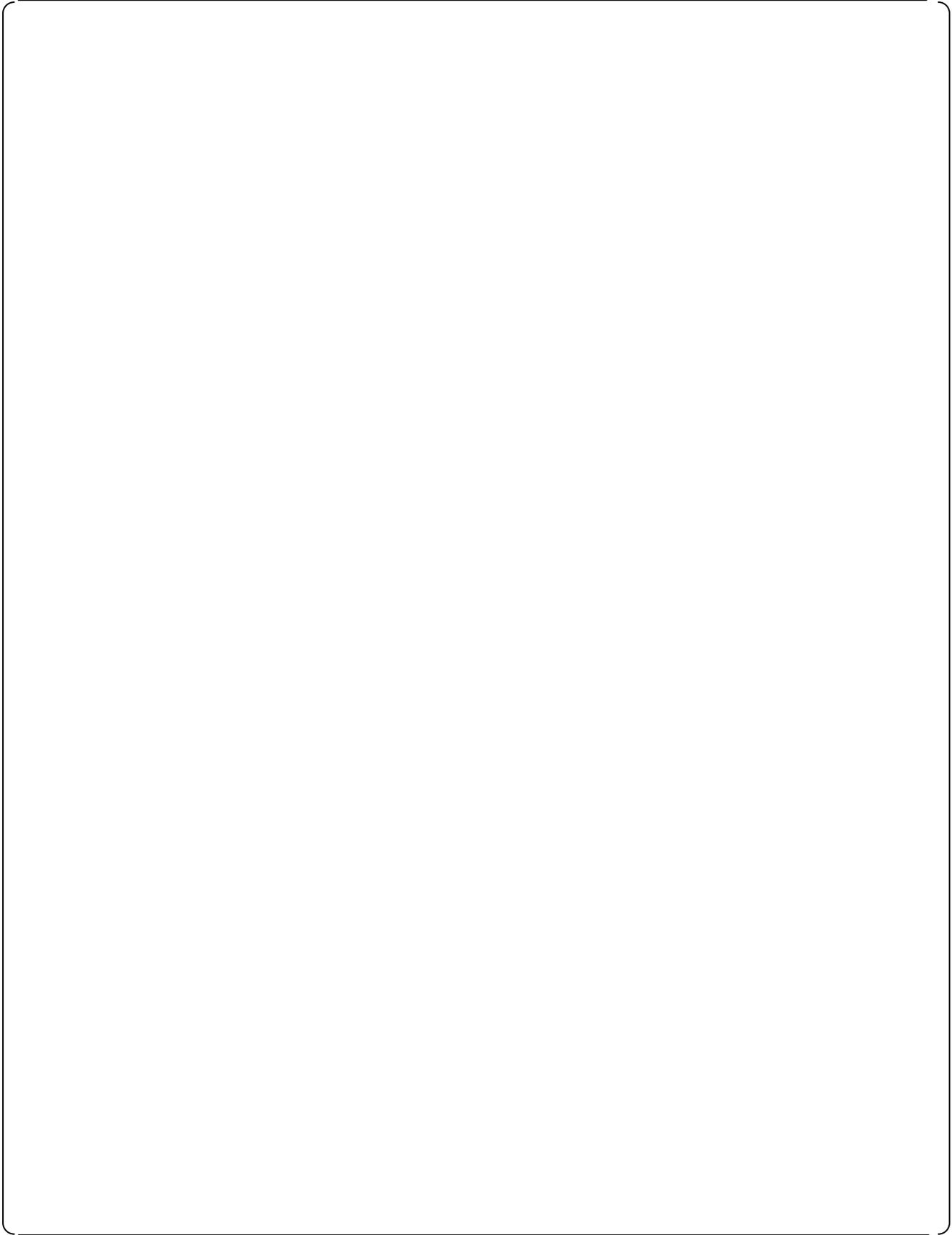


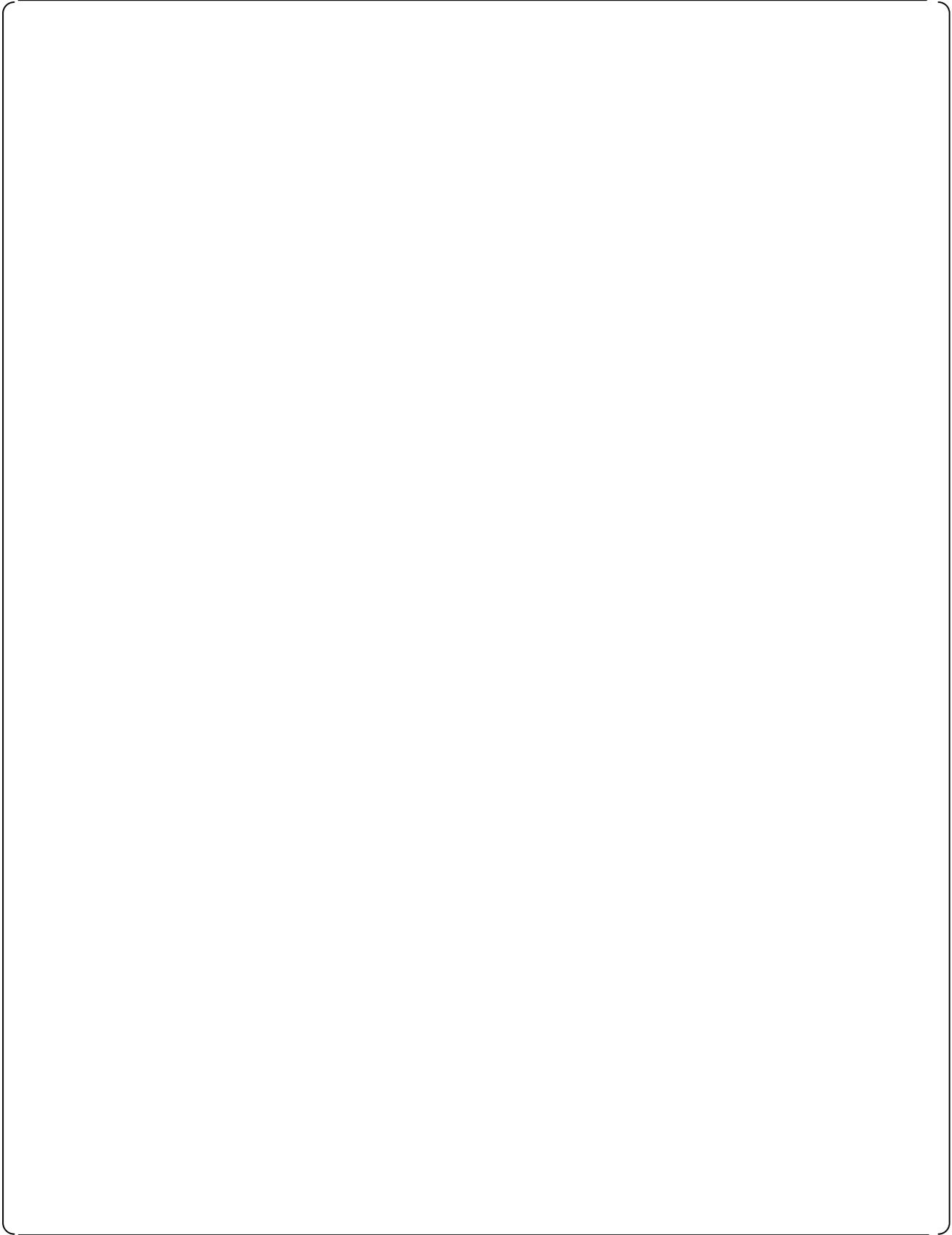


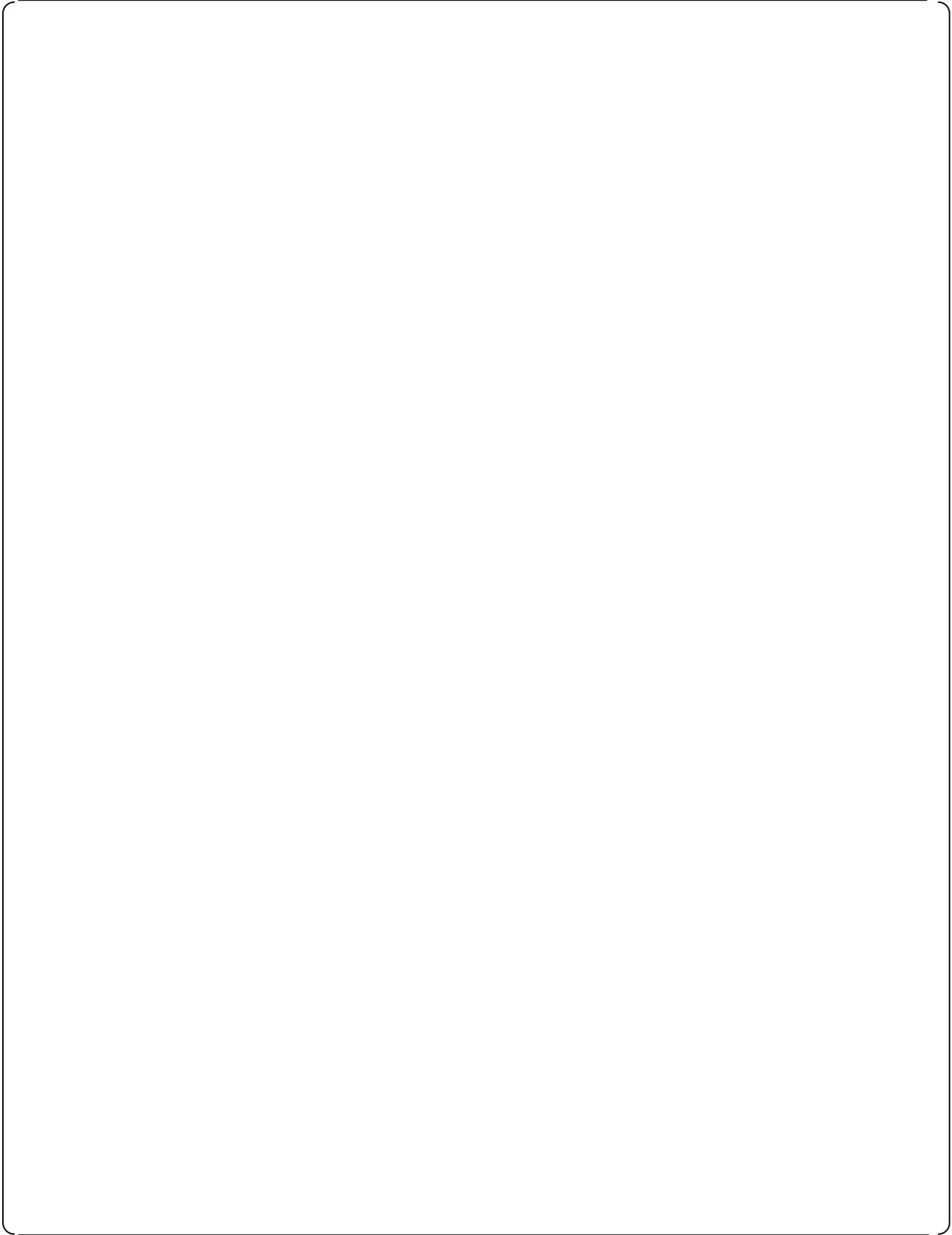


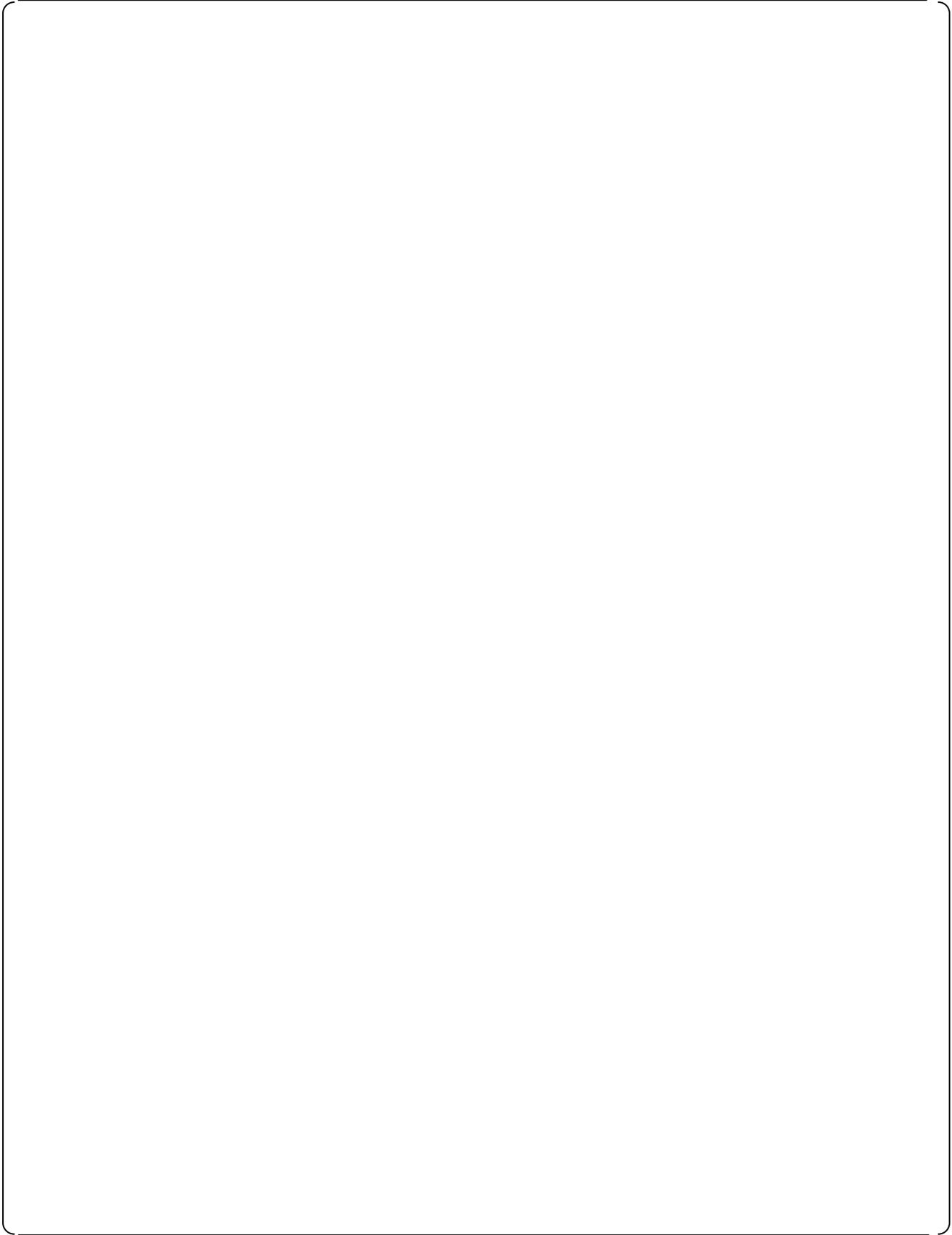


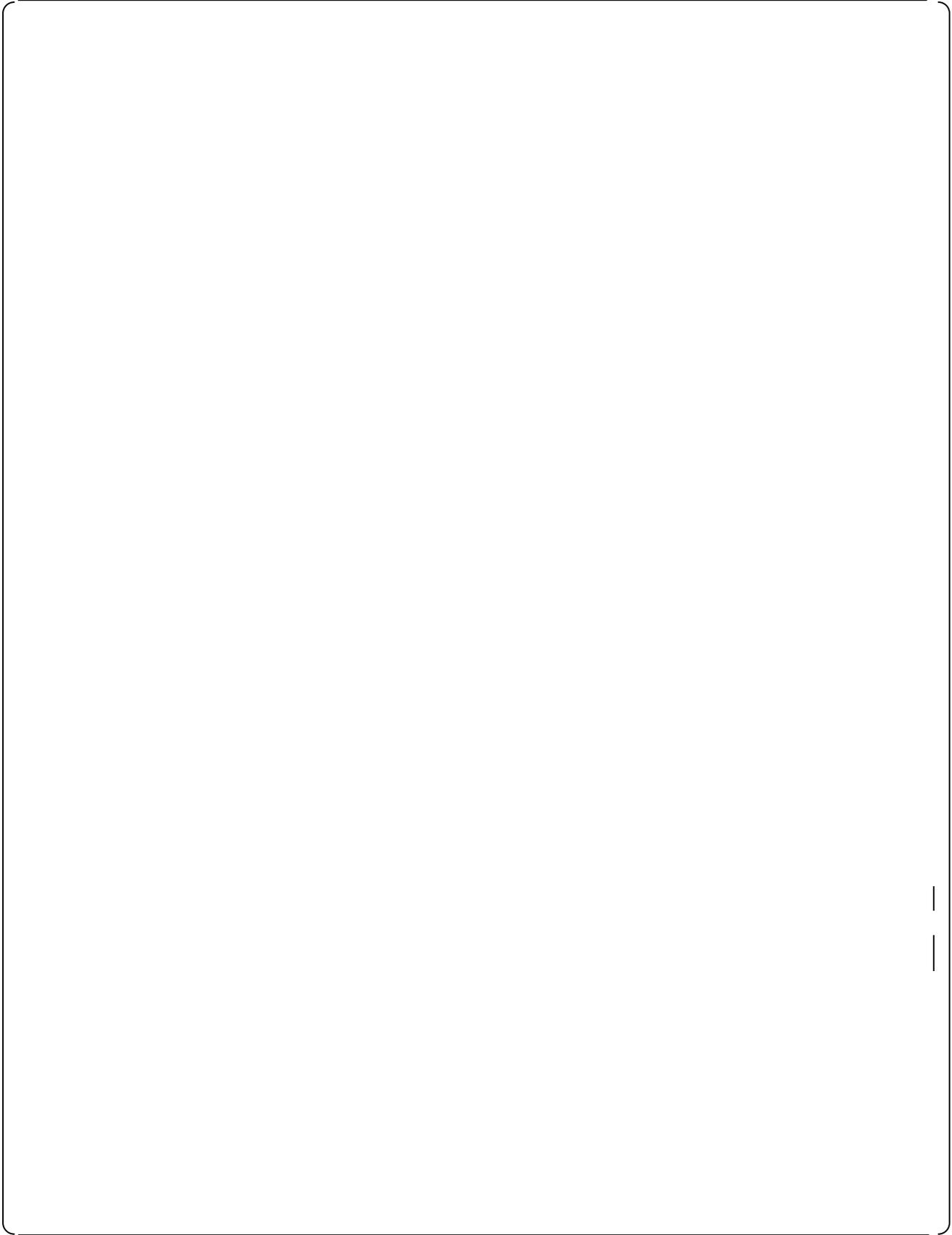


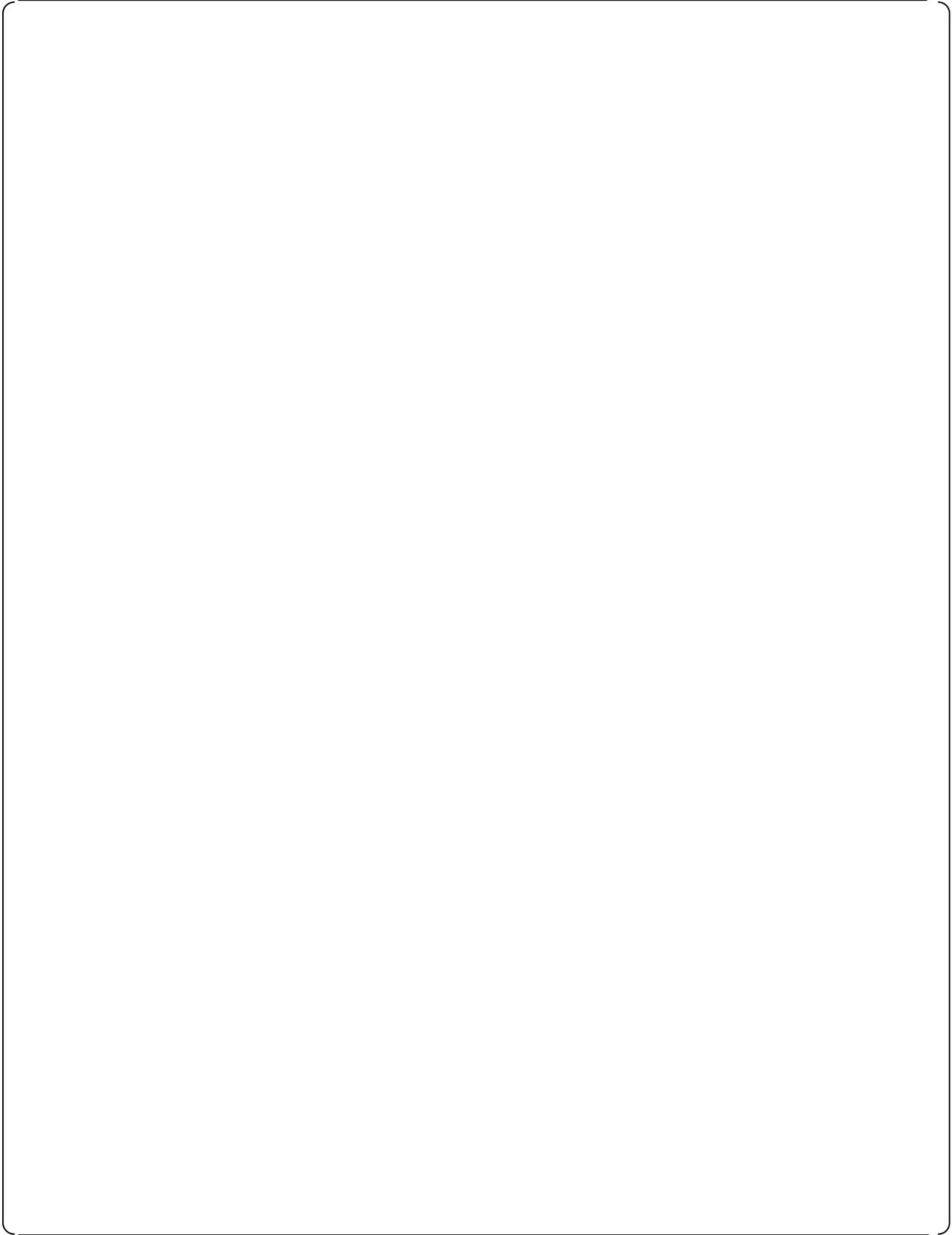


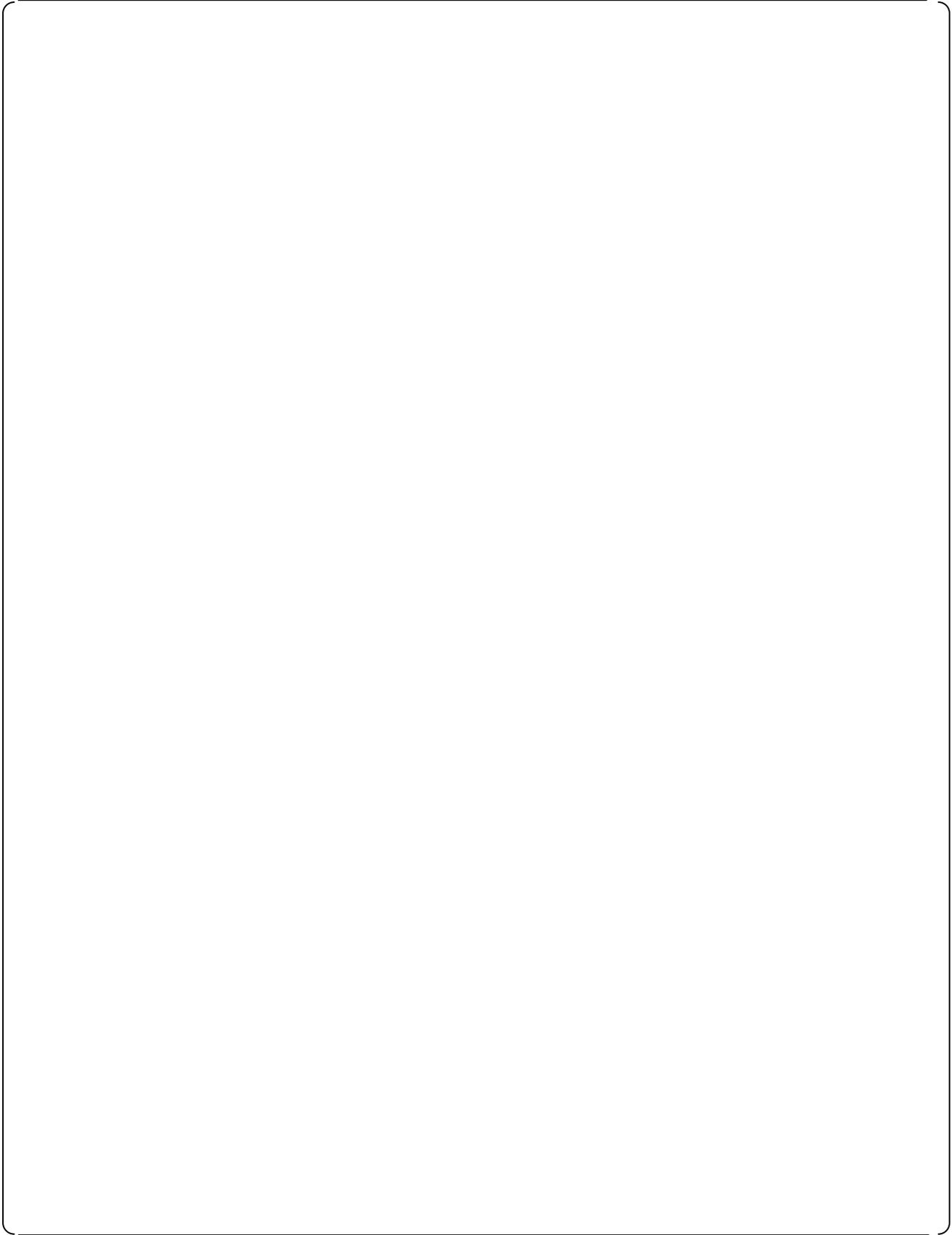


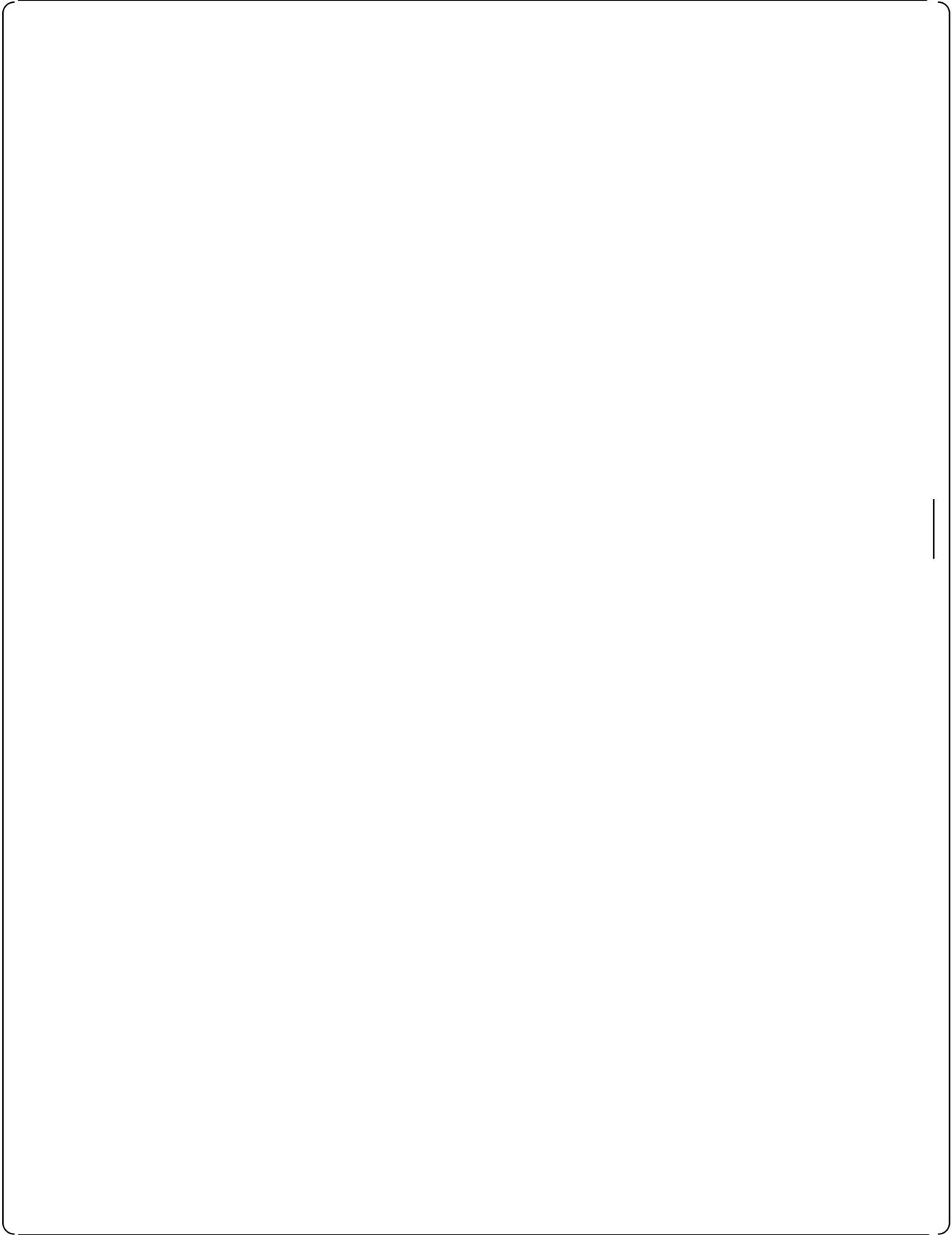


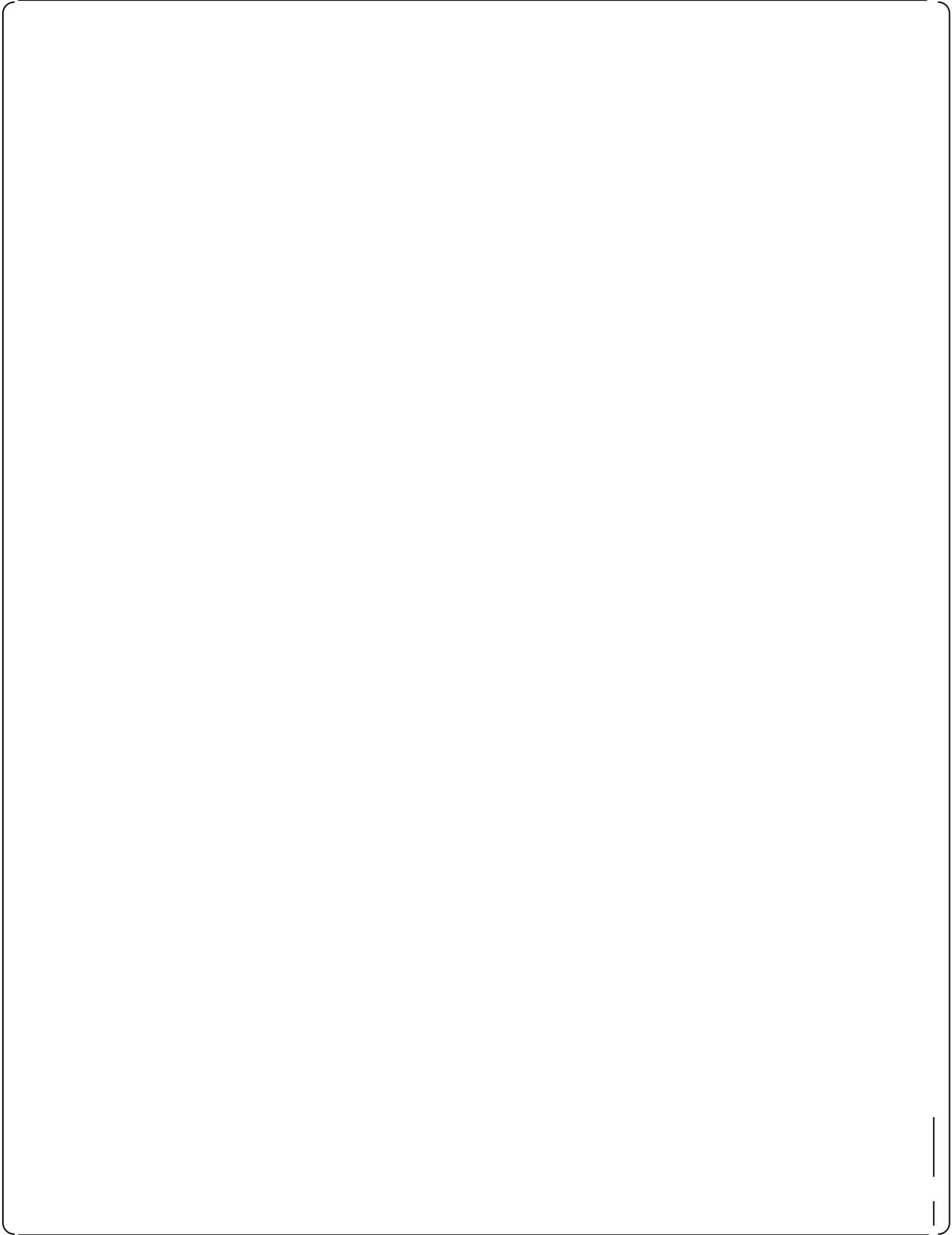


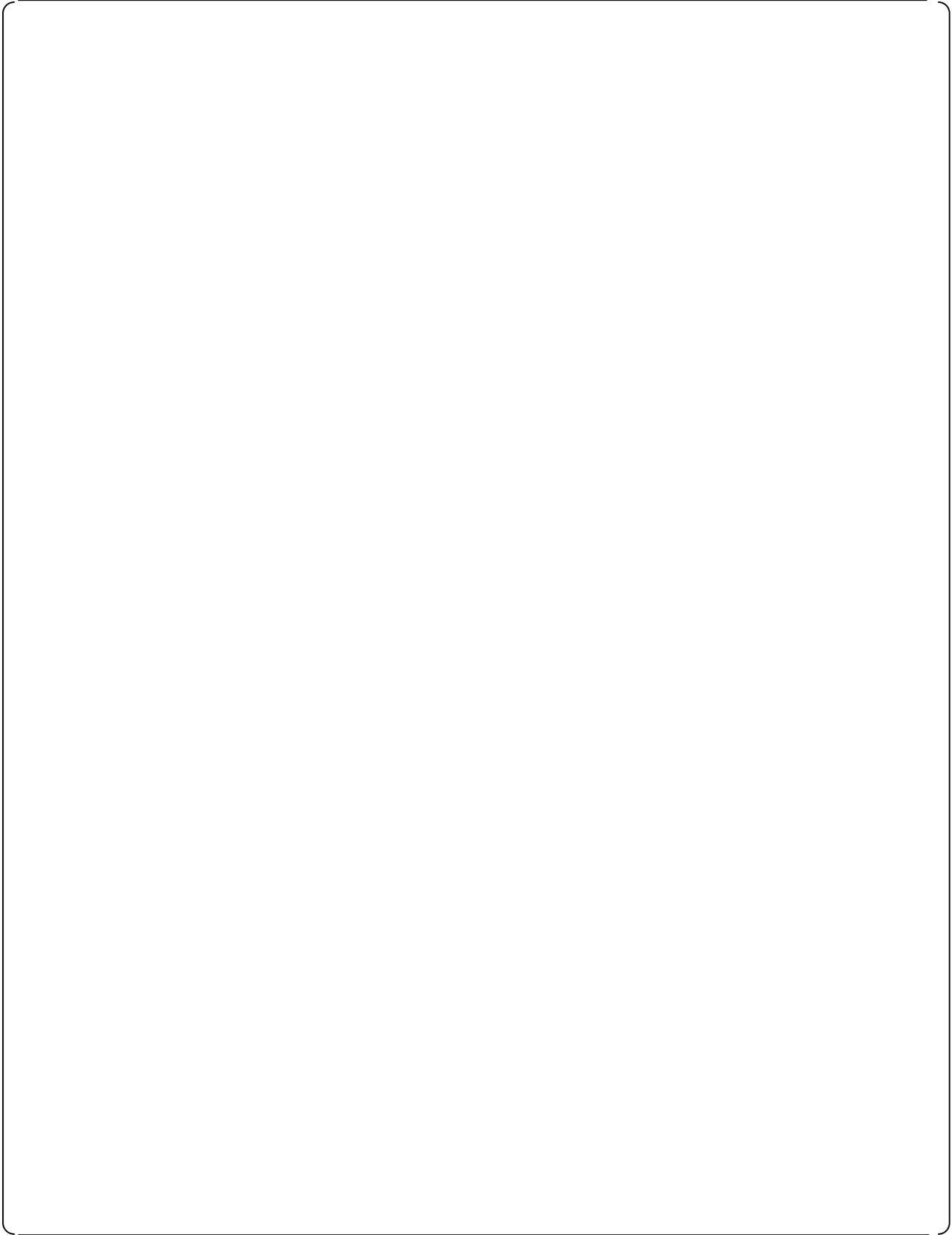


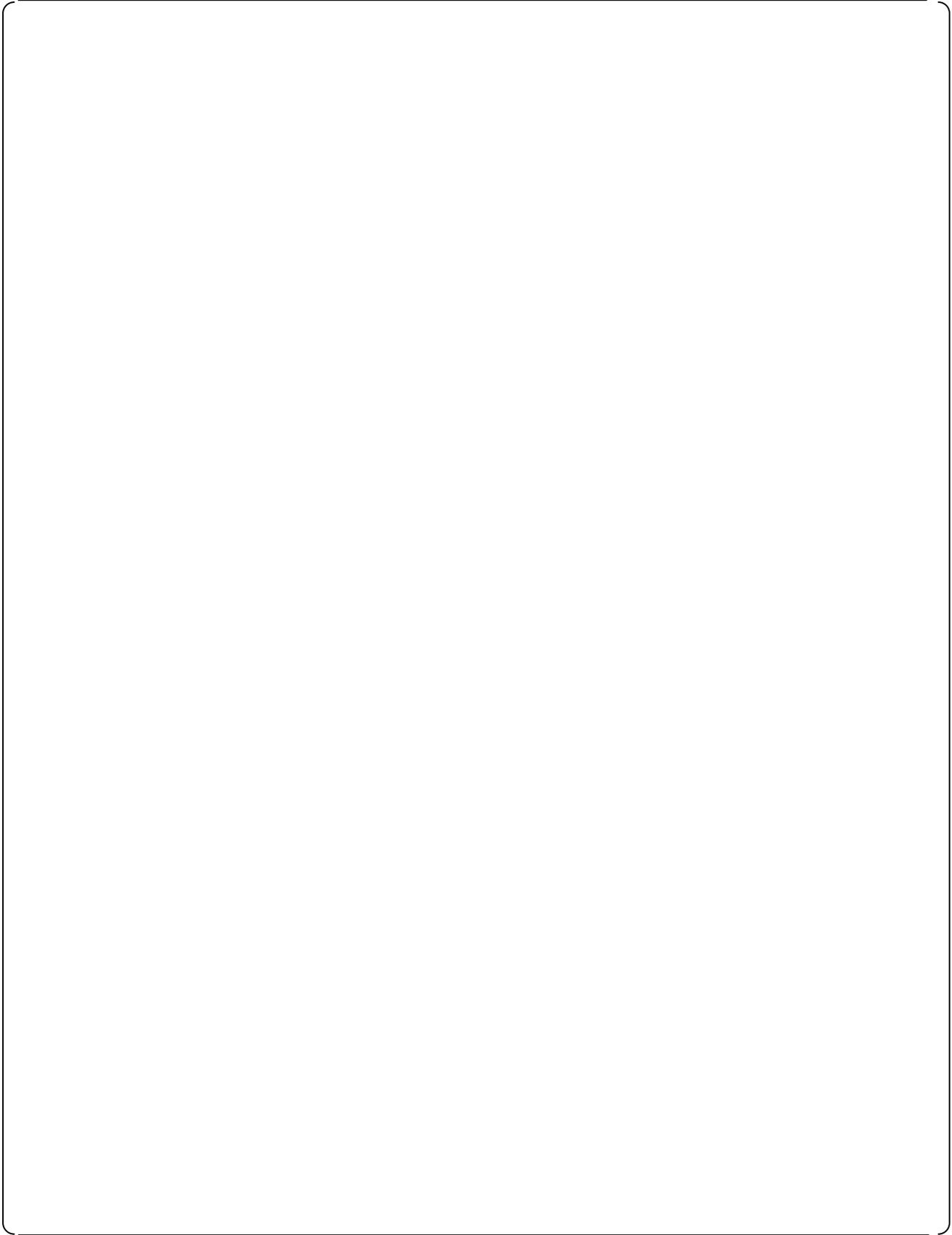


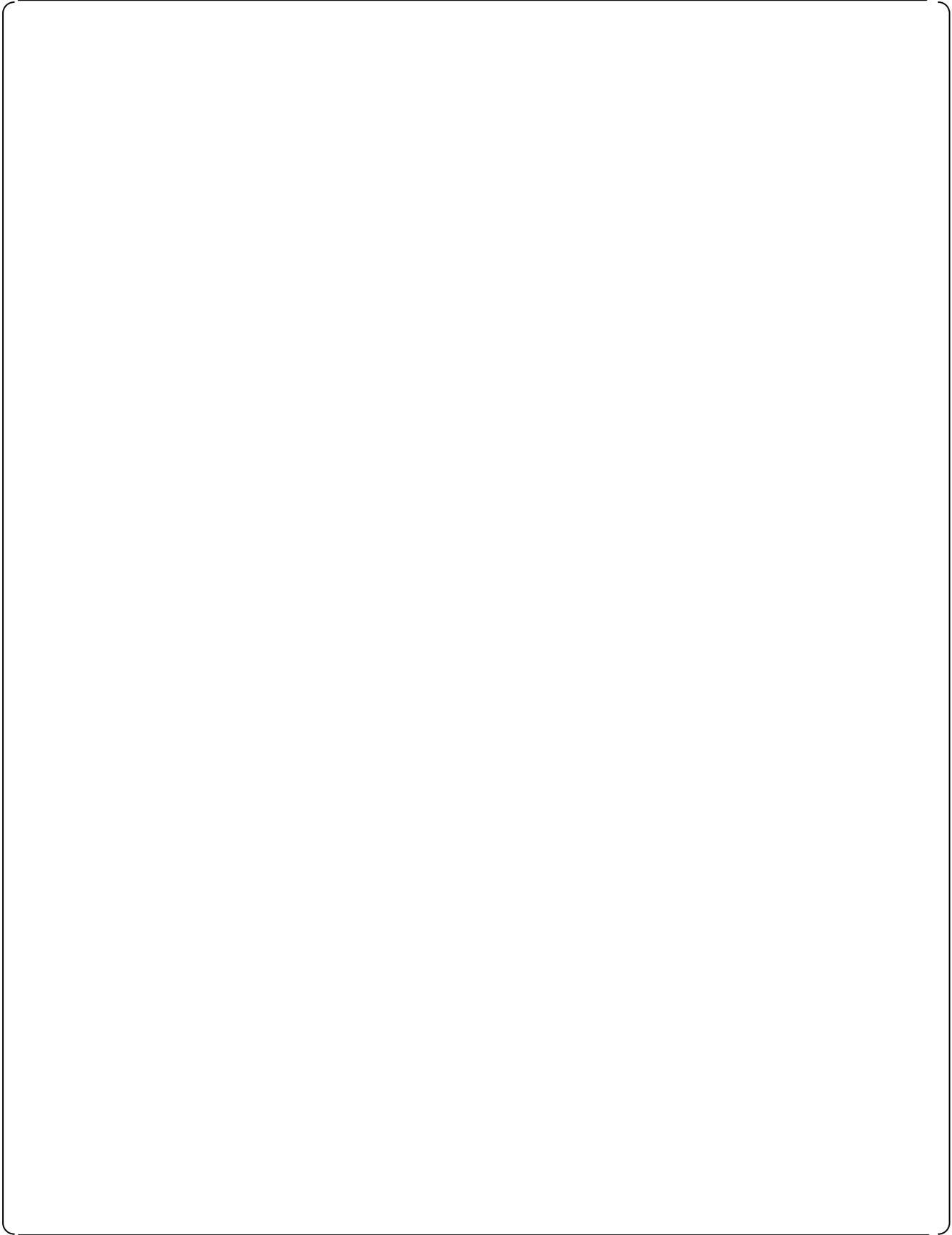


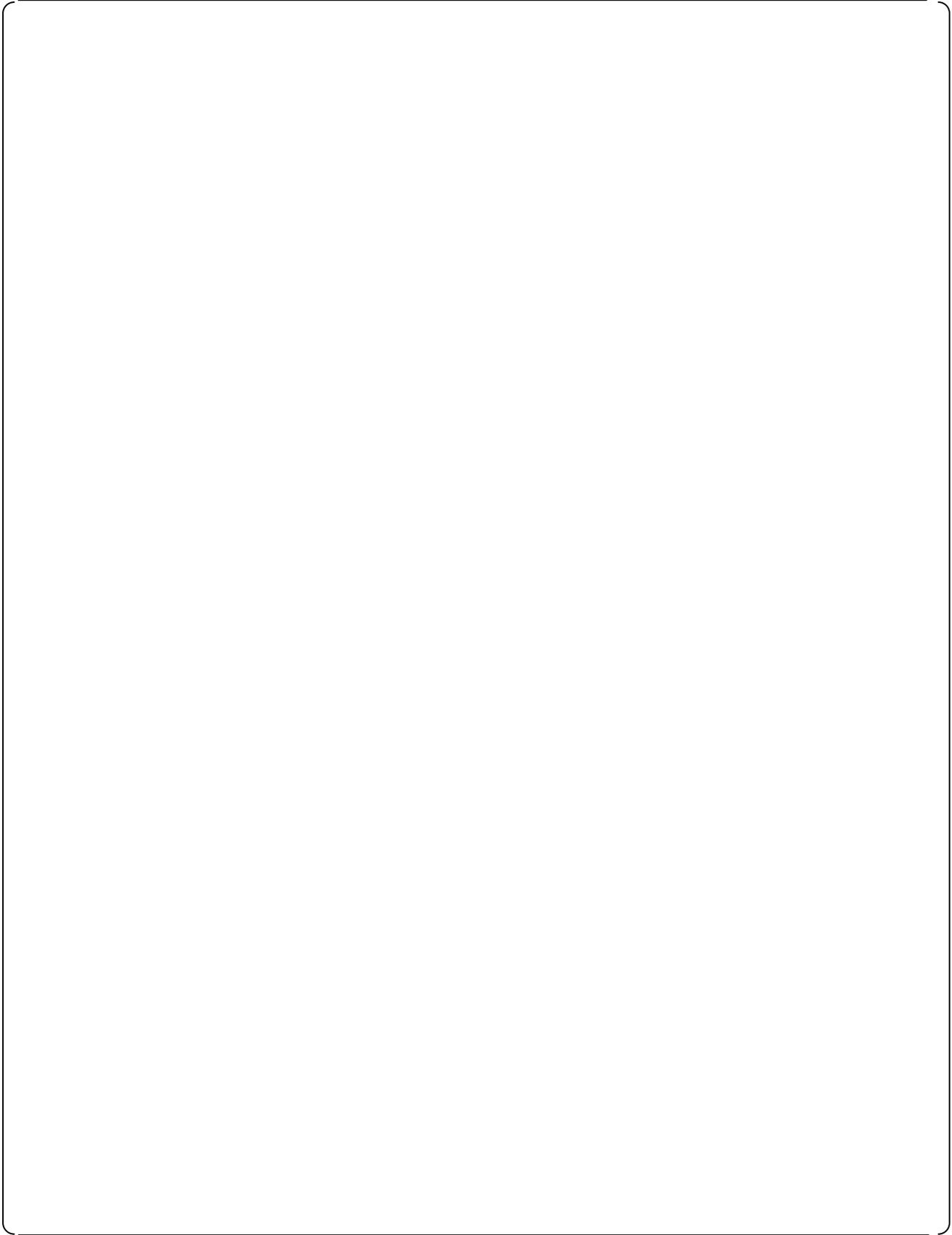


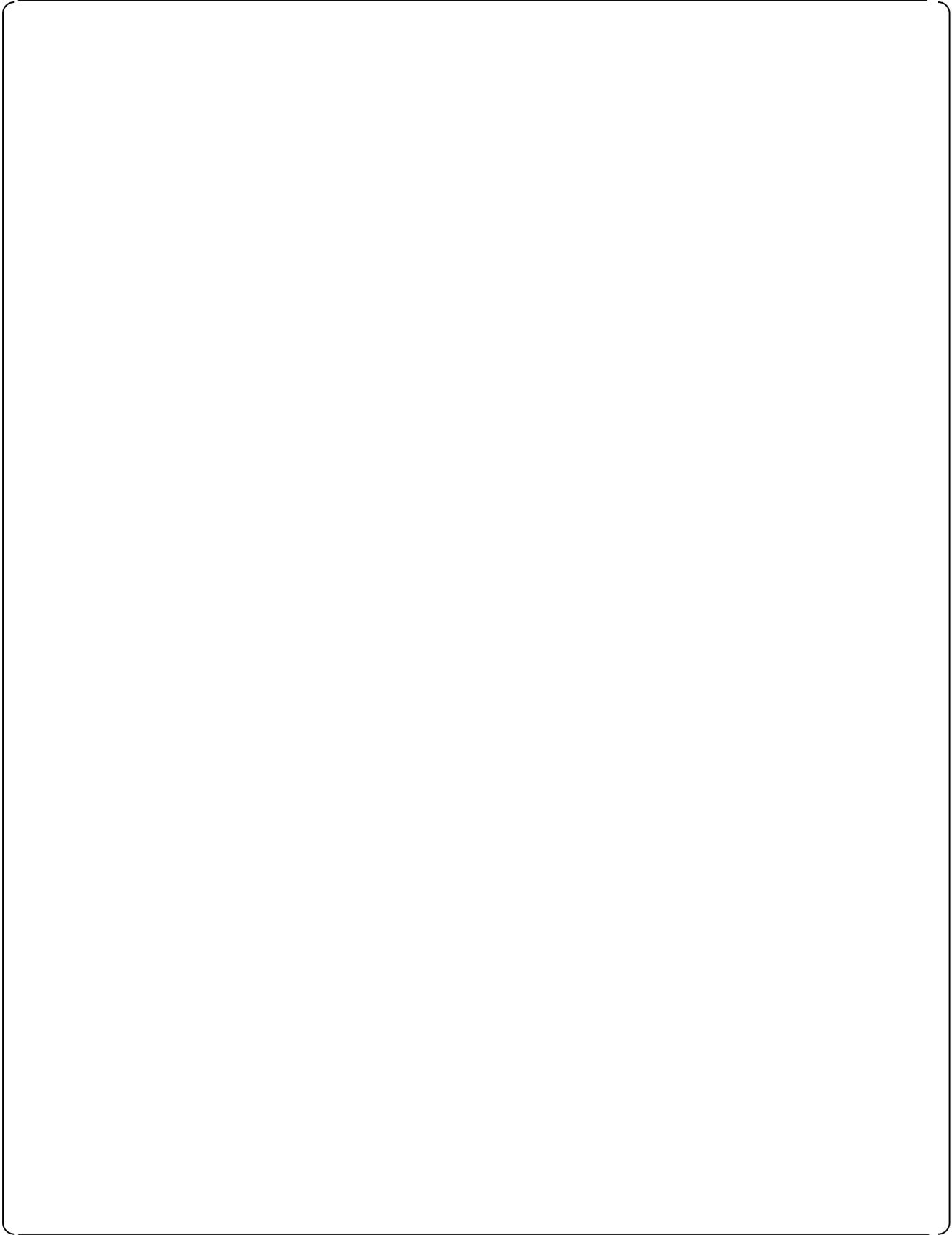


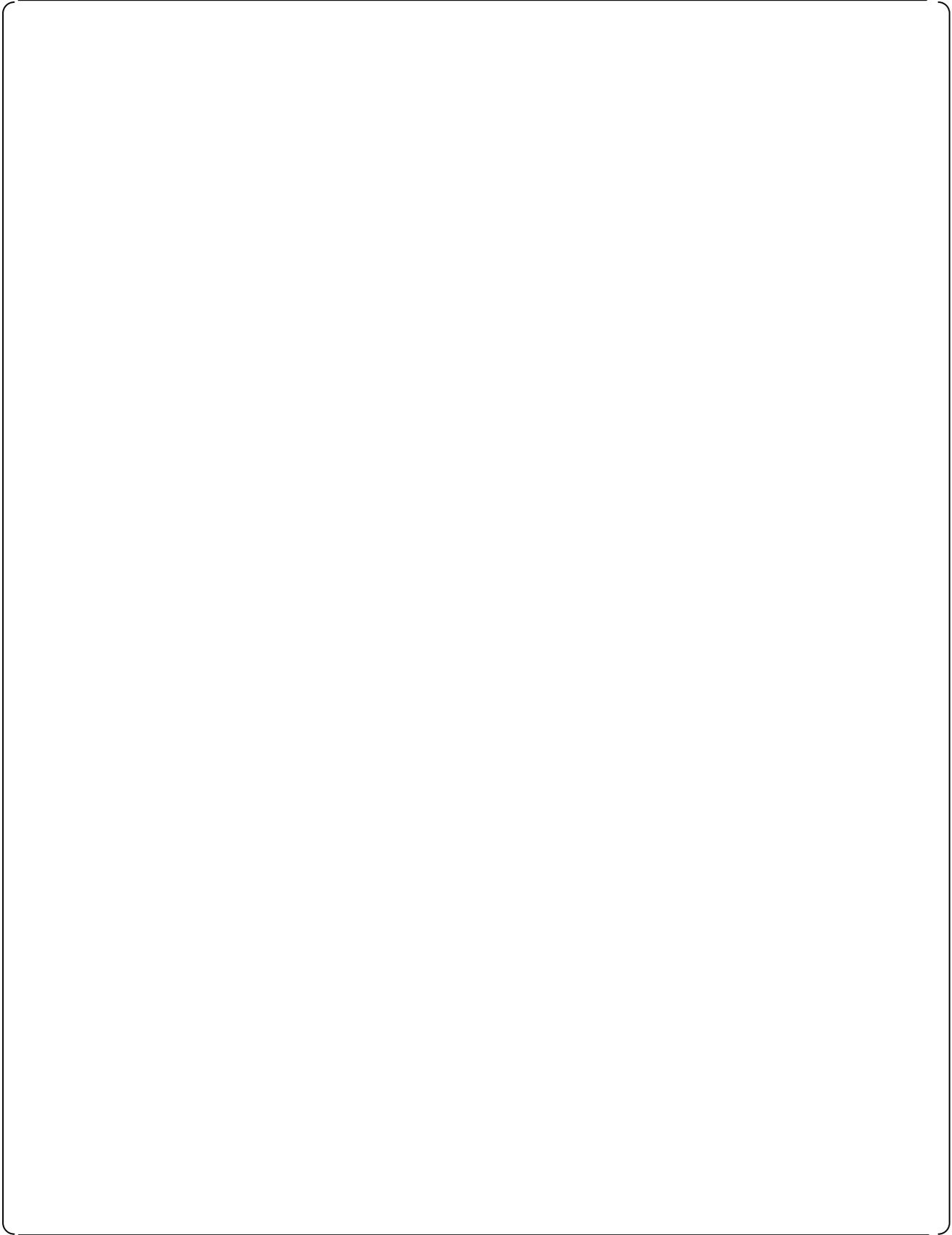


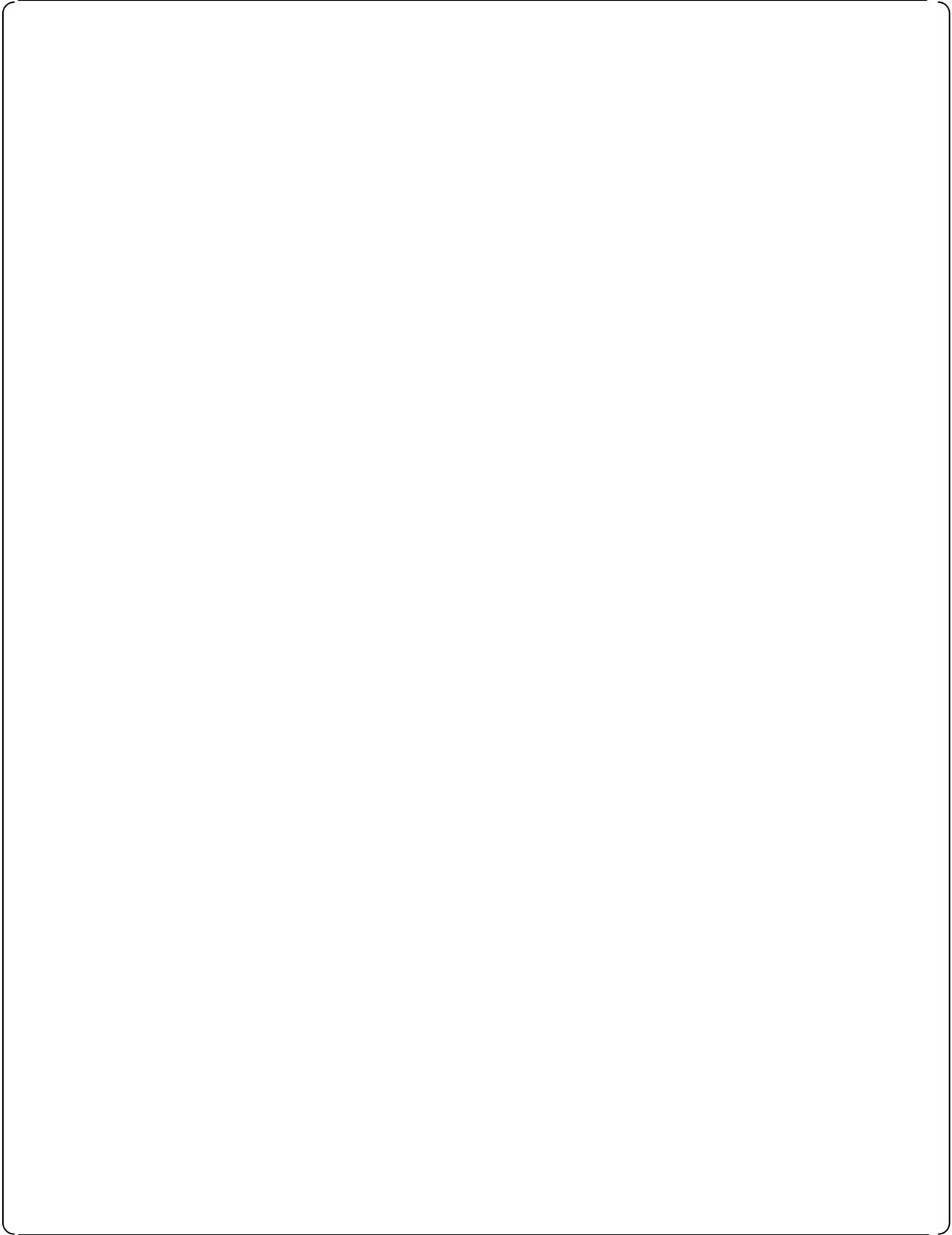


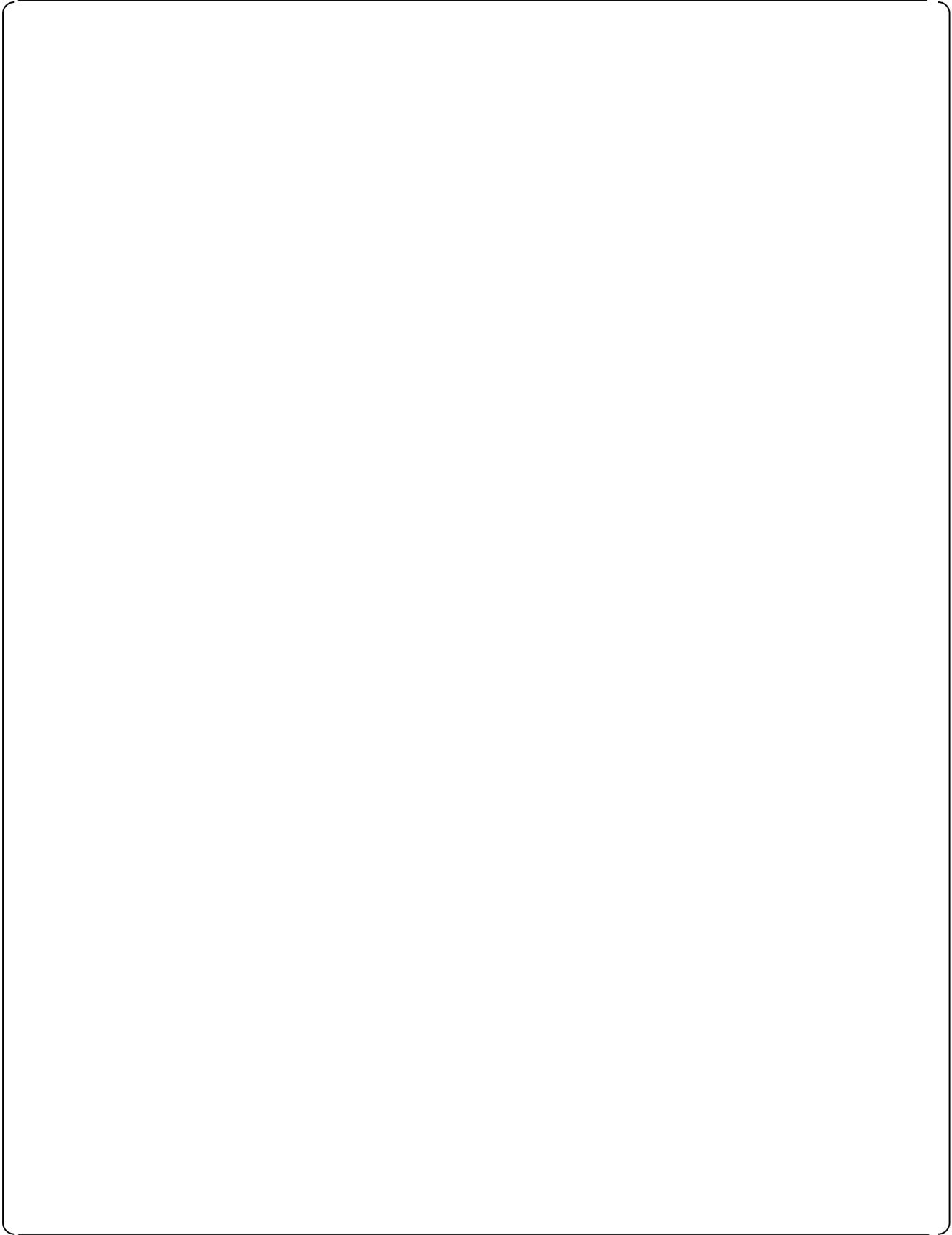


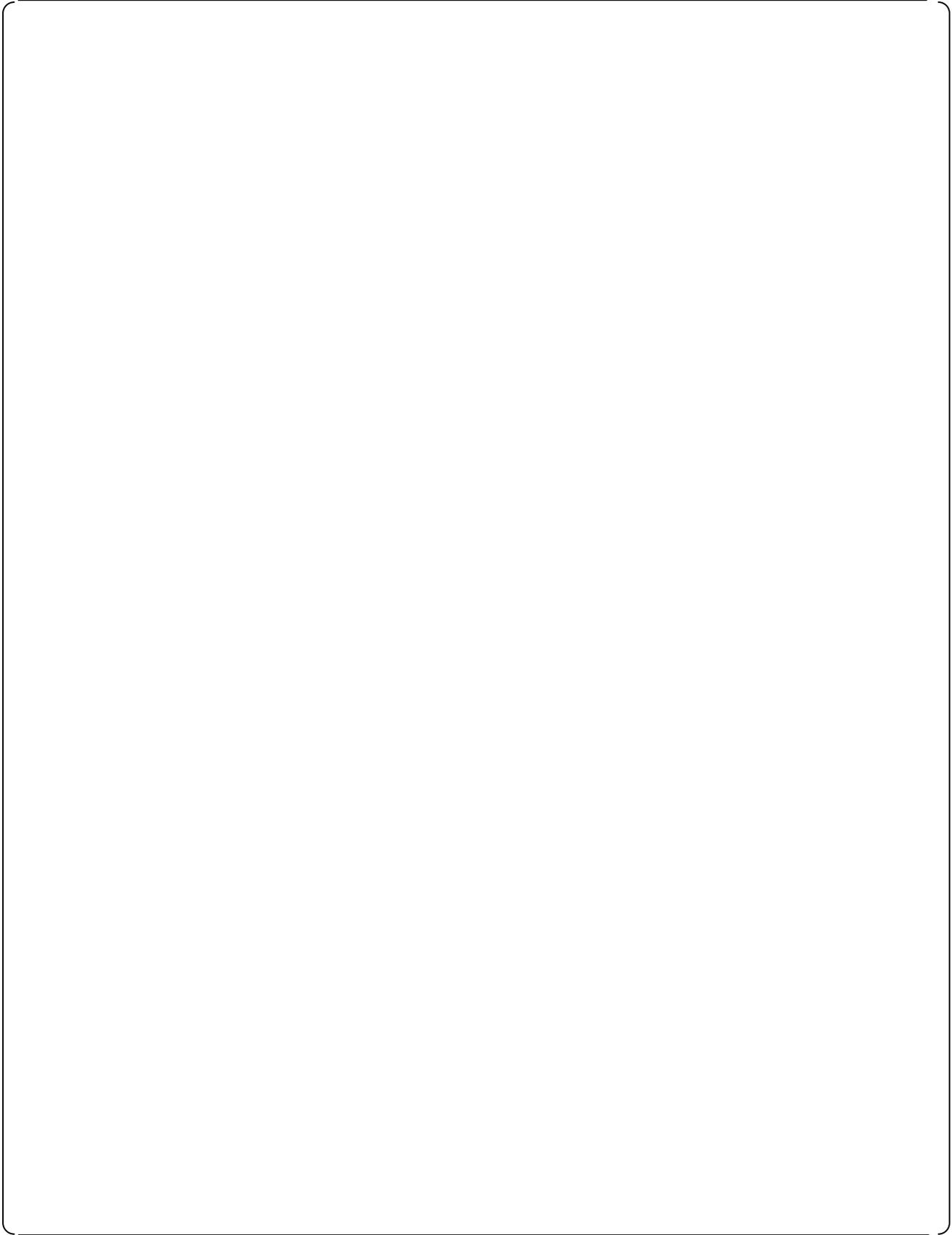












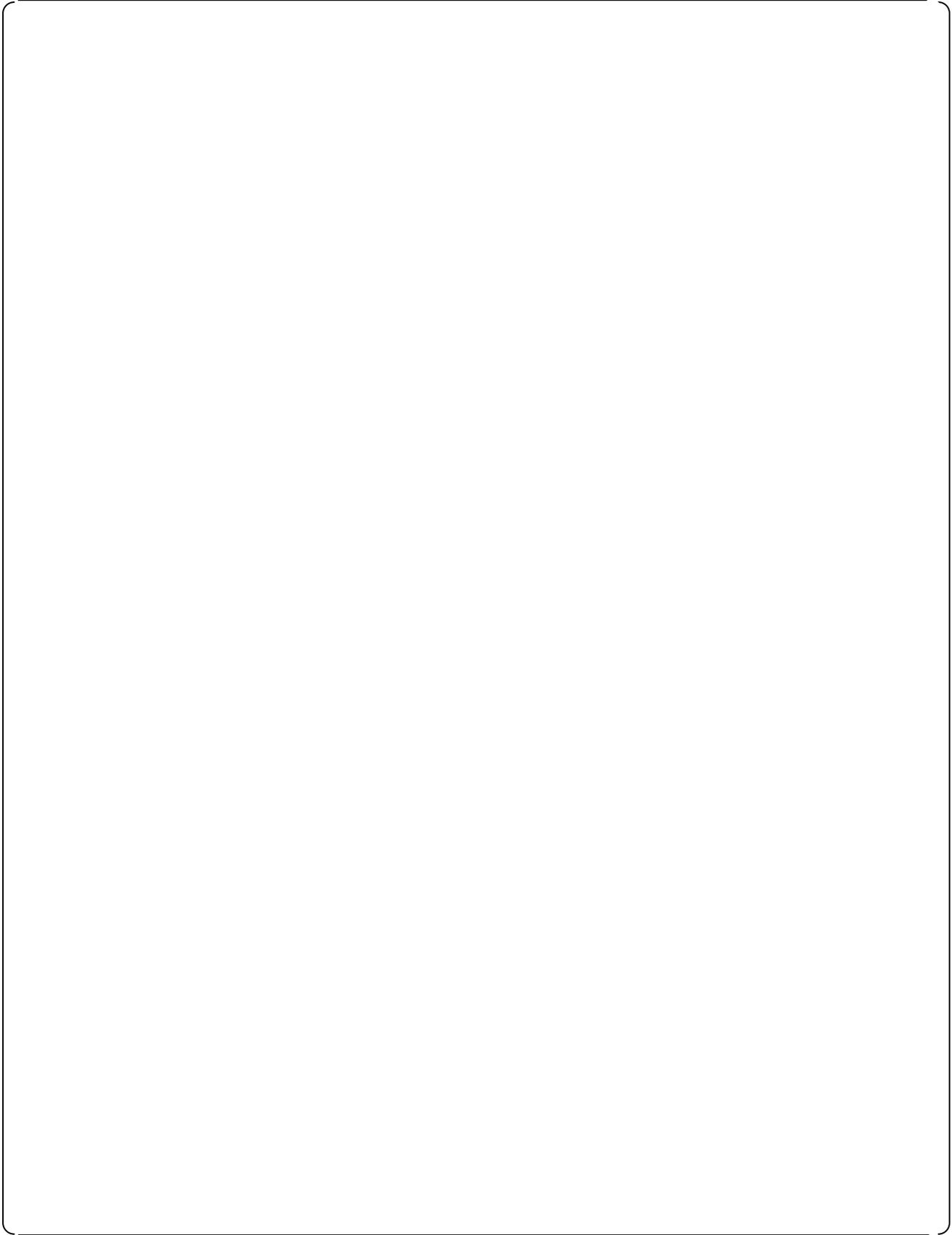


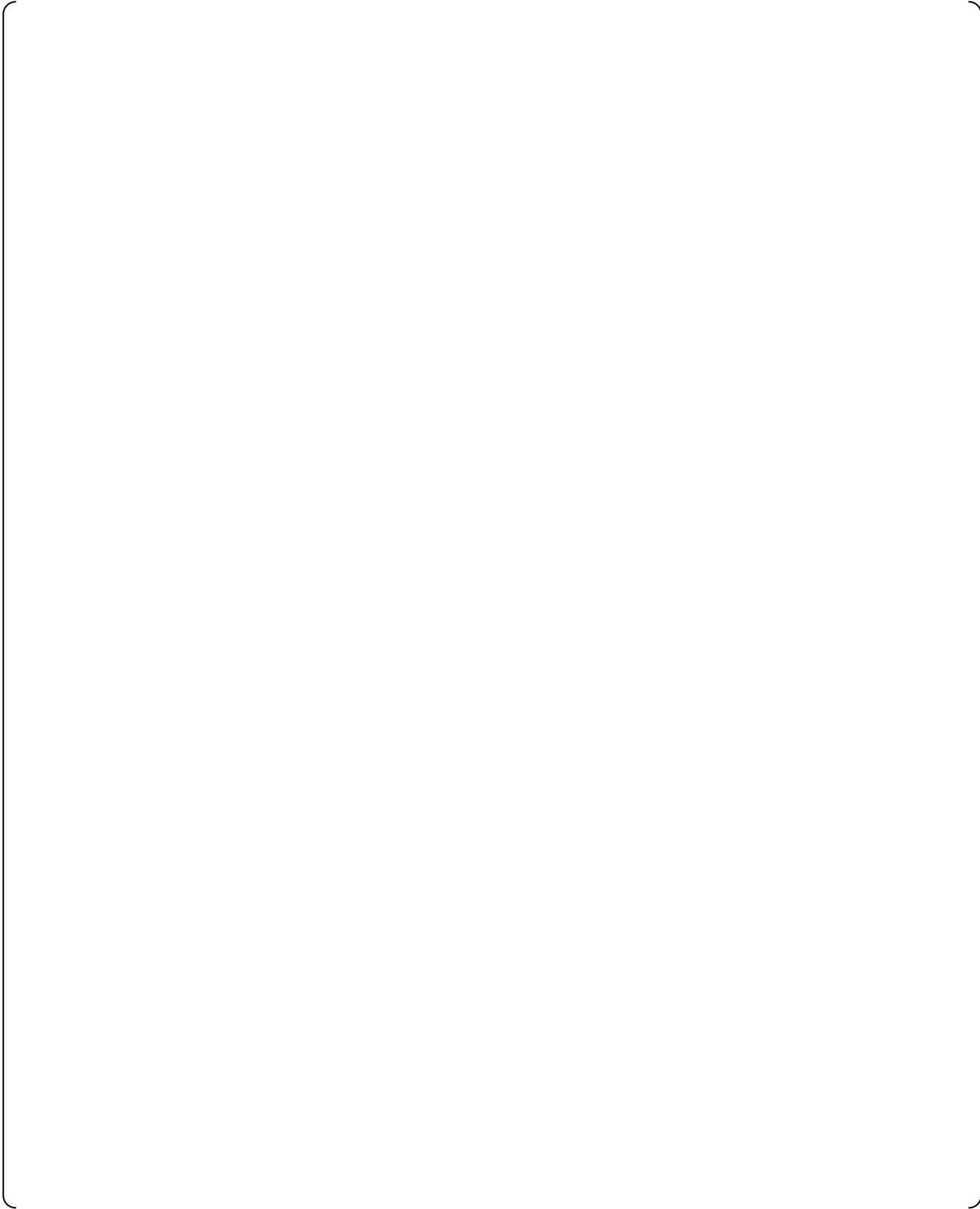


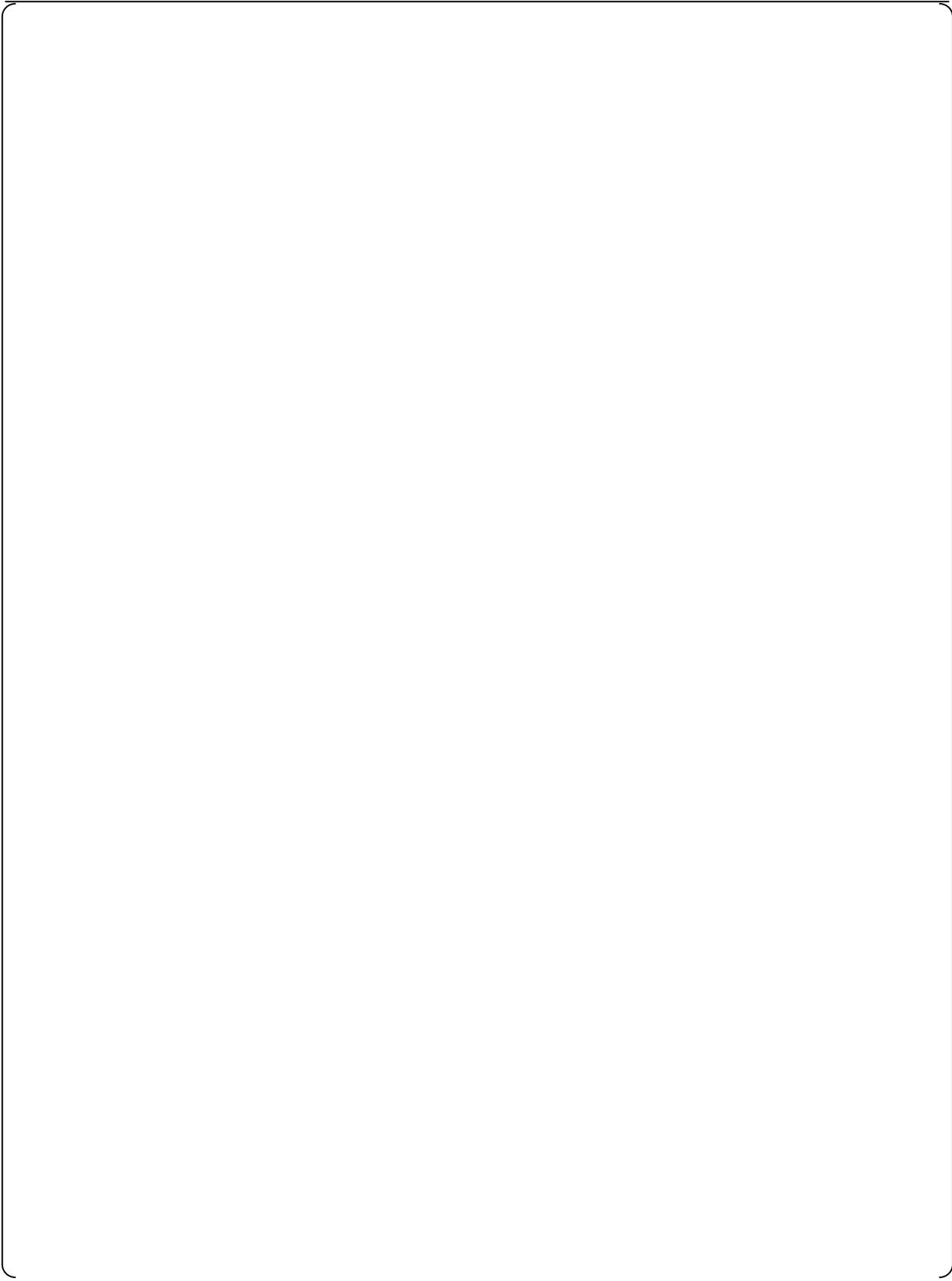
Figure E-1 Component Control Signal Interface from Operational VDU to Safety-Related System

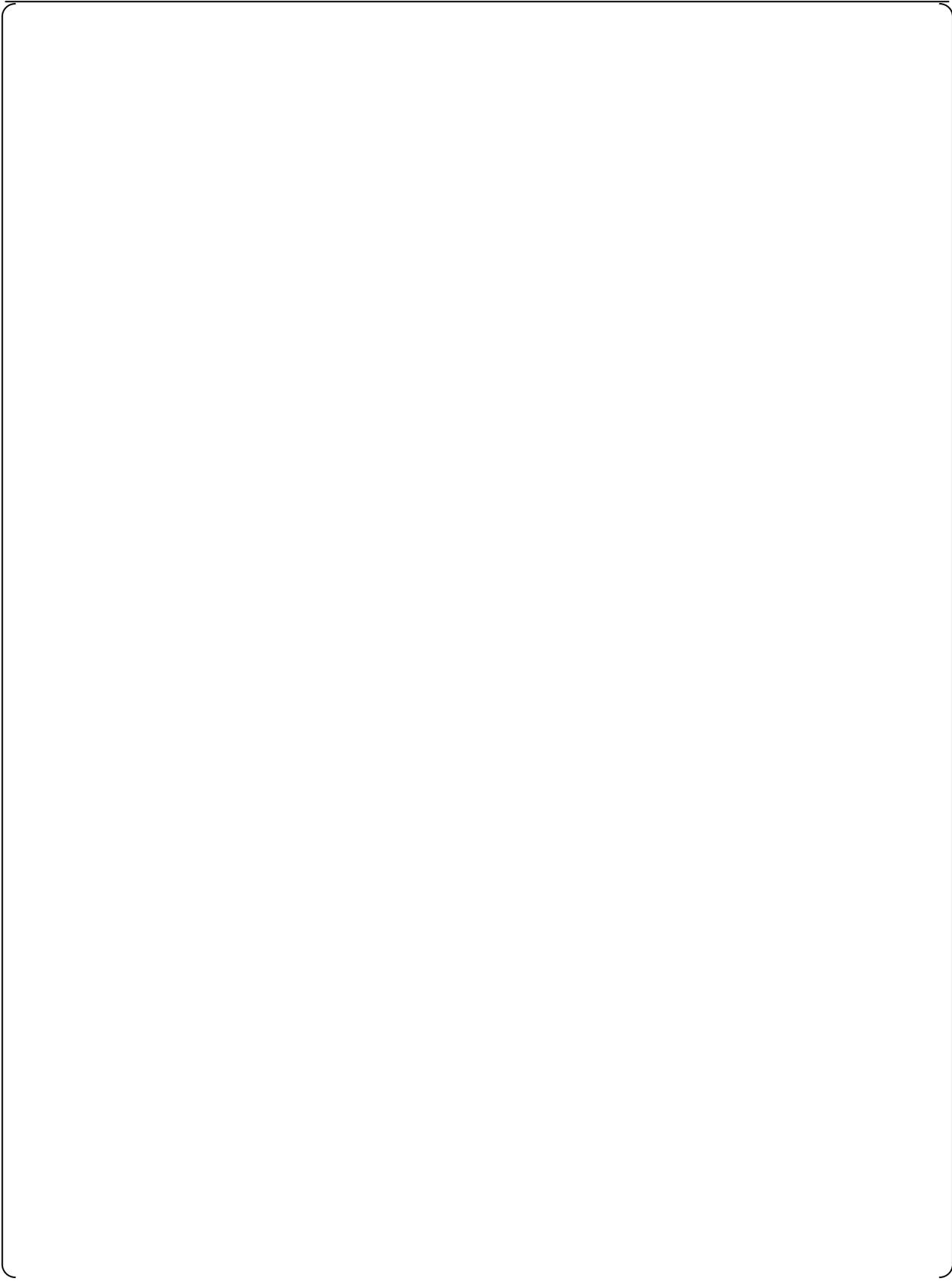


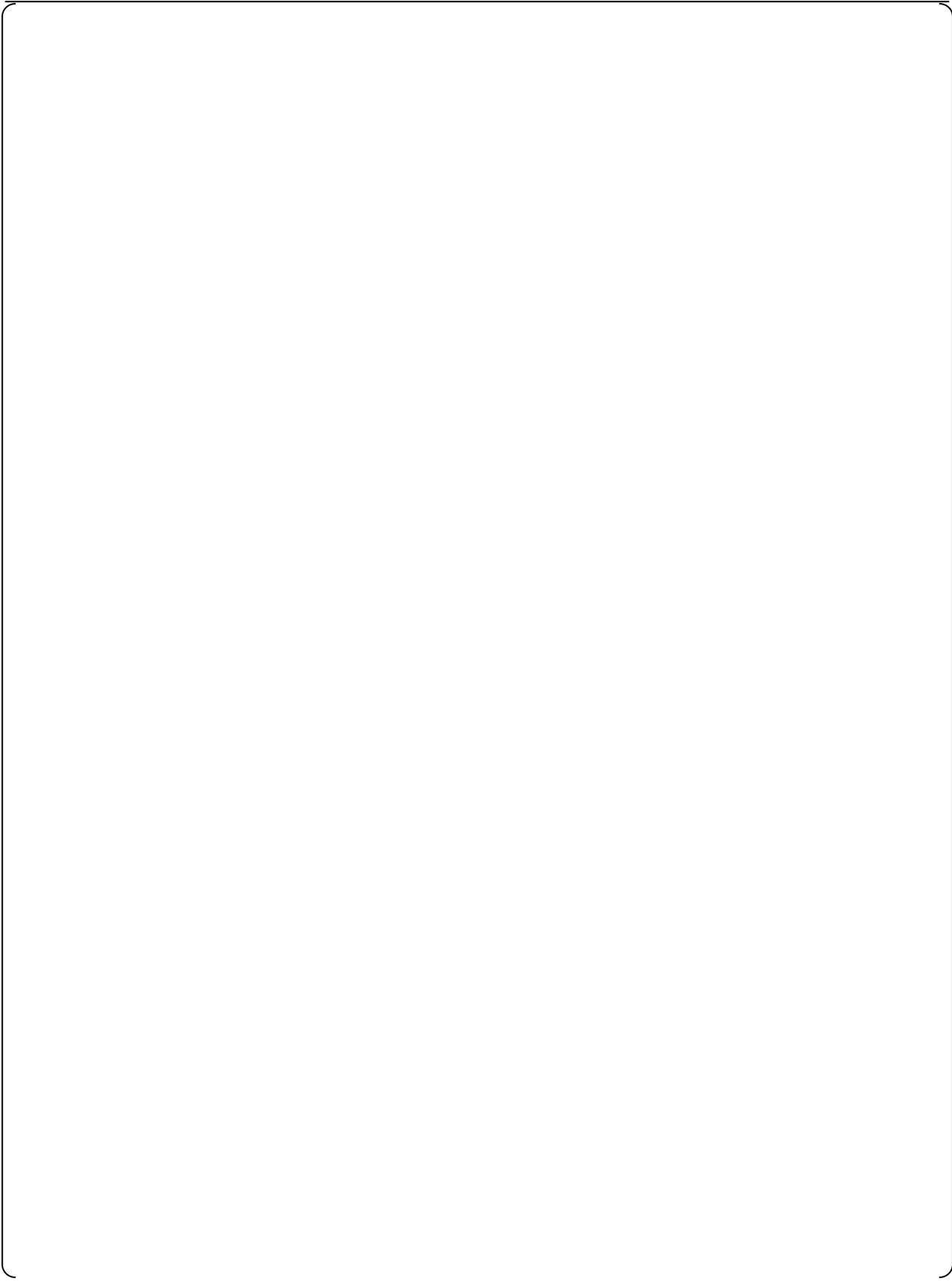
Figure E-2 Operational/Maintenance Bypass, Reset and Lock Signal Interface from Operational VDU to Safety-Related System

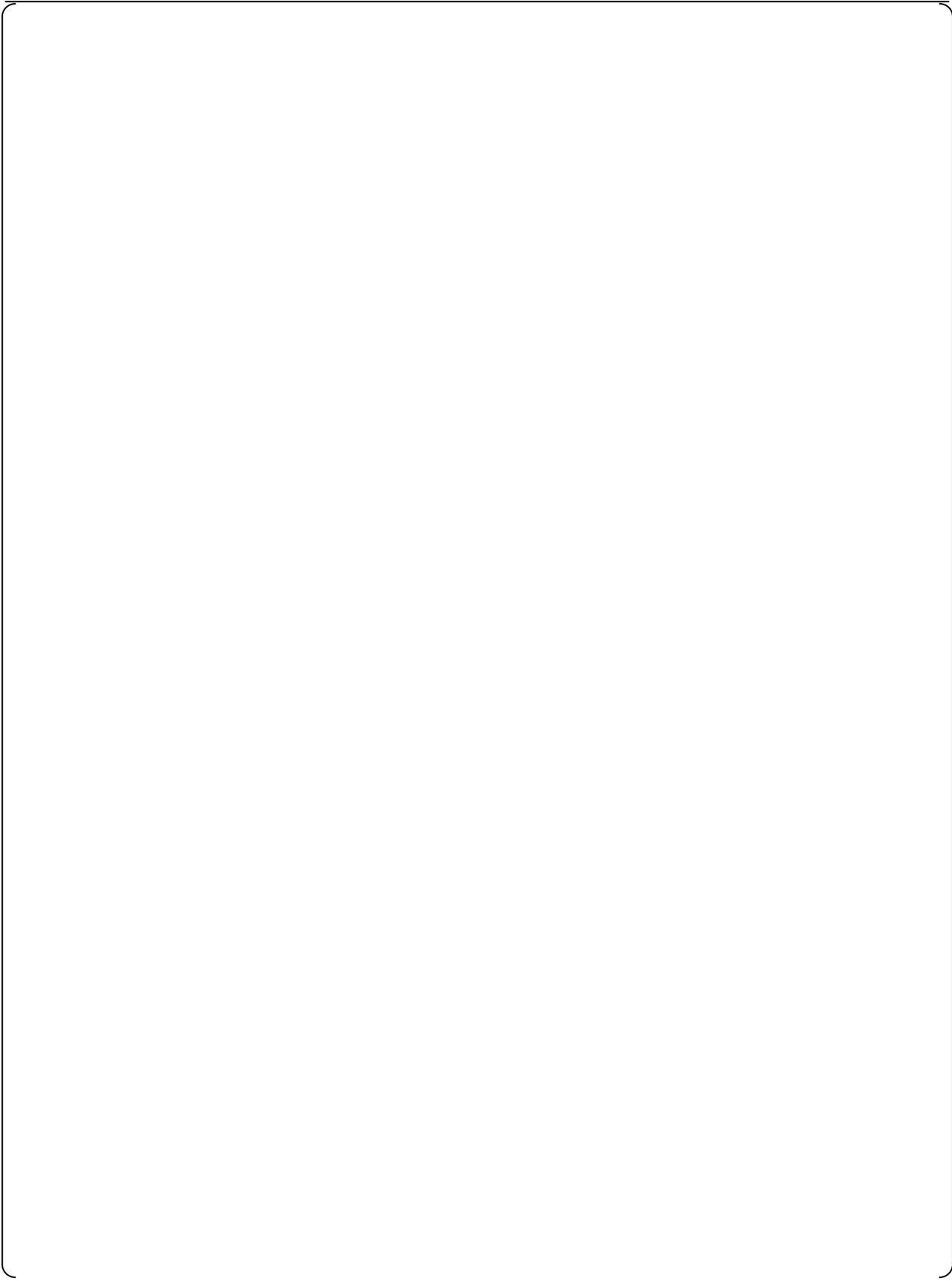
Appendix F Safety-related Digital I&C Design Detail Conformance to Essential Safety Criteria

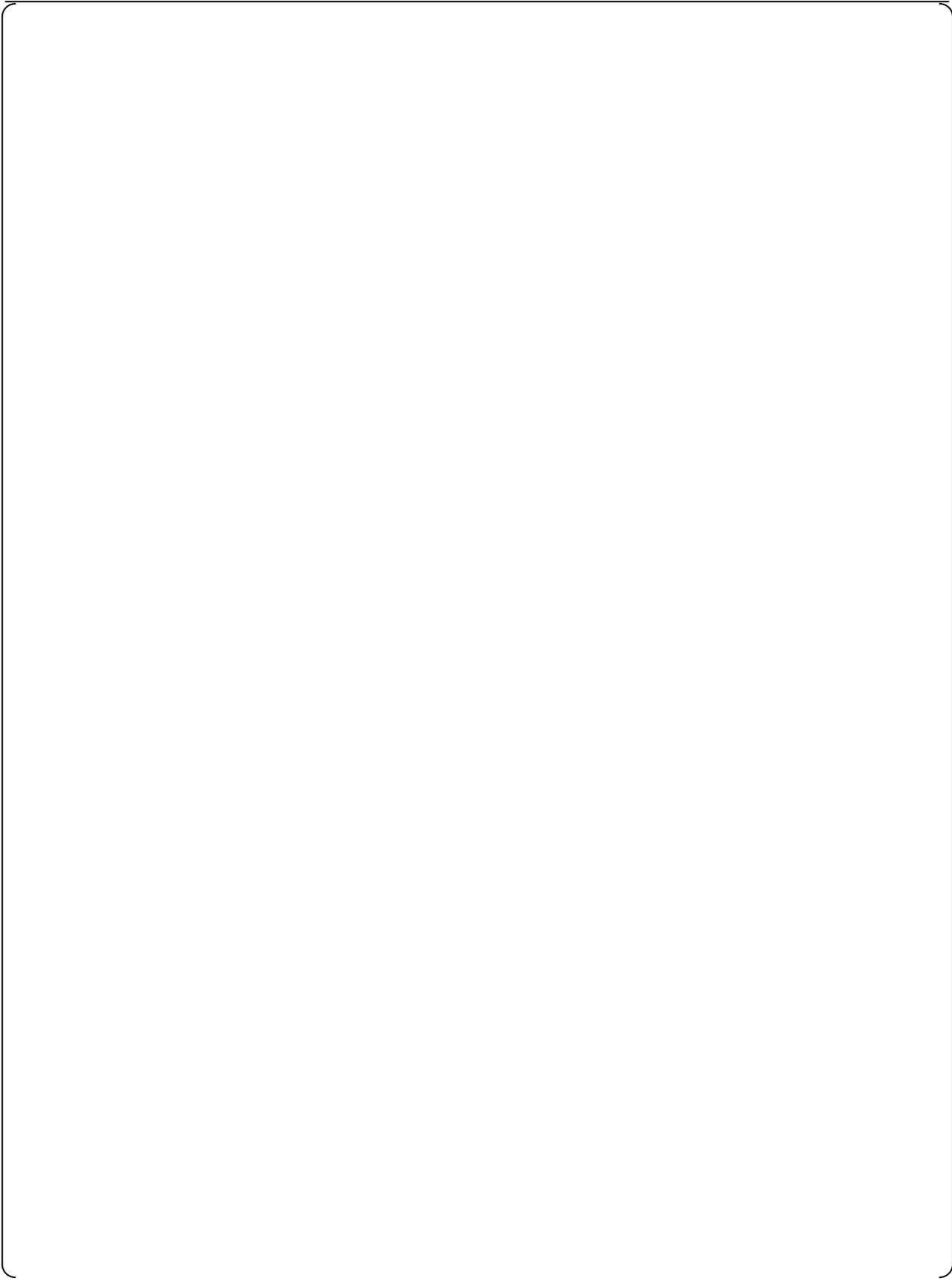












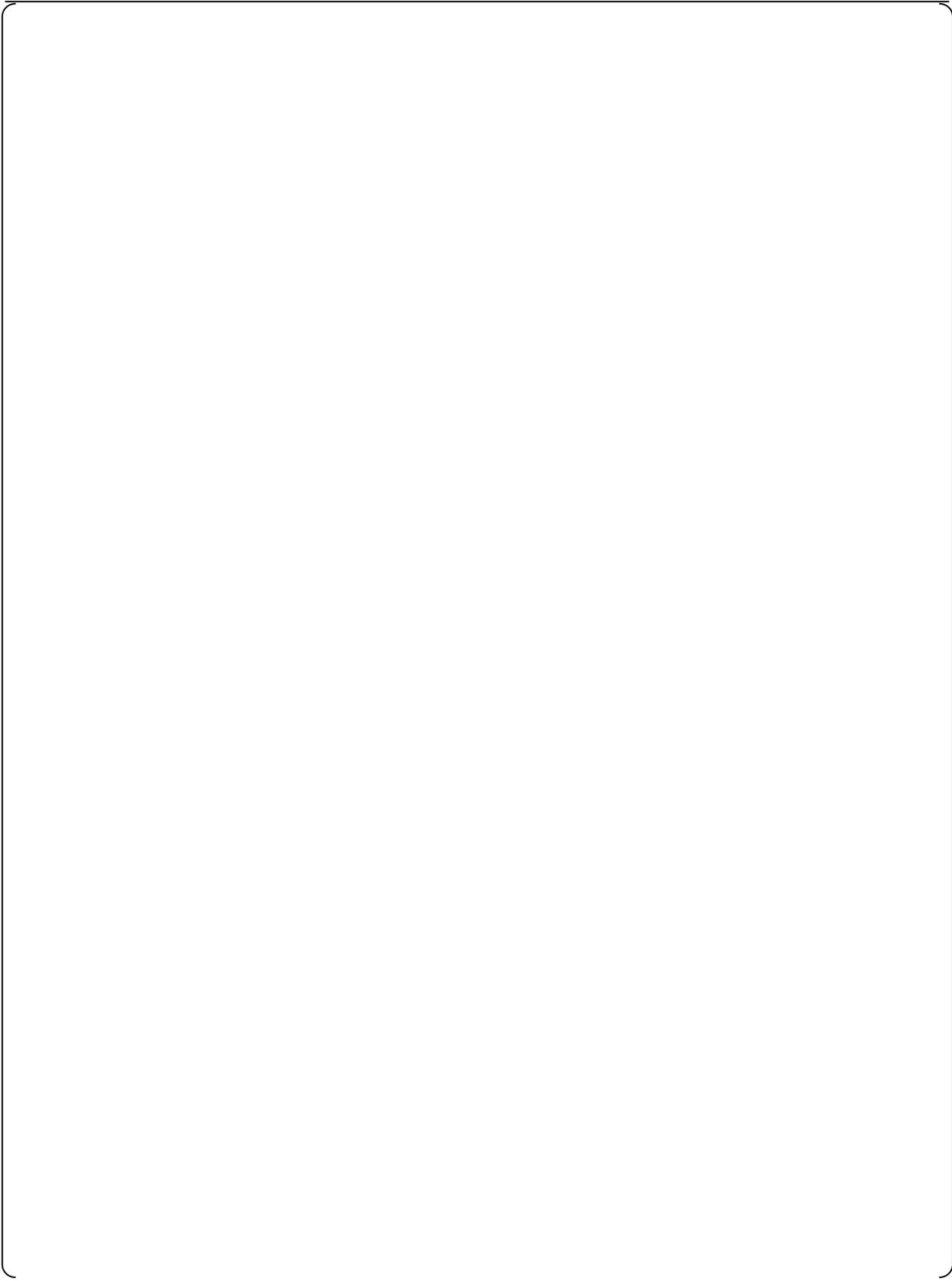


Figure F.1-1 Independence Design of RPS

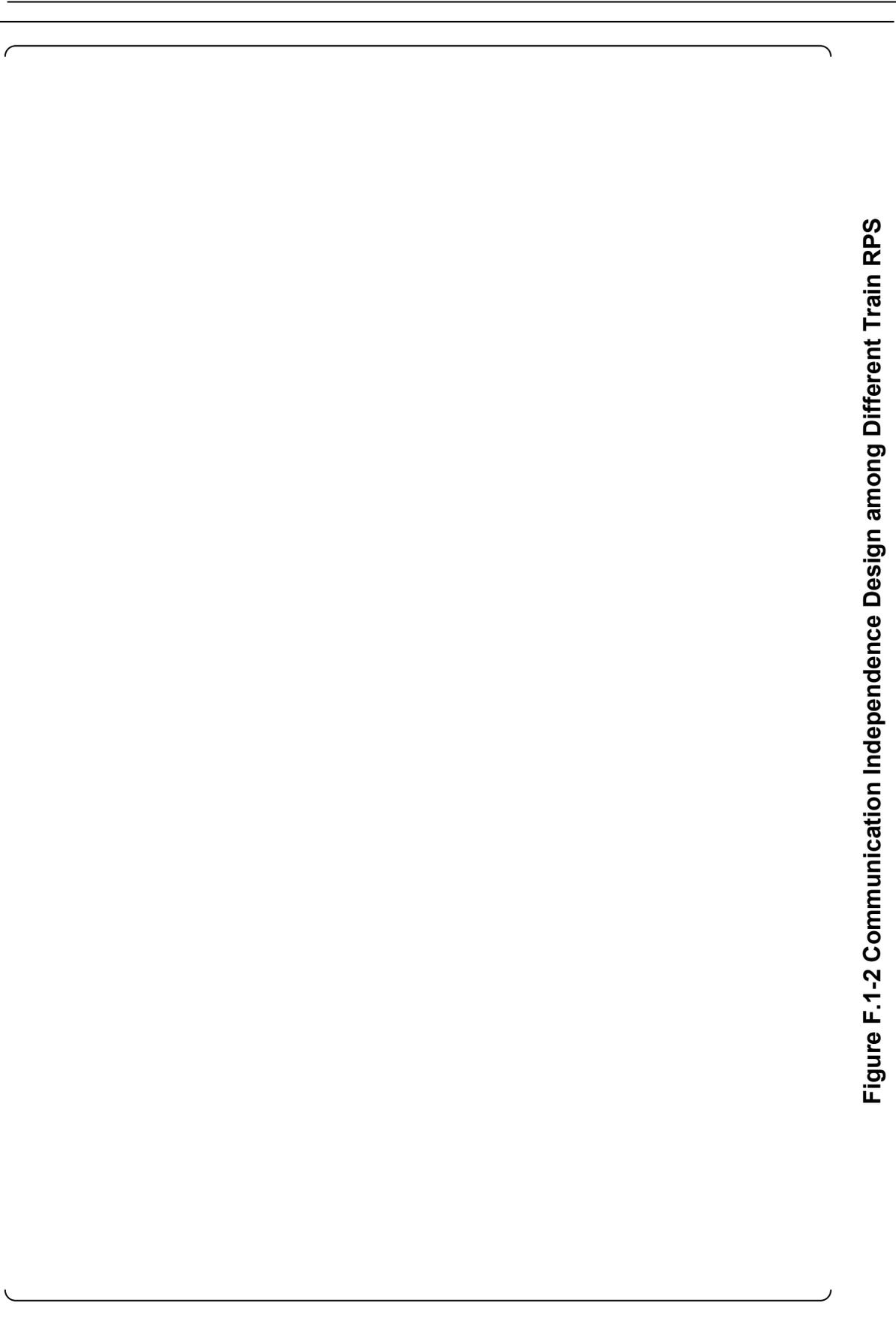


Figure F.1-2 Communication Independence Design among Different Train RPS

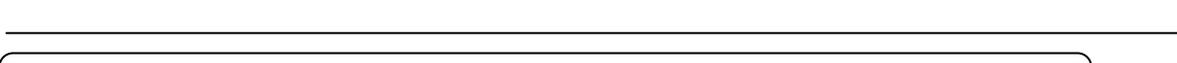
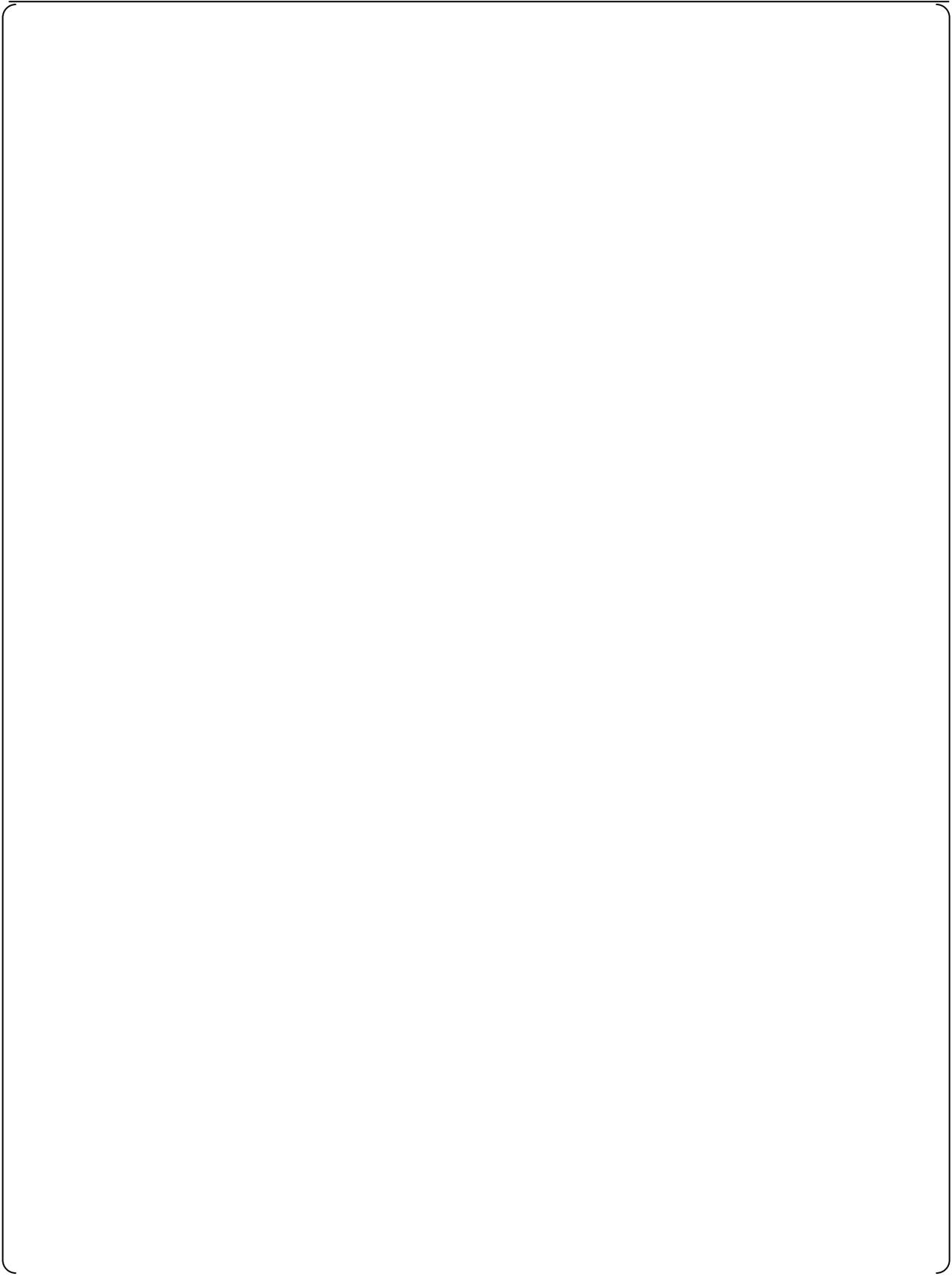


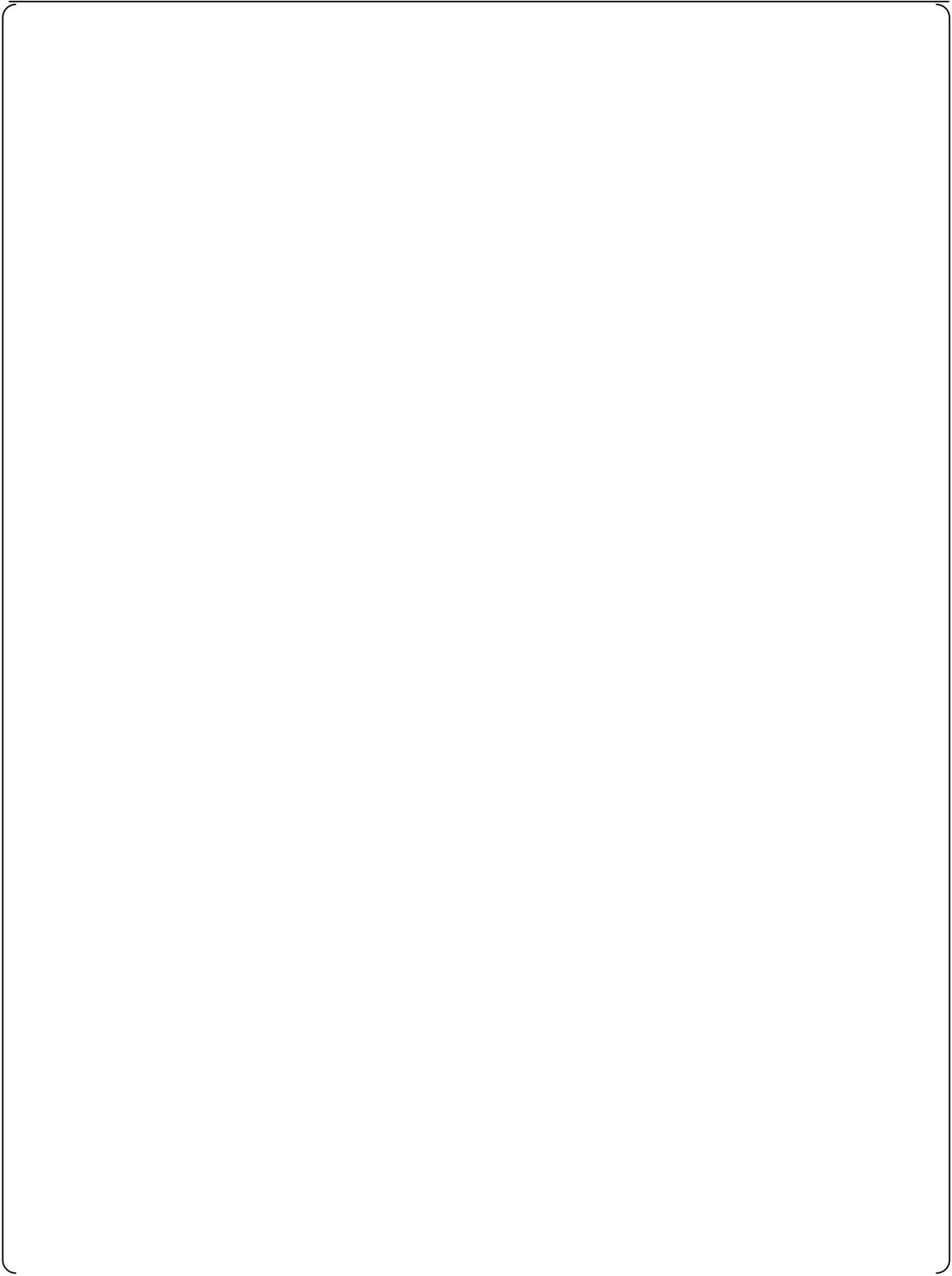
Figure F.1-3 Communication Independence Design from RPS to Unit Bus

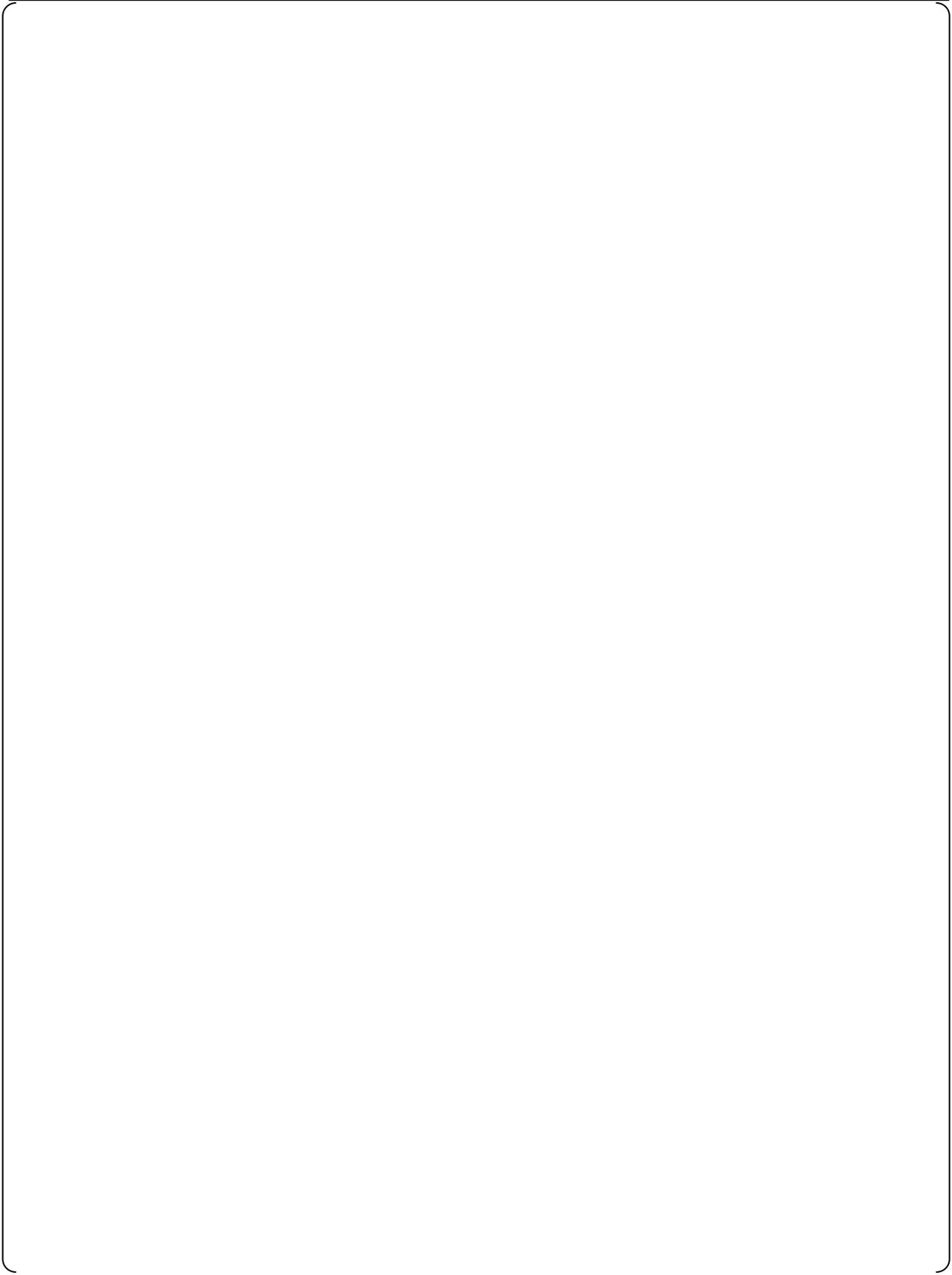


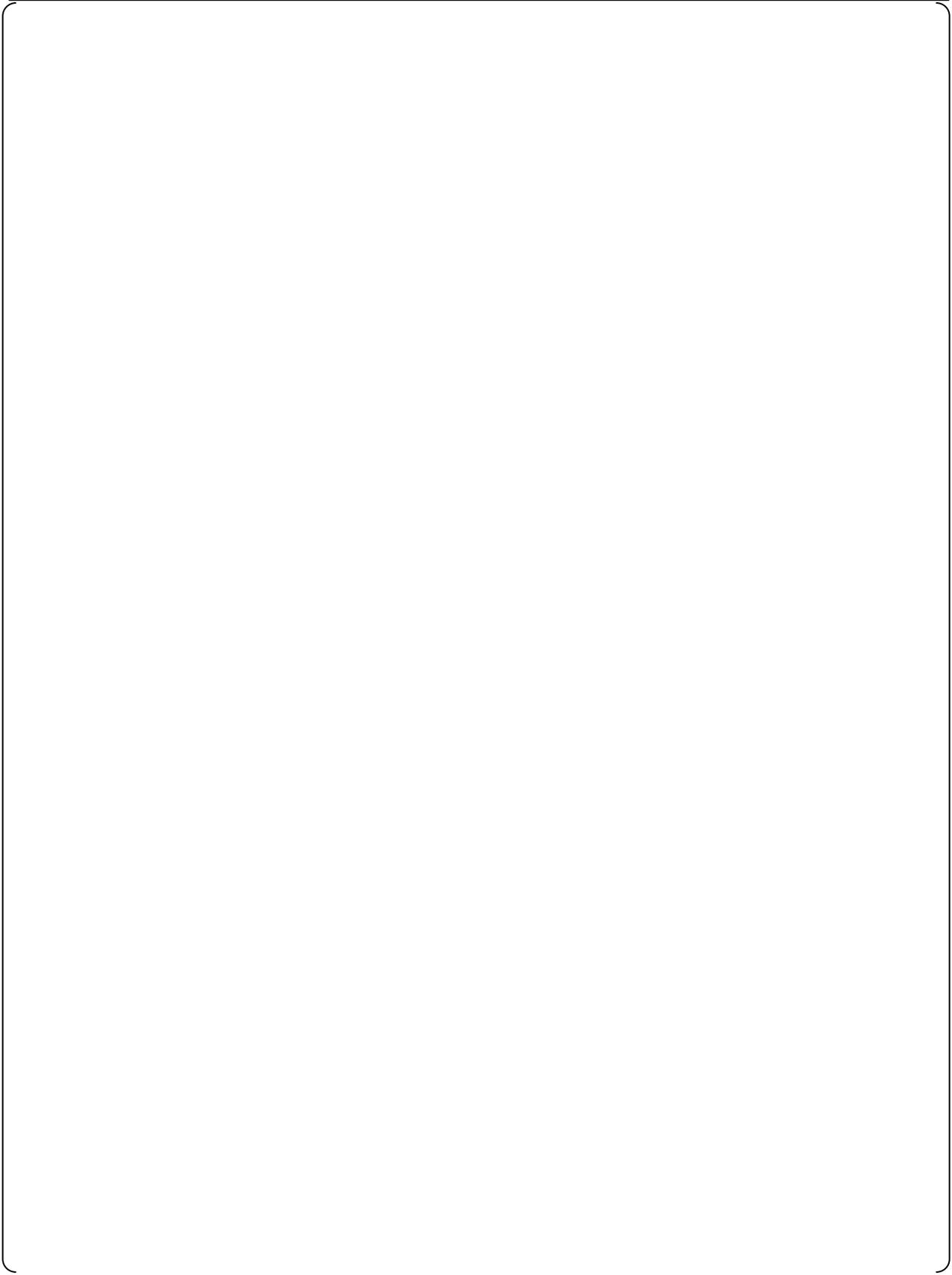
Figure F.1.4 Overall Signal Interfaces of 2-out-of-4 Bypass Logic

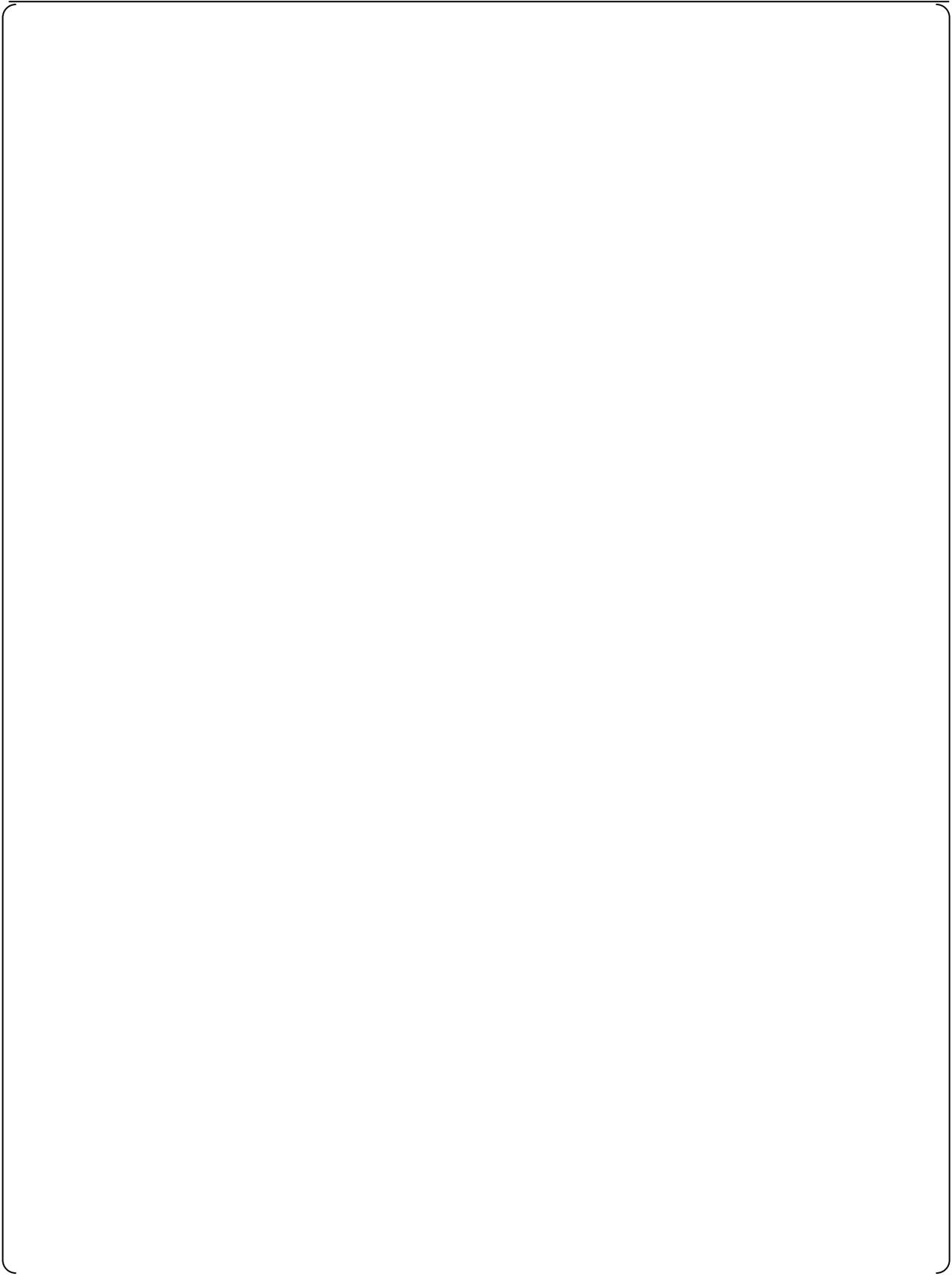
Figure F.1-5 MELTAC Platform Basic Software Processes and Execution Order

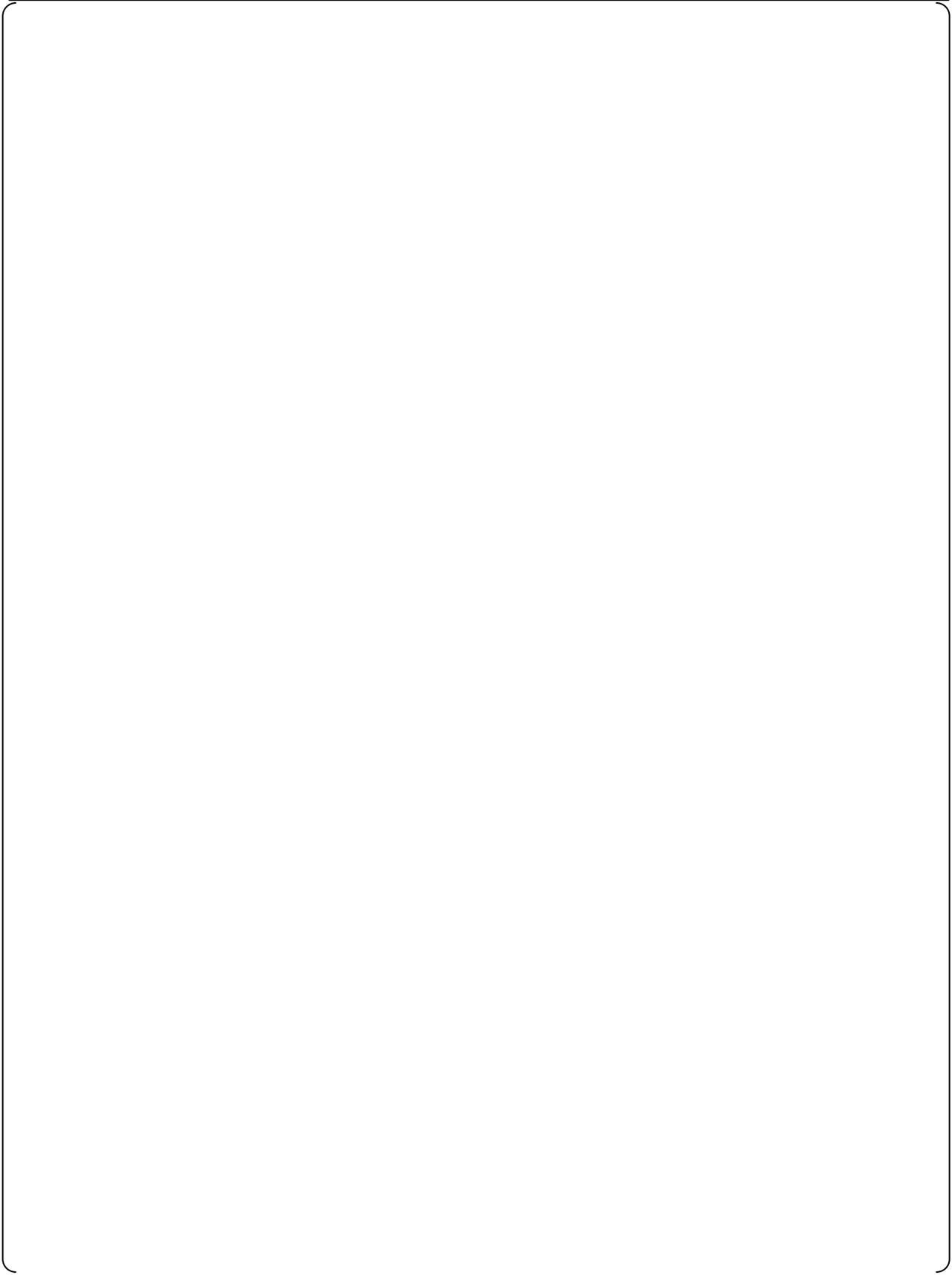


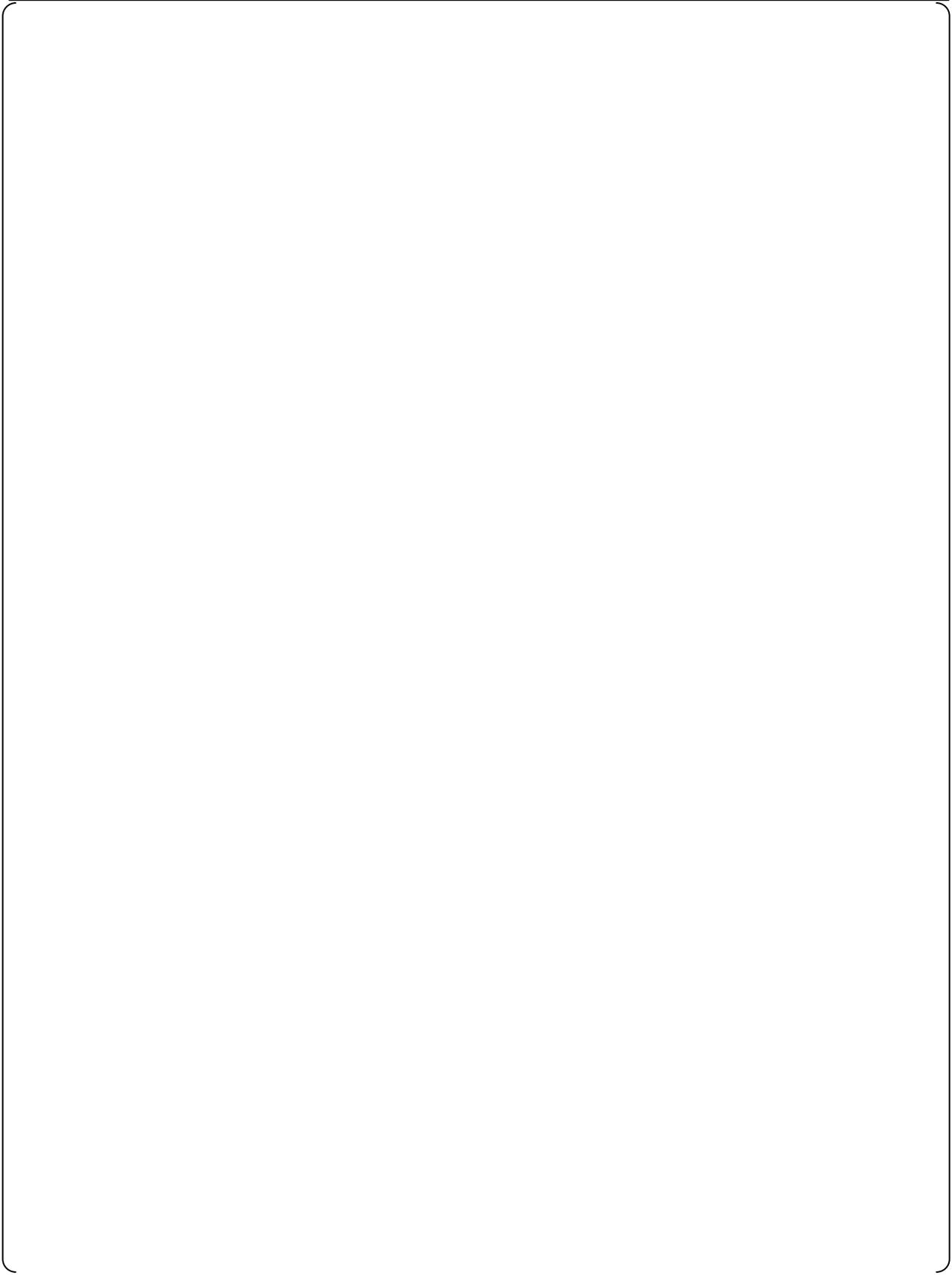


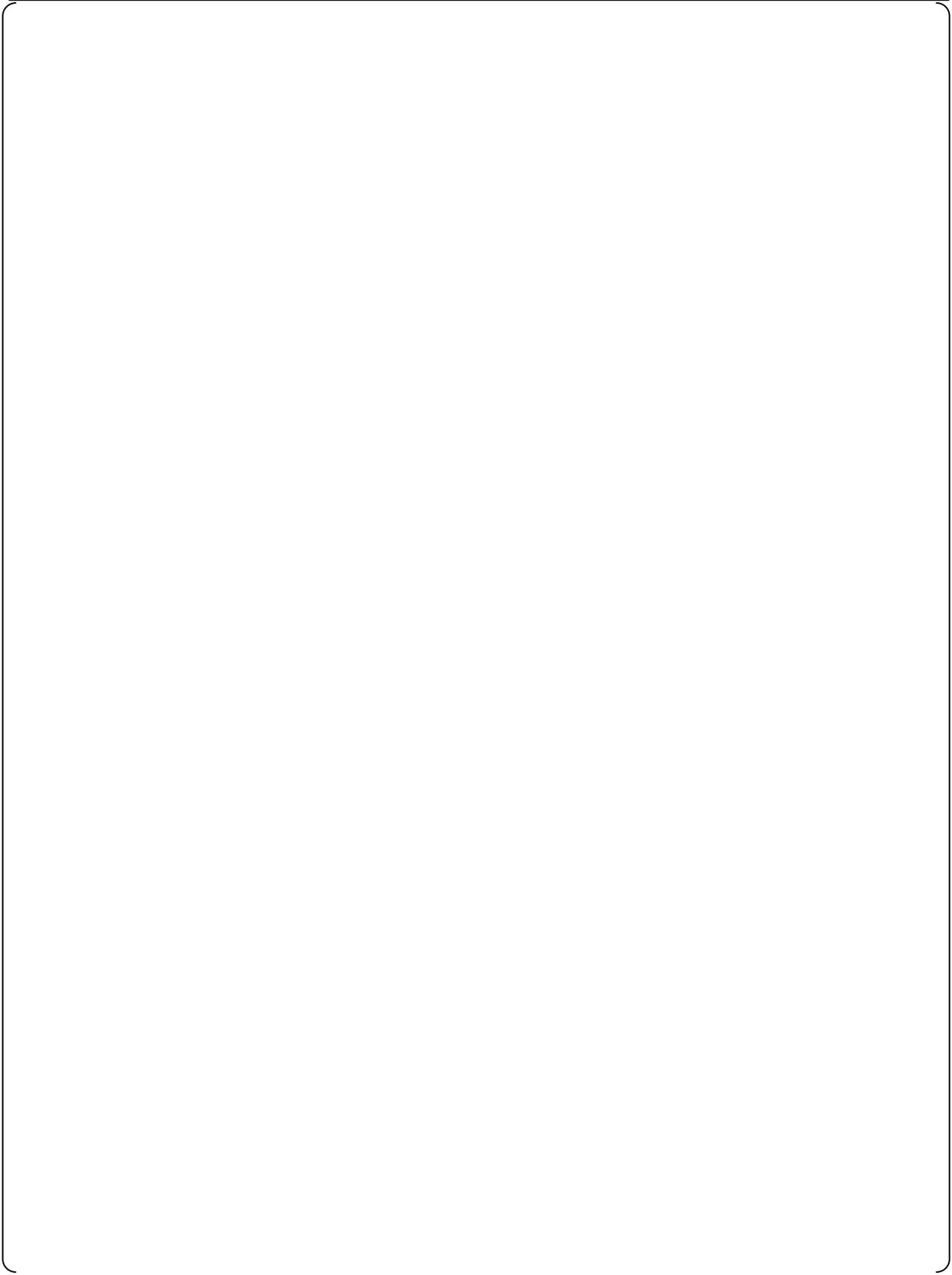












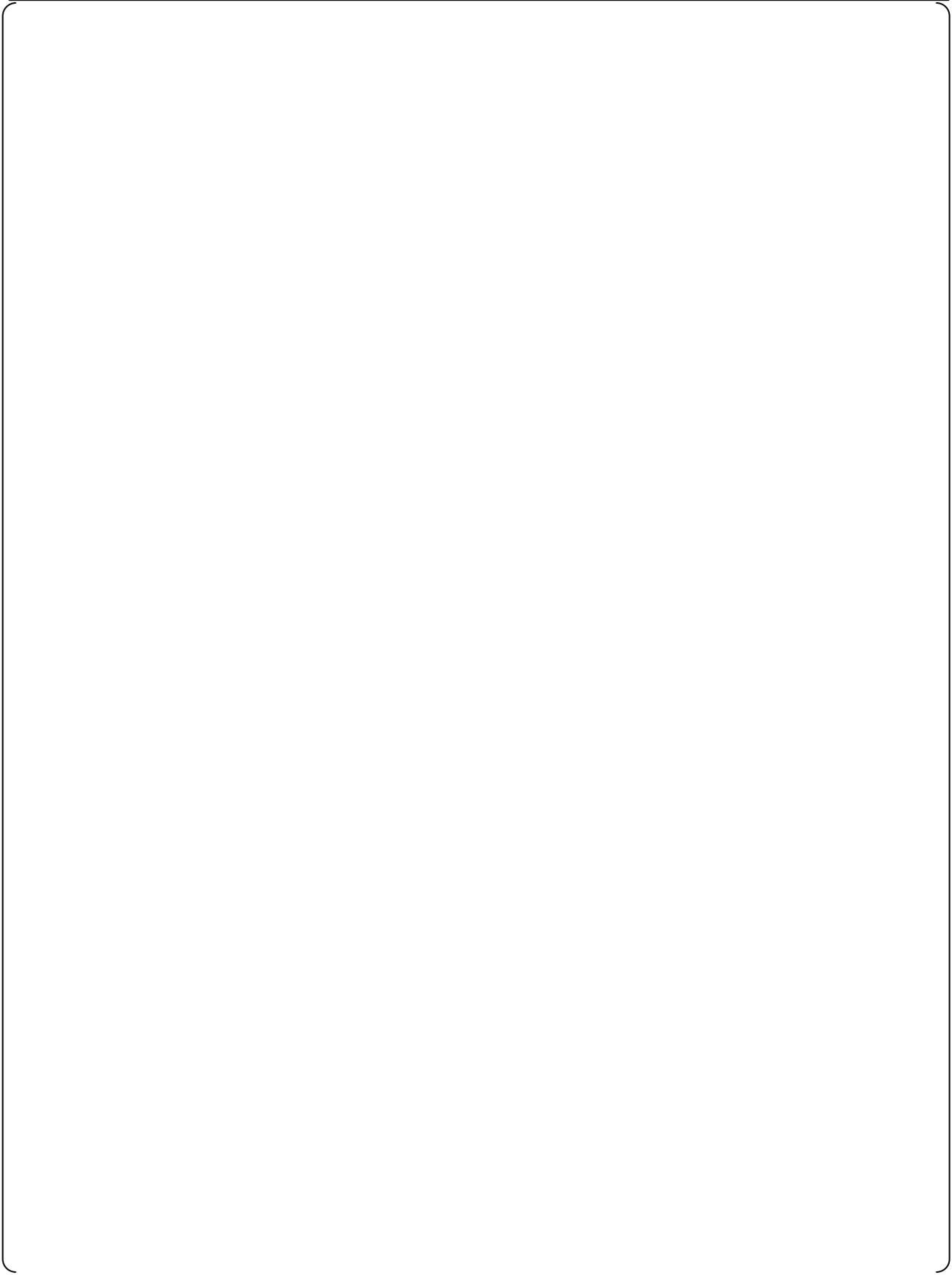


Figure F.2-1 Independence Design of ESFAS

Figure F.2-2 Independence Design of SLS

Figure F.2-3 Independence Design of COM



Figure F.2-4 Independence Design of Safety VDU



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

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

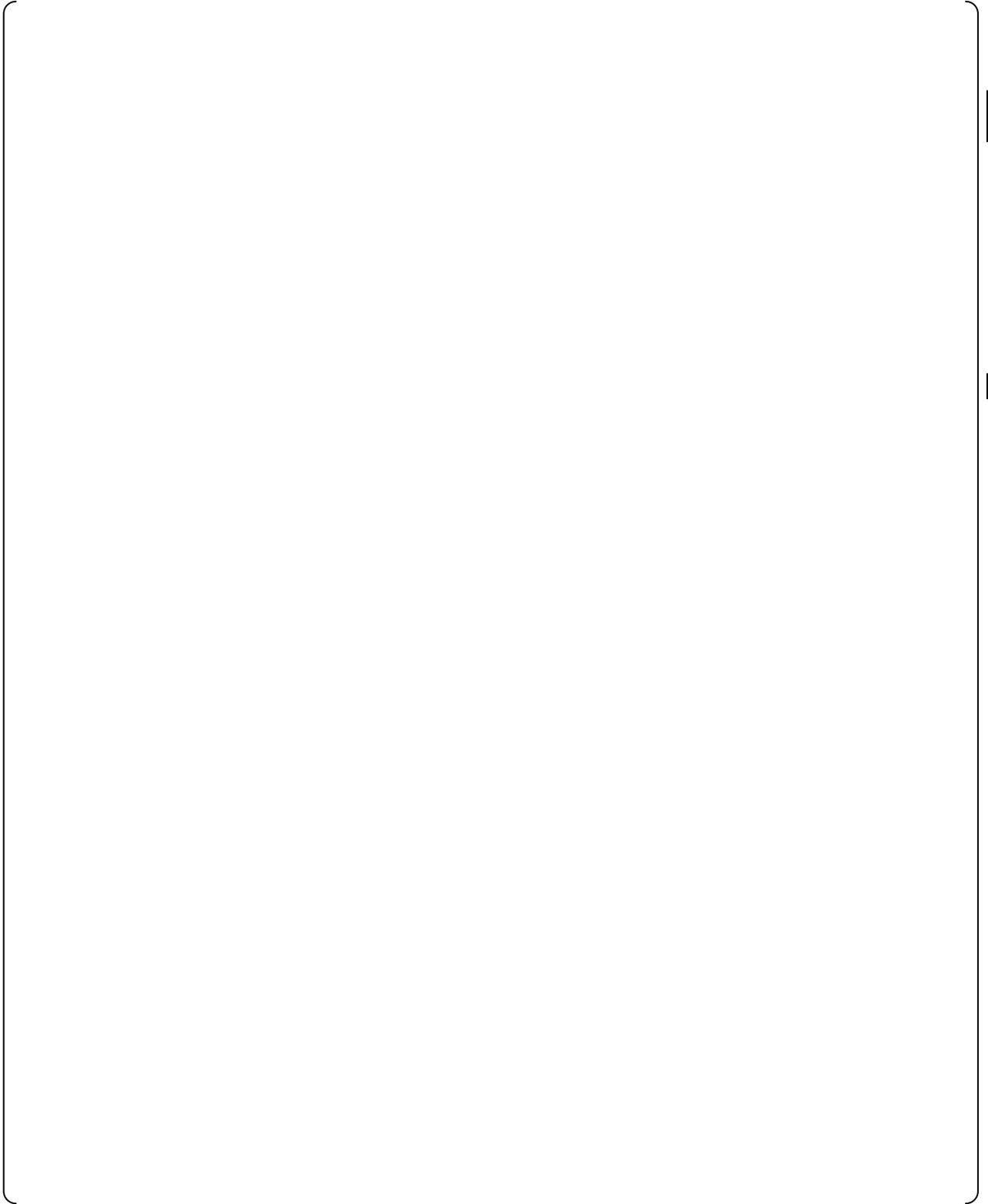
Figure F.2-7 Communication Independence Design from Unit Bus to COM-2

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

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

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

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





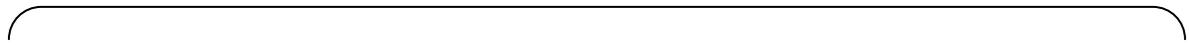


Figure G.1-1 System Configuration for FMEA of RT and ESF Actuation in PSMS

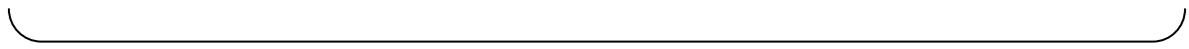


Table G.2-1 FMEA for RT in PSMS (for Figure G1-1)
(Sheet 1 of 9)

Table G.2-1 FMEA for RT in PSMS (for Figure G1-1)
(Sheet 2 of 9)

Table G.2-1 FMEA for RT in PSMS (for Figure G1-1)
(Sheet 3 of 9)

Table G.2-1 FMEA for RT in PSMS (for Figure G1-1)
(Sheet 4 of 9)

Table G.2-1 FMEA for RT in PSMS (for Figure G1-1)
(Sheet 5 of 9)

Table G.2-1 FMEA for RT in PSMS (for Figure G1-1)
(Sheet 6 of 9)

Table G.2-1 FMEA for RT in PSMS (for Figure G1-1)
(Sheet 7 of 9)

Table G.2-1 FMEA for RT in PSMS (for Figure G1-1)
(Sheet 8 of 9)

Table G.2-1 FMEA for RT in PSMS (for Figure G1-1)
(Sheet 9 of 9)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G1-1)
(Sheet 1 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G1-1)
(Sheet 2 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G1-1)
(Sheet 3 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G1-1)
(Sheet 4 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G1-1)
(Sheet 5 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G1-1)
(Sheet 6 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G1-1)
(Sheet 7 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G1-1)
(Sheet 8 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G1-1)
(Sheet 9 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G1-1)
(Sheet 10 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G1-1)
(Sheet 11 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G1-1)
(Sheet 12 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G1-1)
(Sheet 13 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G1-1)
(Sheet 14 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G1-1)
(Sheet 15 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G1-1)
(Sheet 16 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G1-1)
(Sheet 17 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G1-1)
(Sheet 18 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G1-1)
(Sheet 19 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G1-1)
(Sheet 20 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G1-1)
(Sheet 21 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G1-1)
(Sheet 22 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G1-1)
(Sheet 23 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G1-1)
(Sheet 24 of 25)

Table G.2-2 FMEA for ESF Actuation in PSMS (for Figure G1-1)
(Sheet 25 of 25)

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

The US-APWR PAM list provided in the DCD Table 7.5-3 was developed to be in compliance with the guidance of RG 1.97 Rev. 4 and IEEE 497-2002, which is endorsed by RG 1.97 Rev. 4. The US-APWR PAM variables are utilized by a combination of previous versions of RG 1.97, Japanese domestic and US operational experience and emergency procedures, and known differences between current operating plants and the US-APWR design to develop a bounding and complete PAM list for the US-APWR. The following subsections describe the selection basis for the variables included in the DCD Table 7.5-3.

Table 3 of RG 1.97 Rev. 3 prescribes a minimum list of Type B, C, D, and E variables to monitor. However, The US-APWR PAM variables are utilized by the performance-based criteria of RG 1.97 Rev. 4 and IEEE 497-2002 to select the Type B, C, D, and E accident monitoring variables for the US-APWR. Therefore, there are some differences between the RG 1.97 Rev. 3 and the US-APWR PAM lists for these variable types. Additionally, Type A variables were not included in RG 1.97 Rev. 3, so a slightly different methodology was utilized to select the bounding list of Type A variables for the US-APWR. A discussion of the variable selection basis for each type of PAM variable is described below. The specific basis for the inclusion or exclusion of a specific variable in the DCD Table 7.5-3 is provided in Tables H.1-1 through H.5-1 for each variable classification type.

The variables required by 10 CFR 50.34(f)(2)xvii are included in RG 1.97 Rev.3. Therefore, conformance to 10 CFR 50.34(f)(2)xvii are also shown in Tables H.1-1 through H.5-1

H.1 Type A Variables

NUREG-1431 Table 3.3.3-1 provides a minimal list of Category 1 variables (any Type) for a typical Westinghouse NSSS plant based on the guidance in RG 1.97 Rev. 3. The US-APWR PAM variables are utilized in this list as an initial starting point for the US-APWR Type A PAM list. Then the US-APWR PAM variables are utilized by the performance-based criteria of RG 1.97 Rev. 4 and IEEE 497-2002 to select the specific Type A accident monitoring variables for the US-APWR. IEEE 497-2002 defines Type A variables as follows.

Type A variables are those variables that provide the primary information required to permit the control room operating staff to:

- a) Take specific planned manually-controlled actions for which no automatic control is provided and that are required for safety-related systems to perform their safety-related functions as assumed in the plant Accident Analysis Licensing Basis.
- b) Take specific planned manually-controlled actions for which no automatic control is provided and that are required to mitigate the consequences of an AOO.

The SGTR is the only event that assumes planned operator actions using the Type A variables listed in Table 7.5-3. Planned operator actions required for other events are initiated by an alarm or they are based on a time limit.

In the event of an SGTR, the DBA analysis in Subsection 15.6.3 assumes the following specific operator actions:

- Identify and Isolate Ruptured SG
- Cool Down Primary Coolant System
- Depressurize Primary Coolant System to Equalize Pressure between Primary and Secondary
- Terminate Safety Injection Flow

Some Type A variables are monitored before the operator takes the above manual actions. These Type A variables are shown in the DCD Table 7.5-11.

Regarding the LOCA event, RWSP level is an important indication in some currently operating plants because operator action is needed to realign the injection of ECCS from the RWSP to the containment sump before the RWSP becomes empty. In the US-APWR, the RWSP is located at the bottom of the containment and the suction of both the SIP and CS/RHRP is the RWSP from the beginning. Therefore, it is not necessary to confirm the RWSP level during the LOCA event and this variable is not included as a Type A variable for the US-APWR.

The analyses of the Steam Line Break (SLB) in the DCD Subsection 15.1.5 and Feedwater Line Break (FLB) in the DCD Subsection 15.2.8 assume EFW isolation from a faulted SG. However, this action is performed automatically by the low main steam line pressure signal EFW isolation function. Therefore, there are no PAM instruments related to operator actions assumed in the SLB and FLB analyses.

In all DBA analysis, except for the SGTR previously discussed, explicit operator actions are not assumed based on primary information from PAM instruments. However, SI termination and long-term core cooling from secondary heat sink are necessary to bring the plant to cold shut down conditions. Operator actions for SI termination and core cooling are already included in the operator actions assumed in the SGTR analysis. Therefore, the instruments associated with these functions have already been included in the bounding PAM list provided in the DCD Table 7.5-3.

Table H.5-1 compares all of the Category 1 variables (any Type) functions in NUREG-1431 Table 3.3.3-1 to the US APWR Type A variables currently listed in the DCD Table 7.5-3 and summarizes the bases for differences between the Type A variables in the US-APWR PAM list and the Category 1 PAM for a typical Westinghouse 4 loop PWR plant. The above described methodology serves as the basis for the selection of the US-APWR Type A PAM variables included in the DCD Table 7.5-3.

H.2 Type B Variables

IEEE 497-2002 defines Type B variables as follows.

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

The plant critical safety functions are those functions necessary to prevent a direct and immediate threat to public health and safety. The following basic critical safety functions are defined in RG 1.97 Rev. 3 and IEEE 497-2002:

- Reactivity Control,
- Core Cooling,
- Maintaining Reactor Coolant System Integrity,
- Maintaining Containment Integrity (including radioactive effluent control).

Plant safety is accomplished by ensuring that certain parameters related to the plant critical safety functions are not exceeded. The US-APWR Emergency Response Guidelines (ERGs) provide protection of these plant critical safety functions. The ERGs establish predefined function-related restoration strategies for responding to emergency transients where the initiating event is unknown and the transient is not predefined. The restoration strategies utilize available plant equipment to restore the parameters used for entry conditions to values sufficient to ensure protection of the plant critical safety function.

The bounding US-APWR Type B PAM variables are selected ensure availability of the variables needed to implement the functional restoration portion of the ERGs as described above. Table H.2-1 describes the bases for the differences between the Type B variables included in the US-APWR PAM list compared to those included in RG 1.97 Rev. 3 Table 3.

H.3 Type C Variables

IEEE 497-2002 defines Type C variables as follows.

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

Table H.3-1 describes the bases for the differences between the Type C variables included in the US-APWR PAM list compared to those included in RG 1.97 Rev. 3 Table 3.

H.4 Type D Variables

IEEE 497-2002 defines Type D variables as follows.

Type D variables are those variables that are required in procedures and LBD to:

- a) Indicate the performance of those safety-related systems and auxiliary supporting features necessary for the mitigation of design basis events.
- b) Indicate the performance of other systems necessary to achieve and maintain a safe shutdown condition.
- c) Verify safety-related system status.

The US-APWR Type D variable list is almost identical to the Type D variables included in Table 3 of RG 1.97 Rev.3. One notable departure is the variable to monitor flow in the low pressure injection system. The accumulators and high head safety injection system in US-APWR are designed to replace the entire low head safety injection function; therefore, this

system is not part of the US-APWR design and this monitoring variable is not applicable to the US-APWR.

Another notable departure from the RG 1.97 Rev.3 Type D variable list involves the chemical volume and control system (CVCS). The high head injection system and emergency letdown system of the US APWR has a required safety-related function to ensure a means for feed and bleed for boration and make up water for compensation of shrinkage if the normal CVCS is unavailable. Since the US-APWR SI system performs the necessary RCS inventory and boration functions, the CVCS-related monitoring variables are not necessary for the US-APWR design and thus not included in the US-APWR Type D variable list.

Table H.4-1 describes the bases for the differences between the Type D variables included in the US-APWR PAM list compared to those included in RG 1.97 Rev. 3 Table 3.

H.5 Type E Variables

IEEE 497-2002 defines Type E variables as follows.

Type E variables are those variables required for use in determining the magnitude of the release of radioactive materials and continually assessing such releases.

The selection of these variables shall include, but not be limited to, the following:

- a) Monitor the magnitude of releases of radioactive materials through identified pathways (e.g., secondary safety valves, and condenser air ejector).
- b) Monitor the environmental conditions used to determine the impact of releases of radioactive materials through identified pathways (e.g., wind speed, wind direction, and air temperature).
- c) Monitor radiation levels and radioactivity in the plant environs.
- d) Monitor radiation levels and radioactivity in the control room and selected plant areas where access may be required for plant recovery.

Table H.5-1 describes the bases for the differences between the Type E variables included in the US-APWR PAM list compared to those included in RG 1.97 Rev. 3 Table 3.

Table H.1-1 Basis for Differences between NUREG-1431 Table 3.3.3-1 and the US-APWR Type A PAM List
(Sheet 1 of 3)

RG 1.97 Function	Purpose	NUREG-1431 Table 3.3.3-1 Variable	Corresponding US-APWR Type A PAM Variable	Basis for Difference
Reactivity Control	Indication of subcritical conditions	Power Range Neutron Flux	-	There are no credited manual actions prompted by indications of subcritical conditions and no credited manual actions that require monitoring subcritical conditions. Wide Range Neutron Flux is a Type B and D variable for the US-APWR.
Reactivity Control	Indication of subcritical conditions	Source Range Neutron Flux	-	There are no credited manual actions prompted by indications of subcritical conditions and no credited manual actions that require monitoring subcritical conditions.
Core Cooling	Indication of core cooling; Manual action; Long-term core cooling	RCS Hot Leg Temperature	Reactor Coolant Hot Leg Temperature (Wide Range)	Intact loop hot leg temperature is applied for determining the termination of RCS cooldown and initiation of RCS depressurization in the SGTR analysis. Therefore, this is a Type A variable for the US-APWR.
Core Cooling	Indication of core cooling; Long-term core cooling	RCS Cold Leg Temperature	Reactor Coolant Cold Leg Temperature (Wide Range)	This parameter is not explicitly assumed in safety analysis; however, monitoring of this parameter is necessary for cooling down after mitigating a PA or AOO. Therefore, this is a Type A parameter for the US-APWR.
Core Cooling; Maintaining RCS Integrity; RCS Pressure Boundary; Primary Coolant System	-SGTR Safety Analysis Manual Action -RCS Depressurization based on EOPs for SGTR event	RCS Pressure (Wide Range)	Reactor Coolant Pressure	No difference.
Core Cooling	To ensure RCS inventory	Reactor Vessel Water Level	-	This parameter is not applied in the safety analysis. RV Water Level is a Type B and D variable for the US-APWR.
Core cooling; Maintaining RCS Integrity; RCS Pressure Boundary	Indication of core cooling function for RWSP switchover and status of ECCS recirculation delivery	Containment Sump Water Level (Wide Range)	-	This parameter is not applied in safety analysis since the US-APWR RWSP is located inside containment and does not require switchover to the recirculation sump. RWSP level is a Type B and D variable for the US-APWR.

Table H.1-1 Basis for Differences between NUREG-1431 Table 3.3.3-1 and the US-APWR Type A PAM List (Sheet 2 of 3)

RG 1.97 Function	Purpose	NUREG-1431 Table 3.3.3-1 Variable	Corresponding US-APWR Type A PAM Variable	Basis for Difference
Maintaining Containment and RCS Integrity; RCS Pressure Boundary	Indication of containment integrity function	Containment Pressure	-	This parameter is not applied in the safety analysis. Containment Pressure is a Type B and D variable for the US-APWR.
Containment Isolation/Integrity	Indication of containment integrity function	Penetration Flow Path Containment Isolation Valve Position	-	This parameter is not applied in the safety analysis. C/V Isolation Valve Position is a Type B and D variable for the US-APWR.
Containment Radiation; RCS Pressure Boundary	Identify challenge to fission product barrier	Containment Area Radiation (High Range)	-	This parameter is not applied in the safety analysis. Containment Area Radiation is a Type C and E variable for the US-APWR.
Primary Coolant System; RCS Pressure Boundary	To ensure proper operation of the pressurizer	Pressurizer Level	Pressurizer Water Level	No difference.
Secondary System; RCS Pressure Boundary	Verification of heat sink availability	Steam Generator Water Level (Wide Range)	-	This parameter is not applied in the safety analysis. SG narrow range level is applied in safety analysis and US-APWR ERG instead of this parameter. SG Wide Range Level is a Type B and D variable for the US-APWR.
Auxiliary Feedwater System	Indication of ability to maintain SG heat sink and indication of long-term AFW operation	Condensate Storage Tank Level	-	The EFW pit has enough water to maintain long-term core cooling; therefore, this variable is not applied in the safety analysis. This is a Type B and D variable for the US-APWR.
Core Cooling; Fuel Cladding Integrity; Maintain RCS Integrity; RCS Pressure Boundary; Primary Coolant System	Indication of core cooling	Core Exit Temperature – Quadrant [1]-[4]	-	This parameter is not applied in the safety analysis. Core Exit Temperature is a Type B and C variable for the US-APWR.
Auxiliary Feedwater System	Verification of automatic actuation and ability to satisfy heat sink requirements	Auxiliary Feedwater Flow	EFW Flow	No difference. This parameter is used to determine if the ECCS termination criteria are met in the SGTR analysis.

Table H.1-1 Basis for Differences between NUREG-1431 Table 3.3.3-1 and the US-APWR Type A PAM List (Sheet 3 of 3)

RG 1.97 Function	Purpose	NUREG-1431 Table 3.3.3-1 Variable	Corresponding US-APWR Type A PAM Variable	Basis for Difference
Secondary System	Verification of manual action for SGTR termination (along w/ RCS Pressure)	-	Main Steam Line Pressure	This parameter is applied for determining the termination of RCS cooldown and initiation of RCS depressurization in the SGTR analysis. Therefore, this is a Type A variable for the US-APWR.
Secondary System; RCS Pressure Boundary	Verification of heat sink availability	-	SG Water Level (Narrow Range)	This parameter is monitored for the operator to determine if the ECCS termination criteria are met in the SGTR analysis. This parameter is also used in the ERGs to identify ruptured SG(s). Therefore, this is a Type A variable for the US-APWR.
Core Cooling	Indication of core cooling	-	Degrees of Subcooling	This parameter is monitored for the operator to determine if the terminating RCS depressurization criteria or ECCS termination criteria are met in the SGTR analysis. Therefore, this is a Type A variable for the US-APWR.

**Table H.2-1 Basis for Type B Differences between RG 1.97 Rev.3 and the US-APWR PAM List
(Sheet 1 of 2)**

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Reactivity Control			
Neutron Flux	Function detection; accomplishment of mitigation	Wide Range Neutron Flux	No difference
Control Rod Position	Verification	-	The primary indication of reactor shutdown is neutron flux (Type B). Therefore, for the US-APWR control rod position is provided, but it is not identified as a PAM variable.
RCS Soluble Boron Concentration	Verification	Reactor Coolant Soluble Boron Concentration	No difference
RCS Cold Leg Water Temperature	Verification	Reactor Coolant Cold Leg Temperature (Wide Range)	No difference
Core Cooling			
RCS Hot Leg Water Temperature	Function detection; accomplishment of mitigation; verification; long-term surveillance	Reactor Coolant Hot Leg Temperature (Wide Range)	No difference
RCS Cold Leg Water Temperature	Function detection; accomplishment of mitigation; verification; long-term surveillance	Reactor Coolant Cold Leg Temperature (Wide Range)	No difference
RCS Pressure	Function detection; accomplishment of mitigation; verification; long-term surveillance	Reactor Coolant Pressure	No difference
Core Exit Temperature	Verification	Core Exit Temperature	No difference
Coolant Inventory	Verification; accomplishment of mitigation	RV Water Level	No difference
Degrees of Subcooling	Verification and analysis of plant conditions	Degrees of Subcooling	No difference

**Table H.2-1 Basis for Type B Differences between RG 1.97 Rev.3 and the US-APWR PAM List
(Sheet 2 of 2)**

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Maintaining Reactor Coolant System Integrity			
RCS Pressure	Function detection; accomplishment of mitigation	Reactor Coolant Pressure	No difference
Containment Sump Water Level	Function detection; accomplishment of mitigation; verification	Refueling Water Storage Pit Water Level (Wide Range) Refueling Water Storage Pit Water Level (Narrow Range)	No difference. The US-APWR RWSP is located inside containment, essentially combining the function of the sump and RWSP.
Containment Pressure	Function detection; accomplishment of mitigation; verification	Containment Pressure	No difference
Maintaining Containment Integrity			
Containment Isolation Valve Position (excluding check valves)	Accomplishment of isolation	Containment Isolation Valve Position (Excluding Check Valves)	No difference
Containment Pressure	Function detection; accomplishment of mitigation; verification	Containment Pressure	No difference
Other			
-	-	Pressurizer Water Level	This parameter is important to monitor because it is related to the SI termination criteria, which is related to maintaining adequate RCS inventory to assure core cooling.
-	-	Main Steam Line Pressure	This parameter is important to monitor the efficiency of removing the decay heat of core, which is related to core cooling.
-	-	SG Water Level (Wide Range)	This parameter provides indication of heat sink availability and is selected to monitor core cooling.
-	-	SG Water Level (Narrow Range)	This parameter provides indication of heat sink availability and is selected to monitor core cooling.
-	-	EFW Flow	This parameter provides verification of the automatic actuation of EFW and is selected to monitor core cooling.
-	-	EFW Pit Water Level	This parameter provides indication of heat sink availability and is selected to monitor core cooling.

Table H.3-1 Basis for Type C Differences between RG 1.97 Rev.3 and the US-APWR PAM List (Sheet 1 of 2)

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Fuel Cladding			
Radioactivity Concentration or Radiation Level in Circulating Primary Coolant	Detection of breach	Radioactivity Concentration or Radiation Level in Circulating Primary Coolant	No difference
Core Exit Temperature	Detection of breach	Core Exit Temperature	No difference
Analysis of Primary Coolant (Gamma Spectrum)	Detail analysis; accomplishment of mitigation; verification; long-term surveillance	-	In the US-APWR, concentration of each radioactive nuclide is derived from RCS sampling. RG 1.97 Rev.3 allows analysis of primary coolant by sampling.
Reactor Coolant Pressure Boundary			
RCS Pressure	Detection of potential for or actual breach; accomplishment of mitigation; long-term surveillance	Reactor Coolant Pressure	No difference
Containment Pressure	Detection of breach; accomplishment of mitigation; long-term surveillance	Containment Pressure	No difference
Containment Sump Water Level	Detection of breach; accomplishment of mitigation; long-term surveillance	-	Containment Pressure is a more direct indication of a potential containment breach. Therefore, RWSP level is not included as a Type C variable for the US-APWR.
Containment Area Radiation	Detection of breach; verification	Containment High Range Area Radiation	No difference.
Effluent Radioactivity - Noble Gas Effluent from Condenser Air Removal System Exhaust	Detection of breach; verification	-	Coolant leakage outside containment to secondary system due to an actual breach of the reactor coolant pressure boundary can be detected by RCS pressure, SG water level, and pressurizer water level. These variables are PAM variables. Therefore, it is not necessary to include effluent radioactivity as a Type C variable.

**Table H.3-1 Basis for Type C Differences between RG 1.97 Rev.3 and the US-APWR PAM List
(Sheet 2 of 2)**

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Containment			
RCS Pressure	Detection of potential for breach; accomplishment of mitigation	Reactor Coolant Pressure	No difference
Containment Hydrogen Concentration	Detection of potential for breach; accomplishment of mitigation; long-term surveillance	-	This instrumentation is used for monitoring severe accidents. Therefore, it does not need to be a Type C variable.
Containment Pressure	Detection of potential for or actual breach; accomplishment of mitigation	Containment Pressure	No difference
Containment Effluent Radioactivity - Noble Gas Effluent from Identified Release Points	Detection of breach; accomplishment of mitigation; verification	-	The plant vent receives the discharge from the containment purge, auxiliary building, control building, fuel building, and the condenser air removal filtration system. This variable can be measured by plant vent radiation monitor (including high range) and therefore is not included as a separate Type C variable for the US-APWR.
Effluent Radioactivity - Noble Gases (from buildings or areas where penetrations and hatches are located, e.g., secondary containment and auxiliary buildings and fuel handling buildings that are in direct contact with primary containment)	Indication of breach	-	The plant vent receives the discharge from the containment purge, auxiliary building, control building, fuel building, and the condenser air removal filtration system. This variable can be measured by plant vent radiation monitor (including high range) and therefore is not included as a separate Type C variable for the US-APWR.

**Table H.4-1 Basis for Type D Differences between RG 1.97 Rev.3 and the US-APWR PAM List
(Sheet 1 of 5)**

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Residual Heat Removal (RHR) or Decay Heat Removal System			
RHR System Flow	To monitor operation	CS/RHR Pump Discharge Flow CS/RHR Pump Minimum Flow	No difference
RHR Heat Exchanger Outlet Temperature	To monitor operation and for analysis	-	Proper operation of the RHR system is verified by CS/RHR flow rate. Additionally, T_{hot} and T_{cold} are available to monitor RHR system performance with respect to decay heat removal. Therefore, it is not necessary to include the RHR heat exchanger outlet temperature as a Type D variable in the US-APWR PAM list.
Safety Injection System			
Accumulator Tank Level and Pressure	To monitor operation	Accumulator Water Level, Accumulator Pressure	No difference
Accumulator Isolation Valve Position	Operation status	-	Accumulator water level and accumulator pressure are available to monitor operation status. Therefore, it is not necessary to include isolation valve position as a separate Type D variable in the US-APWR PAM list.
Boric Acid Charging Flow	To monitor operation	-	The safety injection system delivers boric acid water to the RCS in the US-APWR. Safety Injection Pump Discharge Flow and Safety Injection Pump Minimum Flow are available to monitor the flow. Therefore it is not necessary to include this as a Type D variable in the US-APWR PAM list.
Flow in HPI System	To monitor operation	Safety Injection Pump Discharge Flow Safety Injection Pump Minimum Flow	No difference
Flow in LPI System	To monitor operation	-	The US-APWR design allows the accumulators and high head safety injection system to fully replace the safety function associated with the low head safety injection system. Therefore, the US-APWR PAM list does not need any variables to indicate LPI system performance.
Refueling Water Storage Tank Level	To monitor operation	Refueling Water Storage Pit Water Level (Wide Range) Refueling Water Storage Pit Water Level (Narrow Range)	No difference

**Table H.4-1 Basis for Type D Differences between RG 1.97 Rev.3 and the US-APWR PAM List
(Sheet 2 of 5)**

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Primary Coolant System			
Reactor Coolant Pump Status	To monitor operation	-	The safety analysis does not rely on the RCP to mitigate design basis events. The RCPs are also not necessary to achieve and maintain a safe shutdown condition. CCW header pressure is available to monitor CCW performance related to its function to deliver seal flow to the RCP in order to maintain its RCS pressure boundary function. Therefore, RCP status is not included as a PAM variable for the US-APWR.
Primary System Safety Relief Valve Positions (including PORV and code valves) or Flow Through or Pressure in Relief Valve Lines	Operation status; to monitor for loss of coolant	-	RCS pressure, Reactor Coolant Hot Leg Temperature, and Reactor Coolant Cold Leg Temperature are available to monitor operation status of the primary coolant system. Consistent trends in changes to the values of these variables are indicative of a loss of coolant. Therefore, it is not necessary to include position indication or flow indication for the primary relief valves in the PAM list.
Pressurizer Level	To ensure proper operation of pressure	Pressurizer Water Level	No difference
Pressurizer Heater Status	To determine operating status	-	Pressurizer water level and RCS pressure are indicative of the performance of the pressurizer heater. Therefore it is not necessary to separately include heater status in the PAM list.
Quench Tank Level	To monitor operation	-	This component is not necessary to mitigate design basis events, and not necessary to achieve and maintain a safe shutdown condition. Therefore, it is not included in the US-APWR PAM list.
Quench Tank Temperature	To monitor operation	-	Same as above
Quench Tank Pressure	To monitor operation	-	Same as above
Secondary System (Steam Generator)			
Steam Generator Level	To monitor operation	SG Water Level (Wide Range), SG Water Level (Narrow Range)	No difference

**Table H.4-1 Basis for Type D Differences between RG 1.97 Rev.3 and the US-APWR PAM List
(Sheet 3 of 5)**

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Steam Generator Pressure	To monitor operation	Main Steam Line Pressure	No difference
Safety/Relief Valve Positions or Main Steam Flow	To monitor operation	-	Main steam line pressure is indicative of main steam flow and is available to monitor its SG operation. Therefore it is not necessary to separately include this variable in the PAM list.
Main Feedwater Flow	To monitor operation	-	SG water level and main steam line pressure are indicative of adequate feedwater flow. Since these variables are available to monitor SG operation, it is not necessary to separately include MFW flow in the PAM list.
Auxiliary Feedwater or Emergency Feedwater System			
Auxiliary or Emergency Feedwater Flow	To monitor operation	EFW Flow	No difference
Condensate Storage Tank Water Level	To ensure water supply for auxiliary feedwater	EFW Pit Water Level	No difference
Containment Cooling Systems			
Containment Spray Flow	To monitor operation	CS/RHR Pump Discharge Flow CS/RHR Pump Minimum Flow	No difference
Heat Removal by the Containment Fan Heat Removal System	To indicate accomplishment of cooling	-	The containment fan heat removal system is not credited in design basis events since containment spray is credited to maintain containment integrity. Therefore this variable is not included in the PAM list.
Containment Atmosphere Temperature	To monitor operation	Containment Temperature	No difference
Containment Sump Water Temperature	To monitor operation	-	Containment pressure, containment temperature, and containment spray flow are utilized to monitor containment cooling system performance. Therefore it is not necessary to include this variable in the US-APWR PAM list.

**Table H.4-1 Basis for Type D Differences between RG 1.97 Rev.3 and the US-APWR PAM List
(Sheet 4 of 5)**

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Chemical and Volume Control System (CVCS)			
Makeup Flow - In	To monitor operation	-	Since RCS inventory and boration are achieved by the safety injection system in the US-APWR, the monitoring variables related to CVCS are not necessary PAM variables for the US-APWR design.
Letdown Flow - Out	To monitor operation	-	Same as above
Volume Control Tank Level	To monitor operation	-	Same as above
Cooling Water System (CCW)			
Component Cooling Water Temperature to ESF System	To monitor operation	-	CCW header pressure provides indication of the performance of the cooling water system. Therefore it is not necessary to separately include this variable in the PAM list.
Component Cooling Water Flow to ESF System	To monitor operation	-	Same as above
Radwaste Systems			
High-Level Radioactive Liquid Tank Level	To indicate storage volume	-	The US-APWR design precludes the need for this variable. This component is not necessary to mitigate design basis events and not necessary to achieve and maintain a safe shutdown condition. Addition of additional radioactive waste to the liquid or gaseous radwaste system following an accident is precluded by design and is not postulated. Therefore, this variable is not included in the US-APWR PAM list.
Radioactive Gas Holdup Tank Pressure	To indicate storage capacity	-	Same as above
Ventilation Systems			
Emergency Ventilation Damper Position	To indicate damper status	-	Containment Isolation Valve Position provides indication of containment integrity. The combination of isolation valve position status and a lack of radioactive release as indicated by the plant vent monitor provides verification of proper automatic ventilation path isolation. Therefore, damper position indication is not included in the US-APWR PAM list.

**Table H.4-1 Basis for Type D Differences between RG 1.97 Rev.3 and the US-APWR PAM List
(Sheet 5 of 5)**

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Power Supplies			
Status of Standby Power and Other Energy Sources Important to Safety (electric, hydraulic, pneumatic) (voltages, currents, pressures)	To indicate system status	Status of Standby Power and Other Energy Sources Important to Safety Class 1E ac Bus Voltage Class 1E dc Bus Voltage	No difference
Other			
-	-	Reactor Coolant Hot Leg Temperature (Wide Range)	This variable indicates the performance of the primary coolant system for maintaining core cooling.
-	-	Reactor Coolant Cold Leg Temperature (Wide Range)	Same as above
-	-	Reactor Coolant Pressure	This variable indicates the performance of the primary coolant system for maintaining core cooling and RCS integrity.
-	-	Degrees of Subcooling	This variable is used to indicate the performance of the primary coolant system for core cooling.
-	-	RV Water Level	This variable provides direct indication of inventory available for maintaining core cooling.
-	-	Wide Range Neutron Flux	This variable directly indicates reactivity control and allows for the monitoring of the performance of the control rod assemblies.
-	-	Containment Pressure	This variable is used to indicate the containment integrity status.
-	-	Containment Isolation Valve Position (Excluding Check Valves)	This variable is used to indicate the containment integrity status.
-	-	CCW Header Pressure	This variable is used to indicate the performance of the CCW system.
-	-	ESW Header Pressure	This variable is used to indicate the performance of the ESW system.

**Table H.5-1 Basis for Type E Differences between RG 1.97 Rev.3 and the US-APWR PAM List
(Sheet 1 of 4)**

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Containment Radiation			
Containment Area Radiation - High Range	Detection of significant releases; release assessment; long-term surveillance; emergency plan actuation	Containment High Range Area Radiation	No difference
Area Radiation			
Radiation Exposure Rate (inside buildings or areas where access is required to service equipment important to safety)	Detection of significant releases; release assessment; long-term surveillance	-	This parameter can be measured by area monitors located where personnel enter areas after the accident. Additional personnel protection will be provided by the use of portable radiation monitors and air sampling. Therefore, it is not necessary to include this variable in the US-APWR PAM list.
Airborne Radioactive Materials Released from Plant			
<i>Noble Gases and Vent Flow Rate</i>			
Containment or Purge Effluent	Detection of significant releases; release assessment	-	The plant vent receives the discharge from the containment purge, auxiliary building, control building, fuel building, and the condenser air removal filtration system. These variables can be measured by plant vent radiation monitor (including high range) and therefore are not included as separate Type E variables for the US-APWR.
Reactor Shield Building (if in design)	Detection of significant releases; release assessment	-	
Auxiliary Building (including any building containing primary system gases, e.g., waste gas decay tank)	Detection of significant releases; release assessment; long-term surveillance	-	
Condenser Air Removal System Exhaust	Detection of significant releases; release assessment	-	

**Table H.5-1 Basis for Type E Differences between RG 1.97 Rev.3 and the US-APWR PAM List
(Sheet 2 of 4)**

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Common Plant Vent or Multipurpose Vent Discharging Any of Above Releases (if containment purge is included)	Detection of significant releases; release assessment; long-term surveillance	-	This variable can be measured by plant vent radiation monitor (including high range) and therefore is not included as a separate Type E variable for the US-APWR.
Vent From Steam Generator Safety Relief Valves or Atmospheric Dump Valves	Detection of significant releases; release assessment	-	This variable is measured by main steam line monitor. Therefore it is not included as a separate Type E variable for the US-APWR.
All Other Identified Release Points	Detection of significant releases; release assessment; long-term surveillance	-	This variable can be measured by plant vent radiation monitor (including high range) and therefore is not included as a separate Type E variable for the US-APWR.
Particulates and Halogens			
All Identified Plant Release Points (except steam generator safety relief valves or atmospheric steam dump valves and condenser air removal system exhaust). Sampling with Onsite Analysis Capability	Detection of significant releases; release assessment; long-term surveillance	-	This can be measured by plant vent sampler (accident sampler). Therefore it is not included as a separate Type E variable for the US-APWR.
Enviorns Radiation and Radioactivity			
Airborne Radiohalogens and Particulates (portable sampling with onsite analysis capability)	Release assessment; analysis	Airborne Radio Halogens and Particulates (Portable Sampling with Onsite Analysis Capability)	No difference

Table H.5-1 Basis for Type E Differences between RG 1.97 Rev.3 and the US-APWR PAM List (Sheet 3 of 4)

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Plant and Environs Radiation (portable instrumentation)	Release assessment; analysis	Plant and Environs Radiation (Portable Instrumentation)	No difference
Plant and Environs Radioactivity (portable instrumentation)	Release assessment; analysis	Plant and Environs Radioactivity (Portable Instrumentation)	No difference
Meteorology			
Wind Direction	Release assessment	Meteorological Parameters (Wind Direction, Wind Speed, Estimation of Atmospheric Stability)	No difference
Wind Speed	Release assessment	Meteorological Parameters (Wind Direction, Wind Speed, Estimation of Atmospheric Stability)	No difference
Estimation of Atmospheric Stability	Release assessment	Meteorological Parameters (Wind Direction, Wind Speed, Estimation of Atmospheric Stability)	No difference
Accident Sampling Capability (Analysis Capability On Site)			
Primary Coolant and Sump <ul style="list-style-type: none"> • Gross Activity • Gamma Spectrum • Boron Content • Chloride Content • Dissolved Hydrogen or Total Gas • Dissolved Oxygen • pH 	Release assessment; verification analysis		These parameters can be measured by sampling. Many operating plants have received NRC approval for eliminating the PASS requirements specified in RG 1.97 Rev. 3. Therefore, these parameters are also not included in the US-APWR Type E PAM list.

**Table H.5-1 Basis for Type E Differences between RG 1.97 Rev.3 and the US-APWR PAM List
(Sheet 4 of 4)**

RG 1.97 Rev. 3 Variable	Purpose	US-APWR PAM Variable	Basis for Difference
Containment Air • Hydrogen Content • Oxygen Content • Gamma Spectrum	Release assessment; verification analysis	-	These parameters can be measured by sampling. Many operating plants have received NRC approval for eliminating the PASS requirements specified in RG 1.97 Rev. 3. Therefore, these parameters are also not included in the US-APWR Type E PAM list.
Other			
-	-	MCR Area Radiation	To monitor radiation and radioactivity levels in the control room.
-	-	MCR Outside Air Intake Radiation	To monitor radiation and radioactivity levels in the control room.
-	-	TSC Outside Air Intake Radiation	To monitor radiation and radioactivity levels in the technical support center.
-	-	Plant Vent Radiation Gas Radiation (Including High Range)	To monitor the magnitude of releases of radioactive materials through identified pathways.
-	-	Main Steam Line Radiation	To monitor the magnitude of releases of radioactive materials through identified pathways.
-	-	GSS Exhaust Fan Discharge Line Radiation (Including High Range)	To monitor the magnitude of releases of radioactive materials through identified pathways.
-	-	Condenser Vacuum Pump Exhaust Line Radiation (Including High Range)	To monitor the magnitude of releases of radioactive materials through identified pathways.
-	-	Plant Air Vent High Concentration Sampling System	To monitor the magnitude of releases of radioactive materials through identified pathways.