ENCLOSURE 2

WATTS BAR NUCLEAR PLANT (WBN) UNIT 2 – NRC MEETING HELD ON AUGUST 4, 2010 - INSTRUMENTATION AND CONTROL - REQUEST FOR ADDITIONAL INFORMATION

Nuclear Power Group Calculation

titled "Segmentation Analysis for WBN Unit 2 DCS (Distributed Control System)"

dated August 2, 2010, Revision 0

NPG CALCULATION COVERSHEET/CCRIS UPDATE

REV 0 EDMS/RIMS NO.	EDMS TYPE: calculations(nuclear)	EDMS ACCESSION NO (N/A for REV. 0)

Calc Title: **SEGMENTATION ANALYSIS FOR WBN UNIT 2 DCS**

CALC ID	TYPE	ORG	PLANT	BRANCH	NUMBER	CUR REV	NEW REV	REVISION APPLICABILITY
CURRENT	CN	NUC						Entire calc ☒
NEW	CN	NUC	WBN	EEB	**DCSSEGMENT**		000	Selected pages ☐

ACTION	NEW ☒ REVISION ☐	DELETE ☐ RENAME ☐	SUPERSEDE ☐ DUPLICATE ☐	CCRIS UPDATE ONLY ☐ (Verifier Approval Signatures Not Required)	No CCRIS Changes ☐ (For calc revision, CCRIS been reviewed and no CCRIS changes required)

UNITS	SYSTEMS	UNIDS
2	001 003 062 063 068 085 092 098	NA

DCN,EDC,N/A	APPLICABLE DESIGN DOCUMENT(S)	CLASSIFICATION
EDCR 54504	NA	D

QUALITY RELATED?	SAFETY RELATED? (If yes, QR = yes)	UNVERIFIED ASSUMPTION	SPECIAL REQUIREMENTS AND/OR LIMITING CONDITIONS?	DESIGN OUTPUT ATTACHMENT?	SAR/TS and/or ISFSI SAR/CoC AFFECTED
Yes ☒ No ☐	Yes ☐ No ☒	Yes ☒ No ☐	Yes ☐ No ☒	Yes ☐ No ☒	Yes ☒ No ☐

PREPARER ID	PREPARER PHONE NO	PREPARING ORG (BRANCH)	VERIFICATION METHOD	NEW METHOD OF ANALYSIS
wdwebb	632-8245	EEB	Design Verification	☐ Yes ☒ No

PREPARER SIGNATURE	DATE	CHECKER SIGNATURE	DATE
W. D. Webb *WD Webb*	7-29-10	J. T. Kepler *J.T. Kepler*	7/29/10
VERIFIER SIGNATURE	**DATE**	**APPROVAL SIGNATURE**	**DATE**
J. T. Kepler *J.T. Kepler*	7-29-10	*Fred D. Mitrech* *Fred D. Mitrech*	8/2/10

STATEMENT OF PROBLEM/ABSTRACT

The obsolete analog control systems for WBN unit 2 are being replaced with a Foxboro IA Distributed Control System (DCS) for control and monitoring of most non-safety related NSSS and BOP systems. The controls are distributed among 15 control groups, each with a redundant processor pair. For those control system functions which are important to plant operation, this analysis evaluates the distribution (segmentation) of the inputs/outputs among these control groups to confirm that no new failures are introduced which could adversely impact plant safety analyses. The analysis includes confirmation that the DCS configuration maintains the functional diversity and independence of the original control systems design.

Based on this analysis, the design of the WBN unit 2 DCS does not introduce new control system failures which could adversely impact the safety analyses as described in the FSAR. Functional diversity and independence are provided for the critical control systems as required by the design basis and in a manner consistent with the original design.

MICROFICHE/EFICHE Yes ☐ No ☒ FICHE NUMBER(S)

☐ LOAD INTO EDMS AND DESTROY
☒ LOAD INTO EDMS AND RETURN CALCULATION TO CALCULATION LIBRARY. ADDRESS:EQB 1M-WBN
☐ LOAD INTO EDMS AND RETURN CALCULATION TO:

NPG CALCULATION COVERSHEET/CCRIS UPDATE

CALC ID	TYPE	ORG	PLANT	BRANCH	NUMBER	REV
	CN	NUC	WBN	EEB	DCSSEGMENT	000

ALTERNATE CALCULATION IDENTIFICATION

BLDG	ROOM	ELEV	COORD/AZIM	FIRM	Print Report Yes ☐
NA	NA	NA	NA	Bechtel	

CATEGORIES NA

KEY NOUNS (A-add, D-delete)

ACTION (A/D)	KEY NOUN	A/D	KEY NOUN
	DCS		
	SEGMENT		
	CONTROL		
	ANALYSIS		
	FOXBORO		

CROSS-REFERENCES (A-add, C-change, D-delete)

ACTION (A/C/D)	XREF CODE	XREF TYPE	XREF PLANT	XREF BRANCH	XREF NUMBER	XREF REV
	P	DN	WBN	EEB	EDCR 52378	
	P	DC	WBN	MEB	WB-DC-40-70	
	P	DC	WBN	MEB	WB-DC-40-58	
	P	DG	WBN	EEB	DG-E18.1.25	
	P	SD	WBN	MEB	WBN2-1-4002	
	P	SD	WBN	MEB	WBN2-3A-4002	
	P	SD	WBN	MEB	WBN2-6-4002	
	P	SD	WBN	MEB	WBN2-47-4002	
	P	SD	WBN	MEB	WBN2-62-4001	
	P	SD	WBN	MEB	WBN2-63-4001	
	P	SD	WBN	MEB	WBN2-68-4001	
	P	SD	WBN	EEB	WBN2-85-4003	
	P	SD	WBN	EEB	WBN2-92-4003	
	P	SD	WBN	EEB	WBN2-99-4003	
	P	CN	WBN	MEB	EPMFBN072892	

CCRIS ONLY UPDATES:
Following are required only when making keyword/cross reference CCRIS updates and page 1 of form NEDP-2-1 is not included:

PREPARER SIGNATURE	DATE	CHECKER SIGNATURE	DATE
PREPARER PHONE NO.	EDMS ACCESSION NO.		

NPG CALCULATION COVERSHEET/CCRIS UPDATE

CALC ID	TYPE	ORG	PLANT	BRANCH	NUMBER	REV
	CN	NUC	WBN	EEB	DCSSEGMENT	000

ALTERNATE CALCULATION IDENTIFICATION

BLDG	ROOM	ELEV	COORD/AZIM	FIRM	Print Report Yes ☐
NA	NA	NA	NA	Bechtel	

CATEGORIES NA

KEY NOUNS (A-add, D-delete)

ACTION (A/D)	KEY NOUN	A/D	KEY NOUN

CROSS-REFERENCES (A-add, C-change, D-delete)

ACTION (A/C/D)	XREF CODE	XREF TYPE	XREF PLANT	XREF BRANCH	XREF NUMBER	XREF REV
	P	VD	WBN	EEB	08F802403-FD-2004-1	
	P	VD	WBN	EEB	08F802403-FD-2005-1	
	P	VD	WBN	EEB	08F802403-FD-2006-1	
	P	VD	WBN	EEB	08F802403-FD-2006-2	
	P	VD	WBN	EEB	08F802403-FD-2006-4	
	P	VD	WBN	EEB	08F802403-FD-2006-5	
	P	VD	WBN	EEB	08F802403-FD-2012-1	
	P	VD	WBN	EEB	08F802403-FD-2101-1	
	P	VD	WBN	EEB	08F802403-FD-2101-4	
	P	VD	WBN	EEB	08F802403-FD-2102-1	
	P	VD	WBN	EEB	08F802403-FD-2103-1	
	P	VD	WBN	EEB	08F802403-FD-2103-3	
	P	VD	WBN	EEB	08F802403-FD-2104-1	
	P	VD	WBN	EEB	08F802403-FD-2104-3	
	P	VD	WBN	EEB	08F802403-FD-2105-1	
	P	VD	WBN	EEB	08F802403-FD-2105-2	
	P	VD	WBN	EEB	08F802403-FD-2105-4	
	P	VD	WBN	EEB	08F802403-FD-2107-1	

CCRIS ONLY UPDATES:
Following are required only when making keyword/cross reference CCRIS updates and page 1 of form NEDP-2-1 is not included:

PREPARER SIGNATURE	DATE	CHECKER SIGNATURE	DATE
PREPARER PHONE NO.	EDMS ACCESSION NO.		

NPG CALCULATION COVERSHEET/CCRIS UPDATE

CALC ID	TYPE	ORG	PLANT	BRANCH	NUMBER	REV
	CN	NUC	WBN	EEB	DCSSEGMENT	000

ALTERNATE CALCULATION IDENTIFICATION

BLDG	ROOM	ELEV	COORD/AZIM	FIRM	Print Report Yes ☐
NA	NA	NA	NA	Bechtel	

CATEGORIES NA

KEY NOUNS (A-add, D-delete)

ACTION (A/D)	KEY NOUN	A/D	KEY NOUN

CROSS-REFERENCES (A-add, C-change, D-delete)

ACTION (A/C/D)	XREF CODE	XREF TYPE	XREF PLANT	XREF BRANCH	XREF NUMBER	XREF REV
	P	VD	WBN	EEB	08F802403-FD-2107-2	
	P	VD	WBN	EEB	08F802403-FD-2107-4	
	P	VD	WBN	EEB	08F802403-FD-2109-1	
	P	VD	WBN	EEB	08F802403-FD-2109-2	
	P	VD	WBN	EEB	08F802403-FD-2110-1	
	P	VD	WBN	EEB	08F802403-FD-2111-1	
	P	VD	WBN	EEB	08F802403-FD-2111-2	
	P	VD	WBN	EEB	08F802403-FD-2201-1	
	P	VD	WBN	EEB	08F802403-FD-2202-1	
	P	VD	WBN	EEB	08F802403-FD-2203-1	
	P	VD	WBN	EEB	08F802403-FD-2205-1	
	P	VD	WBN	EEB	08F802403-FD-2205-2	
	P	VD	WBN	EEB	08F802403-FD-2300-1	
	P	VD	WBN	EEB	08F802403-FD-2300-6	
	P	VD	WBN	EEB	08F802403-FD-2301-1	
	P	VD	WBN	EEB	08F802403-FD-2301-6	
	P	VD	WBN	EEB	08F802403-FD-2302-1	
	P	VD	WBN	EEB	08F802403-FD-2302-6	

CCRIS ONLY UPDATES:
Following are required only when making keyword/cross reference CCRIS updates and page 1 of form NEDP-2-1 is not included:

PREPARER SIGNATURE	DATE	CHECKER SIGNATURE	DATE
PREPARER PHONE NO.	EDMS ACCESSION NO.		

NPG CALCULATION COVERSHEET/CCRIS UPDATE

CALC ID	TYPE	ORG	PLANT	BRANCH	NUMBER	REV
	CN	NUC	WBN	EEB	DCSSEGMENT	000

ALTERNATE CALCULATION IDENTIFICATION

BLDG	ROOM	ELEV	COORD/AZIM	FIRM	Print Report Yes ☐
NA	NA	NA	NA	Bechtel	

CATEGORIES NA

KEY NOUNS (A-add, D-delete)

ACTION (A/D)	KEY NOUN	A/D	KEY NOUN

CROSS-REFERENCES (A-add, C-change, D-delete)

ACTION (A/C/D)	XREF CODE	XREF TYPE	XREF PLANT	XREF BRANCH	XREF NUMBER	XREF REV
	P	VD	WBN	EEB	08F802403-FD-2303-1	
	P	VD	WBN	EEB	08F802403-FD-2303-6	
	P	VD	WBN	EEB	08F802403-FD-2304-1	
	P	VD	WBN	EEB	08F802403-FD-2304-3	
	P	VD	WBN	EEB	08F802403-FD-2304-4	
	P	VD	WBN	EEB	08F802403-FD-2304-8	
	P	VD	WBN	EEB	08F802403-FD-2304-9	
	P	VD	WBN	EEB	08F802403-FD-2304-10	
	P	VD	WBN	EEB	08F802403-FD-2400-1	
	P	VD	WBN	EEB	08F802403-FD-2400-3	
	P	VD	WBN	EEB	08F802403-FD-2400-5	
	P	VD	WBN	EEB	08F802403-FD-2400-6	
	P	VD	WBN	EEB	08F802403-FD-2400-7	
	P	VD	WBN	EEB	08F802403-FD-2401-1	
	P	VD	WBN	EEB	08F802403-FD-2401-5	
	P	VD	WBN	EEB	08F802403-FD-2401-6	
	P	VD	WBN	EEB	08F802403-FD-2401-12	

CCRIS ONLY UPDATES:
Following are required only when making keyword/cross reference CCRIS updates and page 1 of form NEDP-2-1 is not included:

PREPARER SIGNATURE	DATE	CHECKER SIGNATURE	DATE
PREPARER PHONE NO.	EDMS ACCESSION NO.		

NPG CALCULATION COVERSHEET/CCRIS UPDATE

CALC ID	TYPE	ORG	PLANT	BRANCH	NUMBER	REV
	CN	NUC	WBN	EEB	DCSSEGMENT	000

ALTERNATE CALCULATION IDENTIFICATION

BLDG	ROOM	ELEV	COORD/AZIM	FIRM	Print Report Yes ☐
NA	NA	NA	NA	Bechtel	

CATEGORIES NA

KEY NOUNS (A-add, D-delete)

ACTION (A/D)	KEY NOUN	A/D	KEY NOUN

CROSS-REFERENCES (A-add, C-change, D-delete)

ACTION (A/C/D)	XREF CODE	XREF TYPE	XREF PLANT	XREF BRANCH	XREF NUMBER	XREF REV
	P	VD	WBN	EEB	08F802403-FD-2402-1	
	P	VD	WBN	EEB	08F802403-FD-2402-3	
	P	VD	WBN	EEB	08F802403-FD-2403-1	
	P	VD	WBN	EEB	08F802403-FD-2403-3	
	P	VD	WBN	EEB	08F802403-FD-2404-1	
	P	VD	WBN	EEB	08F802403-FD-2404-6	
	P	VD	WBN	EEB	08F802403-FD-2404-8	
	P	VD	WBN	EEB	08F802403-FD-2404-10	
	P	VD	WBN	EEB	08F802403-FD-2501-1	
	P	VD	WBN	EEB	08F802403-FD-2600-1	
	P	VD	WBN	EEB	08F802403-FD-2601-1	
	P	VD	WBN	EEB	08F802403-FD-2603-1	
	P	VD	WBN	EEB	08F802403-FD-2603-2	
	P	VD	WBN	EEB	08F802403-FD-2603-3	
	P	VD	WBN	EEB	08F802403-FD-2604-1	
	P	VD	WBN	EEB	08F802403-FD-2605-1	
	P	VD	WBN	EEB	08F802403-FD-2607-1	

CCRIS ONLY UPDATES:
Following are required only when making keyword/cross reference CCRIS updates and page 1 of form NEDP-2-1 is not included:

PREPARER SIGNATURE	DATE	CHECKER SIGNATURE	DATE
PREPARER PHONE NO.	EDMS ACCESSION NO.		

NPG CALCULATION COVERSHEET/CCRIS UPDATE

CALC ID	TYPE	ORG	PLANT	BRANCH	NUMBER	REV
	CN	NUC	WBN	EEB	DCSSEGMENT	000

ALTERNATE CALCULATION IDENTIFICATION

BLDG	ROOM	ELEV	COORD/AZIM	FIRM	Print Report Yes ☐
NA	NA	NA	NA	Bechtel	

CATEGORIES NA

KEY NOUNS (A-add, D-delete)

ACTION (A/D)	KEY NOUN	A/D	KEY NOUN

CROSS-REFERENCES (A-add, C-change, D-delete)

ACTION (A/C/D)	XREF CODE	XREF TYPE	XREF PLANT	XREF BRANCH	XREF NUMBER	XREF REV
	P	VD	WBN	EEB	08F802403-FD-2608-1	
	P	VD	WBN	EEB	08F802403-FD-2609-1	
	P	VD	WBN	EEB	08F802403-FD-2616-1	
	P	VD	WBN	EEB	08F802403-FD-2818-1	
	P	VD	WBN	EEB	08F802403-FD-2908-1	
	P	VD	WBN	EEB	08F802403-FD-2909-1	
	P	VD	WBN	EEB	08F802403-FD-2910-1	
	P	VD	WBN	EEB	2-65717-108D408-5	
	P	VD	WBN	EEB	2-65717-108D408-6	
	P	VD	WBN	EEB	108D408-23	
	P	VD	WBN	EEB	108D408-24	
	P	VD	WBN	EEB	108D408-25	
	P	VD	WBN	EEB	108D408-26	
	P	VD	WBN	EEB	108D408-27	
	P	VD	WBN	EEB	108D408-28	
	P	VD	WBN	EEB	108D408-31	
	P	VD	WBN	EEB	108D408-32	

CCRIS ONLY UPDATES:
Following are required only when making keyword/cross reference CCRIS updates and page 1 of form NEDP-2-1 is not included:

PREPARER SIGNATURE	DATE	CHECKER SIGNATURE	DATE
PREPARER PHONE NO.	EDMS ACCESSION NO.		

NPG CALCULATION COVERSHEET/CCRIS UPDATE

CALC ID	TYPE	ORG	PLANT	BRANCH	NUMBER	REV
	CN	NUC	WBN	EEB	DCSSEGMENT	000

ALTERNATE CALCULATION IDENTIFICATION

BLDG	ROOM	ELEV	COORD/AZIM	FIRM	Print Report Yes ☐
NA	NA	NA	NA	Bechtel	

CATEGORIES NA

KEY NOUNS (A-add, D-delete)

ACTION (A/D)	KEY NOUN	A/D	KEY NOUN

CROSS-REFERENCES (A-add, C-change, D-delete)

ACTION (A/C/D)	XREF CODE	XREF TYPE	XREF PLANT	XREF BRANCH	XREF NUMBER	XREF REV
	P	VD	WBN	EEB	108D408-33	
	P	VD	WBN	EEB	2-65717-108D408-36	
	P	VD	WBN	EEB	108D408-41	
	P	VD	WBN	EEB	2-54114-1-5655D87-9	
	P	VD	WBN	EEB	2-54114-1-5655D87-10	
	P	VD	WBN	EEB	2-54114-1-5655D87-11	
	P	VD	WBN	EEB	2-54114-1-5655D87-12	
	P	VD	WBN	EEB	2-54114-1-5655D87-13	
	P	VD	WBN	EEB	2-54114-1-5655D87-14	
	P	DW	WBN	EEB	1-47W610-1-1	
	P	DW	WBN	EEB	1-47W610-1-1A	
	P	DW	WBN	EEB	1-47W610-1-2	
	P	DW	WBN	EEB	1-47W610-1-2A	
	P	DW	WBN	EEB	1-47W610-1-3	
	P	DW	WBN	EEB	1-47W610-1-3A	
	P	DW	WBN	EEB	2-47W610-1-1	
	P	DW	WBN	EEB	2-47W610-1-1A	

CCRIS ONLY UPDATES:
Following are required only when making keyword/cross reference CCRIS updates and page 1 of form NEDP-2-1 is not included:

PREPARER SIGNATURE	DATE	CHECKER SIGNATURE	DATE
PREPARER PHONE NO.	EDMS ACCESSION NO.		

NPG CALCULATION COVERSHEET/CCRIS UPDATE

CALC ID	TYPE	ORG	PLANT	BRANCH	NUMBER	REV
	CN	NUC	WBN	EEB	DCSSEGMENT	000

ALTERNATE CALCULATION IDENTIFICATION

BLDG	ROOM	ELEV	COORD/AZIM	FIRM	Print Report Yes ☐
NA	NA	NA	NA	Bechtel	

CATEGORIES NA

KEY NOUNS (A-add, D-delete)

ACTION (A/D)	KEY NOUN	A/D	KEY NOUN

CROSS-REFERENCES (A-add, C-change, D-delete)

ACTION (A/C/D)	XREF CODE	XREF TYPE	XREF PLANT	XREF BRANCH	XREF NUMBER	XREF REV
	P	DW	WBN	EEB	2-47W610-1-2	
	P	DW	WBN	EEB	2-47W610-1-2A	
	P	DW	WBN	EEB	2-47W610-1-3	
	P	DW	WBN	EEB	2-47W610-1-3A	
	P	DW	WBN	EEB	1-47W610-3-1	
	P	DW	WBN	EEB	1-47W610-3-1A	
	P	DW	WBN	EEB	1-47W610-3-1B	
	P	DW	WBN	EEB	1-47W610-3-1C	
	P	DW	WBN	EEB	1-47W610-3-1D	
	P	DW	WBN	EEB	1-47W610-3-2	
	P	DW	WBN	EEB	1-47W610-3-2A	
	P	DW	WBN	EEB	1-47W610-3-2B	
	P	DW	WBN	EEB	1-47W610-3-2C	
	P	DW	WBN	EEB	1-47W610-3-3	
	P	DW	WBN	EEB	1-47W610-3-4	
	P	DW	WBN	EEB	1-47W610-3-5	
	P	DW	WBN	EEB	1-47W610-3-5A	

CCRIS ONLY UPDATES:
Following are required only when making keyword/cross reference CCRIS updates and page 1 of form NEDP-2-1 is not included:

PREPARER SIGNATURE	DATE	CHECKER SIGNATURE	DATE
PREPARER PHONE NO.	EDMS ACCESSION NO.		

NPG CALCULATION COVERSHEET/CCRIS UPDATE

CALC ID	TYPE	ORG	PLANT	BRANCH	NUMBER	REV
	CN	NUC	WBN	EEB	DCSSEGMENT	000

ALTERNATE CALCULATION IDENTIFICATION

BLDG	ROOM	ELEV	COORD/AZIM	FIRM	Print Report Yes ☐
NA	NA	NA	NA	Bechtel	

CATEGORIES NA

KEY NOUNS (A-add, D-delete)

ACTION (A/D)	KEY NOUN	A/D	KEY NOUN

CROSS-REFERENCES (A-add, C-change, D-delete)

ACTION (A/C/D)	XREF CODE	XREF TYPE	XREF PLANT	XREF BRANCH	XREF NUMBER	XREF REV
	P	DW	WBN	EEB	2-47W610-3-1	
	P	DW	WBN	EEB	2-47W610-3-1A	
	P	DW	WBN	EEB	2-47W610-3-1B	
	P	DW	WBN	EEB	2-47W610-3-1C	
	P	DW	WBN	EEB	2-47W610-3-1D	
	P	DW	WBN	EEB	2-47W610-3-2	
	P	DW	WBN	EEB	2-47W610-3-2A	
	P	DW	WBN	EEB	2-47W610-3-2B	
	P	DW	WBN	EEB	2-47W610-3-2C	
	P	DW	WBN	EEB	2-47W610-3-3	
	P	DW	WBN	EEB	2-47W610-3-4	
	P	DW	WBN	EEB	2-47W610-3-5	
	P	DW	WBN	EEB	2-47W610-3-5A	
	P	DW	WBN	EEB	1-47W610-62-1	
	P	DW	WBN	EEB	1-47W610-62-2	
	P	DW	WBN	EEB	1-47W610-62-3	
	P	DW	WBN	EEB	2-47W610-62-1	

CCRIS ONLY UPDATES:
Following are required only when making keyword/cross reference CCRIS updates and page 1 of form NEDP-2-1 is not included:

PREPARER SIGNATURE	DATE	CHECKER SIGNATURE	DATE
PREPARER PHONE NO.	EDMS ACCESSION NO.		

NPG CALCULATION COVERSHEET/CCRIS UPDATE

CALC ID	TYPE	ORG	PLANT	BRANCH	NUMBER	REV
	CN	NUC	WBN	EEB	DCSSEGMENT	000

ALTERNATE CALCULATION IDENTIFICATION

BLDG	ROOM	ELEV	COORD/AZIM	FIRM	Print Report Yes ☐
NA	NA	NA	NA	Bechtel	

CATEGORIES NA

KEY NOUNS (A-add, D-delete)

ACTION (A/D)	KEY NOUN	A/D	KEY NOUN

CROSS-REFERENCES (A-add, C-change, D-delete)

ACTION (A/C/D)	XREF CODE	XREF TYPE	XREF PLANT	XREF BRANCH	XREF NUMBER	XREF REV
	P	DW	WBN	EEB	2-47W610-62-2	
	P	DW	WBN	EEB	2-47W610-62-3	
	P	DW	WBN	EEB	1-47W610-68-1	
	P	DW	WBN	EEB	1-47W610-68-2	
	P	DW	WBN	EEB	1-47W610-68-3	
	P	DW	WBN	EEB	1-47W610-68-4	
	P	DW	WBN	EEB	1-47W610-68-5	
	P	DW	WBN	EEB	1-47W610-68-5A	
	P	DW	WBN	EEB	1-47W610-68-6	
	P	DW	WBN	EEB	1-47W610-68-8	
	P	DW	WBN	EEB	1-47W610-68-9	
	P	DW	WBN	EEB	1-47W610-68-10	
	P	DW	WBN	EEB	1-47W610-68-11	
	P	DW	WBN	EEB	2-47W610-68-1	
	P	DW	WBN	EEB	2-47W610-68-2	
	P	DW	WBN	EEB	2-47W610-68-3	
	P	DW	WBN	EEB	2-47W610-68-4	

CCRIS ONLY UPDATES:
Following are required only when making keyword/cross reference CCRIS updates and page 1 of form NEDP-2-1 is not included:

PREPARER SIGNATURE	DATE	CHECKER SIGNATURE	DATE
PREPARER PHONE NO.	EDMS ACCESSION NO.		

NPG CALCULATION COVERSHEET/CCRIS UPDATE

CALC ID	TYPE	ORG	PLANT	BRANCH	NUMBER	REV
	CN	NUC	WBN	EEB	DCSSEGMENT	000

ALTERNATE CALCULATION IDENTIFICATION

BLDG	ROOM	ELEV	COORD/AZIM	FIRM	Print Report Yes ☐
NA	NA	NA	NA	Bechtel	

CATEGORIES NA

KEY NOUNS (A-add, D-delete)

ACTION (A/D)	KEY NOUN	A/D	KEY NOUN

CROSS-REFERENCES (A-add, C-change, D-delete)

ACTION (A/C/D)	XREF CODE	XREF TYPE	XREF PLANT	XREF BRANCH	XREF NUMBER	XREF REV
	P	DW	WBN	EEB	2-47W610-68-5	
	P	DW	WBN	EEB	2-47W610-68-5A	
	P	DW	WBN	EEB	2-47W610-68-6	
	P	DW	WBN	EEB	2-47W610-68-8	
	P	DW	WBN	EEB	2-47W610-68-9	
	P	DW	WBN	EEB	2-47W610-68-10	
	P	DW	WBN	EEB	2-47W610-68-11	
	P	DW	WBN	EEB	1-47W611-1-1	
	P	DW	WBN	EEB	1-47W611-1-2	
	P	DW	WBN	EEB	2-47W611-1-1	
	P	DW	WBN	EEB	2-47W611-1-2	
	P	DW	WBN	EEB	1-47W611-3-1	
	P	DW	WBN	EEB	1-47W611-3-2	
	P	DW	WBN	EEB	1-47W611-3-6	
	P	DW	WBN	EEB	2-47W611-3-1	
	P	DW	WBN	EEB	2-47W611-3-2	
	P	DW	WBN	EEB	2-47W611-3-6	

CCRIS ONLY UPDATES:
Following are required only when making keyword/cross reference CCRIS updates and page 1 of form NEDP-2-1 is not included:

PREPARER SIGNATURE	DATE	CHECKER SIGNATURE	DATE
PREPARER PHONE NO.	EDMS ACCESSION NO.		

NPG CALCULATION COVERSHEET/CCRIS UPDATE

CALC ID	TYPE	ORG	PLANT	BRANCH	NUMBER	REV
	CN	NUC	WBN	EEB	DCSSEGMENT	000

ALTERNATE CALCULATION IDENTIFICATION

BLDG	ROOM	ELEV	COORD/AZIM	FIRM	Print Report
NA	NA	NA	NA	Bechtel	Yes ☐

CATEGORIES NA

KEY NOUNS (A-add, D-delete)

ACTION (A/D)	KEY NOUN	A/D	KEY NOUN

CROSS-REFERENCES (A-add, C-change, D-delete)

ACTION (A/C/D)	XREF CODE	XREF TYPE	XREF PLANT	XREF BRANCH	XREF NUMBER	XREF REV
	P	DW	WBN	EEB	1-47W611-62-1	
	P	DW	WBN	EEB	1-47W611-62-2	
	P	DW	WBN	EEB	1-47W611-62-3	
	P	DW	WBN	EEB	1-47W611-62-4	
	P	DW	WBN	EEB	2-47W611-62-1	
	P	DW	WBN	EEB	2-47W611-62-2	
	P	DW	WBN	EEB	2-47W611-62-3	
	P	DW	WBN	EEB	2-47W611-62-4	
	P	DW	WBN	EEB	1-47W611-68-1	
	P	DW	WBN	EEB	1-47W611-68-2	
	P	DW	WBN	EEB	1-47W611-68-3	
	P	DW	WBN	EEB	2-47W611-68-1	
	P	DW	WBN	EEB	2-47W611-68-2	
	P	DW	WBN	EEB	2-47W611-68-3	

CCRIS ONLY UPDATES:
Following are required only when making keyword/cross reference CCRIS updates and page 1 of form NEDP-2-1 is not included:

PREPARER SIGNATURE	DATE	CHECKER SIGNATURE	DATE
PREPARER PHONE NO.	EDMS ACCESSION NO.		

NPG CALCULATION RECORD OF REVISION

CALCULATION IDENTIFIER: **DCSSEGMENT**

Title **SEGMENTATION ANALYSIS FOR WBN UNIT 2 DCS**

Revision No.	DESCRIPTION OF REVISION
0	Initial issue for EDCR 52378 and related FCRs for installation of the Foxboro I/A distributed control system. Page Count: Main body of calculation (including 2a-2k) 36 Appendices A and B 19 and Attachments 3 Total pages 58 SAR changes submitted in support of EDCR 52378 were incorporated into the Unit 2 UFSAR Amendment 97. The need for additional SAR or Technical Specification changes will be evaluated in implementation of FCRs for EDCR 52378.

NPG CALCULATION VERIFICATION FORM

Calculation Identifier: **DCSSEGMENT** Revision 0

Method of verification used:

1. Design Review ☒
2. Alternate Calculation ☐
3. Qualification Test ☐

Verifier J.T. Kepler Date 7/29/10

Comments:

Comments: See Attachment 1, Design Verification Report and Checklist, 25402-3DP-G04G-00027-003 for calculation DCSSEGMENT R0.

NPG CALCULATION TABLE OF CONTENTS

Calculation Identifier: **DCSSEGMENT**	Revision:	0

TABLE OF CONTENTS

SECTION	TITLE	PAGE
	Coversheet	1
	Record of Revision	3
	Design Verification Form	4
	Table of Contents	5
1.0	Purpose	6
2.0	Sources of Design Inputs / References	6
3.0	Assumptions	9
4.0	DCS Design Description	10
5.0	Analysis	13
5.1	Feedwater/SG Level	15
5.2	Main Feedwater Pumps	16
5.3	SG PORVs	17
5.4	Rod Control	18
5.5	Steam Dump	19
5.6	Pressurizer Pressure	20
5.7	Pressurizer Level, Charging and Letdown	21
5.8	Volume Control Tank Level	23
5.9	BOP Turbine Runback	23
6.0	Conclusions	24
	Appendix A (Figures)	
	1. Shared Signals	
	2. Feedwater/SG Level	
	3. Feedwater Pumps	
	4. SG PORVs	
	5. Rod Control	
	6. Steam Dump	
	7. Pressurizer Pressure	
	8. Cold Overpressure Mitigation	
	9. Pressurizer Level	
	10. Volume Control Tank	
	Appendix B: Safety Analysis Review	
	Attachment 1: Design Verification Report	

1.0 Purpose

The existing analog control systems for WBN Unit 2 are being replaced with a Foxboro (Invensys) I/A Distributed Control System (DCS) for control and monitoring of most non-safety related NSSS and BOP systems. The controls are distributed among 15 control groups, each with a redundant processor pair. The purpose of this analysis is to evaluate the distribution (segmentation) of the inputs/outputs of those control systems important to plant operation among these control groups to confirm that no new failures are introduced which could adversely impact plant safety analyses.

2.0 Sources of Design Inputs / References

1. EDCR 52378, Replace Obsolete Non-Safety Analog NSSS and BOP Control Systems with a Foxboro I/A Distributed Control System
2. Invensys Letter INV-WBN2-802403-239 dated July 19, 2010, Drawing Submittal for post-FAT changes.
3. Design Criteria
   - A. WB-DC-40-70 R18, Accident Analysis Parameters Checklist
   - B. WB-DC-40-58 R5, Auxiliary Control System
4. Unit 2 UFSAR, Amendment 99
5. Unit 2 Technical Specifications
6. DG-E18.1.25 R2, Digital System Development, Procurement, and Implementation
7. Draft revision of "Effects of Common Cause Failure" prepared by Altran Solutions for the NRC Task Working Group on Defense-in-Depth & Diversity, August 2007
8. System Descriptions
   - C. WBN2-1-4002 R2, Main Steam System
   - D. WBN2-3A-4002 R2, Main Feedwater, Feedwater Control And Injection Water
   - E. WBN2-6-4002 R1, Heater Drains and Vents
   - F. WBN2-47-4002 R1, Turbogenerator System (Part 1) and Turbogenerator Control and Protection System (Part 2)
   - G. WBN2-62-4001 R1, Chemical And Volume Control System
   - H. WBN2-63-4001 R1, Safety Injection System
   - I. WBN2-68-4001 R0, Reactor Coolant System
   - J. WBN2-85-4003 R1, Control Rod Drive System
   - K. WBN2-92-4003 R1, Neutron Monitoring System
   - L. WBN2-99-4003 R0, Reactor Protection System
9. Foxboro Functional Diagrams (contract 69247)
   - A. 08F802403-FD-2004-1 R2

B. 08F802403-FD-2005-1 R3
C. 08F802403-FD-2006-1 R3, -2 R2, -4 R3, -5 R4
D. 08F802403-FD-2012-1 R4
E. 08F802403-FD-2101-1 R2, -4 R2
F. 08F802403-FD-2102-1 R3
G. 08F802403-FD-2103-1 R2, -3 R2
H. 08F802403-FD-2104-1 R4, -3 R3
I. 08F802403-FD-2105-1 R3, -2 R3, -4 R2
J. 08F802403-FD-2107-1 R3, -2 R3, -4 R2
K. 08F802403-FD-2109-1 R2, -2 R2
L. 08F802403-FD-2110-1 R3
M. 08F802403-FD-2111-1 R3, -2 R2
N. 08F802403-FD-2201-1 R5
O. 08F802403-FD-2202-1 R6
P. 08F802403-FD-2203-1 R4
Q. 08F802403-FD-2205-1 R6, -2 R6
R. 08F802403-FD-2300-1 R3, -6 R3
S. 08F802403-FD-2301-1 R2, -6 R3
T. 08F802403-FD-2302-1 R2, -6 R3
U. 08F802403-FD-2303-1 R2, -6 R3
V. 08F802403-FD-2304-1 R5, -3 R2, -4 R2, -8 R4, -9 R4, -10 R2
W. 08F802403-FD-2400-1 R5, -3 R5, -5 R4, -6 R5, -7 R4
X. 08F802403-FD-2401-1 R7, -5 R5, -6 R5, -12 R0
Y. 08F802403-FD-2402-1 R5, -3 R6
Z. 08F802403-FD-2403-1 R5, -3 R4
AA. 08F802403-FD-2404-1 R6, -6 R7, -8 R6, -10 R7
BB. 08F802403-FD-2501-1 R2
CC. 08F802403-FD-2600-1 R3
DD. 08F802403-FD-2601-1 R4
EE. 08F802403-FD-2603-1 R4, -2 R4, -3 R5
FF. 08F802403-FD-2604-1 R3
GG. 08F802403-FD-2605-1 R5
HH. 08F802403-FD-2607-1 R4

II. 08F802403-FD-2608-1 R5

JJ. 08F802403-FD-2609-1 R4

KK. 08F802403-FD-2616-1 R3

LL. 08F802403-FD-2818-1 R3

MM. 08F802403-FD-2908-1 R3

NN. 08F802403-FD-2909-1 R4

OO. 08F802403-FD-2910-1 R4

10 Control Drawings

A. 1-47W610-1-1 R30, -1A R16, -2 R29, -2A R20, -3 R10, -3A R7

B. 2-47W610-1-1 R2, -1A R2, -2 R2, -2A R2, -3 R1, -3A R0

C. 1-47W610-3-1 R28, -1A R6, -1B R11, -1C R4, -1D R7, -2 R19, -2A R18, -2B R3, -2C R8, -3 R22, -4 R17, -5 R18, -5A R9

D. 2-47W610-3-1 R1, -1A R0, -1B R0, -1C R0, -1D R1, -2 R0, -2A R1, -2B R0, -2C R1, -3 R2, -4 R1, -5 R1, -5A R1

E. 1-47W610-62-1 R21, -2 R24, -3 R25

F. 2-47W610-62-1 R1, -2 R3, -3 R0

G. 1-47W610-68-1 R18, -2 R15, -3 R21, -4 R18, -5 R22, -5A R4, -6 R12, -8 R8, -9 R5, -10 R5, -11 R9

H. 2-47W610-68-1 R0, -2 R0, -3 R1, -4 R1, -5 R1, -5A R1, -6 R1, -8 R0, -9 R0, -10 R0, -11 R0

11 Logic Drawings

A. 1-47W611-1-1 R13, -2 R12

B. 2-47W611-1-1 R1, -2 R1

C. 1-47W611-3-1 R12, -2 R22, -6 R18

D. 2-47W611-3-1 R2, -2 R3, -6 R1

E. 1-47W611-62-1 R6, -2 R8, -3 R9, -4 R11

F. 2-47W611-62-1 R1, -2 R1, -3 R1, -4 R1

G. 1-47W611-68-1 R10, -2 R7, -3 R8

H. 2-47W611-68-1 R1, -2 R1, -3 R1

12 Westinghouse Functional Diagrams, 5655D87 series (contract 54114-01)

A. 2-54114-1-5655D87-9 R0

B. 2-54114-1-5655D87-10 R0

C. 2-54114-1-5655D87-11 R0

D. 2-54114-1-5655D87-12 R0

E. 2-54114-1-5655D87-13 R0

F. 2-54114-1-5655D87-14 R0

13 Westinghouse Process Control Block Diagrams, 108D408 series (contract 54114-01 and 65717)

A. 108D408-5 RE, 2-65717-108D408-5 R0

B. 108D408-6 RE, 2-65717-108D408-6 R0

C. 108D408-23 RF

D. 108D408-24 RE

E. 108D408-25 RD

F. 108D408-26 RD

G. 108D408-27 RE

H. 108D408-28 RD

I. 108D408-31 RD

J. 108D408-32 RD

K. 108D408-33 RF

L. 108D408-36 RF, 2-65717-108D408-36 R0

M. 108D408-41 RD

14 Calculation EPMFBN072892 R3, "Maximum Feedwater Flow for Multiple Loop Failures."

15 NPG Critical Digital Review of the Foxboro I/A Series Platform (B43 090303 001)

3.0 Assumptions

1. Unverified assumption: The post-FAT functional logic changes submitted in reference 2 and evaluated in this calculation will be implemented by EDCR 52378 (reference 1) via FCR 55490.

2. Unverified assumption: A network data storm test will be performed with the system installed and prior to final commissioning. The test will confirm that the system will continue to function with a failed communication network without any plant upset.

4.0 DCS Design Description

The functional design of the WBN unit 2 control systems implemented in the DCS is similar to unit 1 but with changes which improve reliability and eliminate many significant single points of failure. The basic components of the DCS are redundant fault-tolerant processor pairs, redundant power supplies with diverse power sources, redundant communication networks, and redundant operator workstations. Redundant field-bus modules (FBMs) are utilized for critical inputs and outputs. The system is designed such that the control system functions most important to safe plant operation are not affected by the failure of a single device or component.

Functional Groups (CP Pairs)

The unit 2 DCS consists of 15 functional groups, each with a redundant control processor (CP) pair. This arrangement provides capability to maintain independence between redundant control functions and to limit the effects of failures on the critical control systems.

Table 1 identifies the primary functions of each of the DCS functional groups. Each group also includes other control and monitoring functions for which segmentation is not considered to be necessary as further discussed in section 5.0.

Table 1
FUNCTIONAL GROUPS

Group (CP Pair)	Primary Functions
01	Steam Generator 1 Level, FW Flow
02	Steam Generator 2 Level, FW Flow
03	Steam Generator 3 Level, FW Flow
04	Steam Generator 4 Level, FW Flow
05	Main FW Pump Speed Control & Steam Dump Loss of Load Interlock
06	Rod Control
07	Steam Generator 1 PORV (Atmospheric Dump)
08	Steam Generator 2 PORV (Atmospheric Dump)
09	Steam Generator 3 PORV (Atmospheric Dump)
10	Steam Generator 4 PORV (Atmospheric Dump)
11	Condenser Steam Dump
12	Pressurizer A (Pressure, Level, Charging, Letdown, Spray, COMS)
13	Pressurizer B (Pressure, Level, Charging, Letdown, Spray, COMS)
14	Auxiliary Control System A
15	Auxiliary Control System B

Auxiliary Control System

Groups 14 and 15 are dedicated to the Auxiliary Control System (ACS) which is not required for normal plant operation. The ACS provides controls and instrumentation needed for plant shutdown from outside the Main Control Room (MCR) in the event that the MCR has to be abandoned. Isolation of the ACS from the normal controls is achieved either by dedicated control loops or by manually-operated transfer switches. The safety related functions of the ACS are implemented independently of the DCS. Groups 14 and 15 are isolated from the network during normal operation, except for maintenance purposes, to eliminate the possibility of events external to the auxiliary control room causing loss of these processor pairs.

Segmentation of the DCS functions of the ACS is not evaluated in this analysis since the ACS is not used for normal plant operation, DCS groups 14 and 15 are isolated from the network during normal operation, the unit will be shut down if the MCR has to be abandoned, and no other design basis event or abnormal plant condition is assumed concurrent with MCR evacuation except fire or design basis flood (reference 3B).

Power Supplies

Each of the redundant power supplies for the control groups is fed from an inverter with battery and emergency diesel generator backup - typically the primary power supply from a 120 VAC Vital Inverter and the secondary from the 120 VAC TSC Inverter. This arrangement ensures that a single power supply or inverter failure will not result in loss of function, eliminating loss of power as a single point of failure. One significant benefit of this configuration is that an inverter failure will not cause a plant trip due to the main feedwater control valves closing.

Signal Selection and Validation

The use of multiple measurement channels for critical parameters such as turbine impulse pressure, steam header pressure, and feedwater pressure allows the use of various signal selectors to improve reliability and eliminate single point failures. Redundant inputs are typically assigned to different input modules to provide additional hardware diversity and eliminate hardware common cause failure.

A median signal selector chooses the median value signal of three inputs for control use. With the median signal selector, a spurious high or low signal from any one channel will not cause a control action. Where only two inputs are available, an average is computed, and a third correlated signal may be provided as a voter. The voter is never used for control. With four inputs, either the highest input (auctioneered) or the second highest input (higher median) is selected for control. The high quality of the median signal selector is documented in reference 15 of section 3.6.

The system also employs signal validation techniques which can remove bad or out-of-service signals from the algorithm and select from the remaining good signals or transfer control to manual in the event of multiple input signal failures. This includes input signals which deviate significantly from the selected signal (auctioneered or

median). These conditions will be alarmed and the bad signal removed from the control algorithm. Use of these techniques eliminates the potential for a transient initiated by the failure of a single input.

Shared Signals

The signals listed in Table 2 are used in more than one functional group or processor pair. They may be provided to each processor as separate inputs, or they may be input to one processor for development of the control signal (auctioneered, median, etc.) which is then transmitted to other processors by either a hardwired analog connection, peer-to-peer network connection or both. No critical control function is dependent upon the network alone. This scheme eliminates the possibility that failure of a single input signal, a single processor pair, or both communication networks will disable multiple control systems or functions.

Figure 1 shows how these input signals or the derived control signals are distributed among multiple processor pairs. Simplified configuration sketches based on the referenced functional logic diagrams are shown in Figures 2 through 10.

External Communication

Two communication links are provided from the DCS to the plant computer. Firewalls between the systems limit the volume of data traffic and ensure that common cause events, such as a data storm, do not impact multiple control systems within the DCS.

There is no digital communication between the control system and the protection system. The control system analog process inputs from the protection system are transmitted via qualified isolators as on unit 1.

Network Data Storm

The impact of erroneous communication internal to the system, such as a data storm due to a processor failure, will be evaluated by test. A Sequoyah factory acceptance test for a Foxboro I/A DCS demonstrated that a data storm can disable the communication networks and cause one CP of a pair to become non-functional. The control groups, however, continued to operate. The network is disabled only during the datastorm event and full system redundancy can be restored by an online reboot of the secondary CP. A data storm test will be performed with the installed WBN Unit 2 system prior to final commissioning to confirm similar results. Further, as noted previously, the system is designed with hardwired analog control signal transmission between CP pairs so that no critical control functions are totally dependent upon the network and the system will continue to function if the network fails.

Table 2
SHARED SIGNALS

Parameter	Loops	Function
Turbine Impulse Press	2-P-1-72 *	Rod Control, Steam Dump, Turb Runback
Turbine Impulse Press	2-P-1-73 *	Rod Control, Steam Dump, Turb Runback
Turbine Impulse Press	2-PT-1-74	Rod Control, Steam Dump, Turb Runback
Turbine Impulse Press	2-PT-1-81	Rod Control, Steam Dump, Turb Runback
RCS Loop 1 Tavg	2-T-68-2 *	Rod Control, Steam Dump, Pzr Level
RCS Loop 2 Tavg	2-T-68-25 *	Rod Control, Steam Dump, Pzr Level
RCS Loop 3 Tavg	2-T-68-44 *	Rod Control, Steam Dump, Pzr Level
RCS Loop 4 Tavg	2-T-68-67 *	Rod Control, Steam Dump, Pzr Level
NIS Reactor Power Ch I	2-LP-92-412 *	Rod Control, SG Level
NIS Reactor Power Ch II	2-LP-92-412 *	Rod Control, SG Level
NIS Reactor Power Ch III	2-LP-92-412 *	Rod Control, SG Level
NIS Reactor Power Ch IV	2-LP-92-412 *	Rod Control, SG Level
Pressurizer Press	2-P-68-322 *	Pressurizer Pressure
Pressurizer Press	2-P-68-323 *	Pressurizer Pressure
Pressurizer Press	2-P-68-334 *	Pressurizer Pressure
Pressurizer Press	2-P-68-340 *	Pressurizer Pressure
Pressurizer Level	2-L-68-320 *	Pressurizer Level
Pressurizer Level	2-L-68-335 *	Pressurizer Level
Pressurizer Level	2-L-68-339 *	Pressurizer Level
Steam Header Press	2-PT-1-33A	Steam Dump, MFP Speed Control
Steam Header Press	2-PT-1-33B	Steam Dump, MFP Speed Control
Steam Header Press	2-PT-1-33C	Steam Dump, MFP Speed Control
Steam Flow Loop 1	2-F-1-3A, 3B *	SG 1 Level, MFP Speed Control
Steam Flow Loop 2	2-F-1-10A, 10B *	SG 2 Level, MFP Speed Control
Steam Flow Loop 3	2-F-1-21A, 21B *	SG 3 Level, MFP Speed Control
Steam Flow Loop 4	2-F-1-28A, 28B *	SG 4 Level, MFP Speed Control
Volume Control Tank Level	2-LT-63-129A	VCT Level
Volume Control Tank Level	2-LT-63-130A	VCT Level

* Input signals from isolated protection system channels.

5.0 Analysis

Control systems which are important to safe plant operation and can affect the plant safety analyses and for which segmentation is necessary or can provide a significant benefit are evaluated in the sections following. Some functions, while important to plant operation, do not lend themselves to or would not be significantly improved by segmentation of inputs and outputs and are not evaluated.

The analysis verifies that no new control system failures are introduced which could adversely impact the safety analyses as described in the FSAR and WB-DC-40-70, Accident Analysis Parameters Checklist. Typically, the control systems are assumed to function only if their operation contributes to more severe accident results. The control

systems evaluated in this analysis are not credited for accident mitigation but their availability can enhance the plant response to an event. The focus of this safety analysis review then is to identify configurations wherein failure of a CP pair could result in plant conditions which are more limiting than those analyzed in the safety analysis. The results of this review are provided in Appendix B and the control system discussions following.

Design basis documents including design criteria, system descriptions and drawings were reviewed for functional and configuration requirements to minimize differences with unit 1 with respect to functional diversity and independence. The unit 1 design limits the effects of a component failure or loss of power by providing redundant hardware and power sources for certain functions. For example, the pressurizer heaters can be turned off by either of two independent channels which have different power sources. Maintaining this approach for unit 2 will limit the effects of failures and requires that certain functions be processed in different CP pairs. Segmentation of important control systems and functions improves availability of these systems for both normal operation and transient/accident response.

The configuration of signals which are shared by more than one control system or functional group are also evaluated to verify that loss of any one signal or processor pair will not cause an unacceptable loss of multiple functions.

Simplified functional logic sketches are provided in Appendix A. These figures are based on the Foxboro functional diagrams listed in reference 9.

Failure Modes

For this analysis, the unlikely failure of both processors of a redundant pair is assumed, with all outputs failing high, low or as-is. Failures resulting in output state changes are recognizable by their effects, e.g., plant components changing state or indicators going off-scale high or low. As-is failures are not likely to have an immediate effect and therefore would not result in a transient; but they may remain undetected until there is a demand failure or until a process parameter exceeds its normal range and actuates an alarm.

The following design and implementation strategies provide reasonable assurance of adequate protection against a common cause failure affecting multiple processor pairs:

- defensive design techniques including multiple processor pairs running asynchronously with different application software, deterministic software programs, redundant hardware and communication paths, system diagnostics, input signal redundancy and functional segmentation;
- design reviews performed during the design process, including a critical design review of the Foxboro I/A platform (reference 15);
- software quality assurance;
- testing before and after installation, i.e., factory and site acceptance tests, startup tests;
- hardware and software configuration control during the design phase and after installation.

Based on the above considerations, simultaneous failure of more than one processor pair and multiple smart combinations of failure states such as high and low are not considered. This approach is supported by reference 7 and is consistent with the guidelines of reference 6 and with the nuclear industry position.

5.1 Feedwater / SG Level

One control processor pair is provided for level control for each steam generator so that a single processor pair failure will not cause more than one SG level control system failure. The controls for SGs 1-4 are located in processors CP01, CP02, CP03, and CP04, respectively. Three water level signals per steam generator are provided via isolated Eagle 21 outputs to the respective processors for control of both the feedwater regulating valves and the feedwater bypass regulating valves. A median signal selector function in the DCS provides a median signal for control use similar to unit 1 except the unit 1 MSS is implemented with hardware and unit 2 with software.

Two feedwater flow signals and two steam flow signals per loop are also provided to the respective SG level control processors. The DCS calculates an average of the two inputs for each variable for input to the controller. If one channel of feedwater flow or one channel of steam flow fails, a voter signal will determine which of the two channels should be used for control. The voter signal is the average of the feedwater flows of the other steam generators. The voter is not used for control. On unit 1 a single channel each of feedwater flow and steam flow are manually selected for control so that operator intervention is required if the selected channel fails or is to be tested. The average steam flow signals are transmitted from each SG level control processor to CP05 to develop the speed control setpoint for the main feedwater pumps.

The steam generator level setpoints for both the main and bypass feedwater regulating valves are generated from the second highest value (high median select) of the four NIS power inputs. Using the higher median signal prevents a single input failure from causing a spurious SG level setpoint change. On unit 1, the programmed level setpoints for loops 1 and 4 are derived from a single NIS channel I module and the setpoints for loops 2 and 3 are similarly derived from NIS channel II. A single input channel or module failure could cause a disturbance on two SG loops. The unit 1 bypass valves controllers also have a bias input from auctioneered high NIS. During low power operation with the bypass valves in auto, a single failure could result in all four bypass valves opening.

The unit 2 level demand signal (NIS power high median) is developed in CP06 (Rod Control). The signal is transmitted independently to each of the four SG level processors by a hardwired connection and also by a peer-to-peer network interface. The programmed level setpoint for each SG is developed in each of the SG level control processors independently of the others except for the common demand signal from CP06. See Figure 2.

Since all four SG level control processors are dependent on CP06 for the level demand, a failure of this processor could affect the level controls for all SGs. However,

the level setpoint algorithm in each of the level control processors limits the setpoint to the range of 38-60% (the no load and full load values). Each of the level control processors contains diagnostics which will detect failure of the level demand inputs and will then freeze the setpoint to the last good value and switch control to manual. This will give operators time to respond before a significant transient is initiated.

At full power, a high failure of the NIS level demand signal from CP06 would not result in any change in SG levels because of the setpoint high limit (60%). At less than full power, the level program would open the feedwater regulating valves to increase SG levels to the high limit. This condition is less severe than the cases evaluated in the "Excessive Heat Removal Due to Feedwater System Malfunction" event described in FSAR section 15.2.10. The analysis considered four cases to be limiting:

1. Accidental opening of one feedwater control valve with the reactor at zero load.
2. Accidental opening of all feedwater control valves with the reactor at zero load.
3. Accidental opening of one feedwater control valve with the reactor at full power.
4. Accidental opening of all feedwater control valves with the reactor at full power.

The analysis concluded that the hot zero power feedwater malfunction is bounded by the hot full power feedwater malfunction. The event is terminated by the steam generator high-high level signal, which closes all feedwater control and isolation valves and trips the main feedwater pumps. The cases assuming all the valves fully open bound the conditions resulting from a high failure of CP06.

Similarly, in response to a low failure of the NIS level demand signal from CP06, the level control system would reduce flow by closing the feedwater valves to match SG levels to the demand value. The system response to this failure is constrained by the low limit on the setpoints (38%). This failure is bounded by the "Loss of Normal Feedwater" event described in FSAR Section 15.2.8.

A failure of one SG level control CP could result in both the main and bypass valves either opening or closing depending on the signals failing high or low. Both these cases are bounded by the analyses as described above.

TVA calculation EPMFBN072892 (reference 14) evaluates feedwater system failures at different power levels to determine the maximum feedwater flows for single and multiple loop failures. In each case the calculation assumes both the main and bypass valves in the failed loop to be wide open instead of in their normal zero or full power position, providing conservatively maximum flow results. The results of this calculation were used as input to the FSAR feedwater malfunction analysis discussed above. The FSAR cases analyzed bound those evaluated in the calculation.

5.2 Main Feedwater Pumps Speed Control

The feedwater pump speed controls in CP05 utilize median signal selectors for three feedwater header pressure (feedwater pump discharge) inputs and three main steam header pressure inputs. Use of the MSS eliminates the potential for a transient initiated by a single transmitter failure as on unit 1. The feedwater pump programmed DP

setpoint is a function of the four-loop average of the loop steam flows with each loop flow being the average of two flow measurements from the respective SG control processor (CP01, CP02, CP03, CP04). The average loop flow for each SG is transmitted to CP05 via the network. The SG 1 and SG 2 flows are also hardwired to provide additional reliability. Failure of the steam flow inputs from two or more SGs, including complete loss of the networked inputs, will freeze the DP setpoint at the last good value. See Figure 3.

Redundant DCS modules provide 4-20 mA speed demand outputs for each MFP. The signals are converted to 10-50 mA and auctioneered before being transmitted to each MFP speed changer. Both the DCS output modules and the external signal converters are current limited. A high failure of a pump speed demand output (such as from a processor pair failure) would result in increased feedwater flow.

The feedwater flow values used in the maximum feedwater flow calculation (reference 14) discussed in the previous section are conservatively large values which in the limiting case are beyond the guaranteed pump operating range and may be at the run-out range as noted in the calculation. Thus, even if a MFP speed control processor failure caused both MFPs to go to the maximum speed allowed by the speed changers and approach runout, the results would still be bounded by the maximum feedwater flow analysis of reference 14 and the FSAR feedwater malfunction analysis. In addition, the level control systems would continue to maintain the desired SG levels by adjusting the feedwater regulating valves.

Low failure of a pump speed demand output would result in decreased feedwater flow and subsequent drop in SG level. This condition is bounded by the Loss of Normal Feedwater event described in FSAR Section 15.2.8.

5.3 SG PORVs

The SG PORVs provide capability for SG pressure control and for a controlled plant cooldown when the condenser steam dump system is not available. The controls for each of the SG PORVs are in separate processors, CP07, CP08, CP09, and CP10, so that only one PORV control system will be affected by a processor pair failure. Steam dump control is assigned to CP11. Each PORV control has three steam pressure inputs from the corresponding steam line, two of which are from isolated Eagle 21 outputs. The median of three steam pressure signals in each CP is input to the PORV controller. See Figure 4. The unit 1 PORV controls have only one pressure input.

The SG PORVs should be available to dump excess steam generated from a loss of load or turbine trip event (FSAR 15.2.7 and reference 3.A section 4.1.7) if the condenser is not available. Separation of the controls for the PORVs and the steam dumps maximizes the availability of steam relief for a single CP failure. In addition, a discrete high pressure output is provided from the steam pressure median signal in each CP to open the PORV when the rate of pressure increase is greater than the controller's capability to control. On unit 1 this interlock is performed by a single mechanical pressure switch.

Inadvertent opening of a SG relief valve is identified as an initiator in the analysis of the Accidental Depressurization of Main Steam event in FSAR section 15.2.13 and described in reference 3.A section 4.1.12. With the SG PORV controls in separate processors, no single CP failure will result in more than one PORV opening. Safety related controls independent of the DCS are available to close a PORV opened by a control system failure.

The safety analyses credit the main steam safety valves for pressure relief for events involving significant pressure increases where the PORVs may be unable to control the pressure increase, such as a load rejection with steamline isolation, or if a PORV fails to open. Safety-grade manual controls are available for control of the PORVs if needed.

5.4 Rod Control

The reactor control system controls reactor power by maintaining reactor coolant average temperature to within ± 3.5°F of the programmed temperature. The system is designed to automatically control the reactor in the range of 15-100 percent of rated power for the following design transients:

- 10 percent step change in load or a ramp increase or decrease of 5 percent/minute without reactor trip, steam dump, or pressurizer relief actuation.
- 50 percent step load decrease without reactor trip (10% control rods, 40% steam dump).

The reactor control signal consists of an error signal used to determine rod speed and position (direction) to maintain programmed Tavg. The two channels used to generate the total error signal are the deviation of the primary coolant average temperature (Tavg) from the programmed average temperature (Tref) and the mismatch between turbine load and nuclear power. The Tavg control signal is the auctioneered highest value of the four loop Tavg inputs from Eagle 21. The Tref signal is generated from the second highest of four turbine impulse pressure signals as determined by a higher median signal selector in the DCS. The Tref signal should be more reliable than unit 1 where it is derived from a single channel.

The error between Tref and Tavg constitutes the primary control signal for rod control. The power mismatch signal improves system performance by enhancing response and reducing transient peaks. The control system maintains Tavg within prescribed limits during normal operation and anticipated operational transients and is capable of restoring coolant average temperature to the programmed value following a change in load.

Turbine load is also represented by the Tref signal. The nuclear power input to the power mismatch circuit is derived from the auctioneered highest of the four NIS power range signals. A second nuclear power signal, the higher median value (2nd highest), is developed for input to the SG level control systems (section 5.1). A channel deviation alarm will be generated if any NIS input deviates significantly from the higher

median value and that input will not be used in the algorithm. The output will be frozen if two or more input signals are determined to be bad.

The Tavg, Tref and nuclear power signals derived in CP06 for use in the rod control system are also used for other control functions. The auctioneered Tavg signal is sent to CP11 for steam dump control (section 5.5) and to CP13 for pressurizer level control (section 5.7). Tref is transmitted to CP11 for steam dump control and to CP05 for the steam dump loss of load interlock. The higher median nuclear power signal is transmitted independently to each of the four SG level control systems in CP01, CP02, CP03 and CP04 as described in section 5.1. See Figure 5.

Since control is based on the highest of the loop average temperatures, control rod position is based upon the most limiting temperature measurement with respect to DNB margins. A spurious low average temperature signal from any loop Tavg channel will cause no control action. Depending on the magnitude, a spurious high average temperature signal could cause rod insertion (safe direction) or may be removed from the algorithm if it deviates excessively from the next highest signal. A channel deviation alarm will be generated by the DCS if any of the Tavg inputs deviates significantly from the auctioneered (highest) value. Operators can block any Tavg channel from control use with the Tavg defeat switch on the main control board or via an operator work station.

Failure of the CP06 outputs could cause rod insertion or withdrawal similar to the analog system failures on unit 1. The control rod drive system (not part of the DCS) is designed such that no more than two banks can be withdrawn at any time. The FSAR section 15.2.2 analysis of an Uncontrolled Rod Cluster Control Assembly Bank Withdrawal at Power, which assumes the simultaneous withdrawal of two banks at maximum speed, remains bounding for unit 2 DCS failures. Rod withdrawal blocks originate from systems external to the DCS.

Rod control and the control systems with which it shares control signals (steam dump, pressurizer level and SG level) are segregated such that failure of CP06 will not disable more than one of these systems.

5.5 Steam Dump

The condenser steam dump system assists in mitigating a load reduction to reduce the effects of the transient imposed on the RCS. As noted previously, the SG PORVs provide capability for SG pressure control and for a controlled plant cooldown when the condenser steam dump system is not available. Therefore, the steam dump controls are assigned to CP11, while the SG PORVs are in CP07, CP08, CP09, and CP10.

Redundant pressure inputs are provided for the steam pressure mode. The median of three steam header pressure channels in CP05 (MFP Speed control) is provided to CP11 by both hardwired and networked connections. One of these three pressure channels is also hardwired as an input to CP11 so that steam dump control in the steam pressure mode is not disabled by failure of CP05.

Turbine impulse pressure, which is representative of turbine load, is used to generate the programmed reference average coolant temperature (Tref) as described previously. The Tref input to steam dump control is the higher median of four turbine impulse pressure signals input to the rod control processor pair CP06. Tref is an input to the load rejection controller and the load rejection bistables which trip on excessive deviation between Tavg and Tref. The Tavg input to steam dump is the auctioneered high Tavg signal, also developed in CP06.

The Tref and Tavg signals are transmitted from CP06 to CP11 by both hardwired and networked connections to improve signal reliability. Due to the upper and lower range limits applied to these signals within CP11, failure of the Tavg and Tref outputs from CP06 would be less severe than failure of the CP11 outputs and similar to failure of a single module in unit 1.

To prevent actuation of steam dump on small load perturbations, an independent load rejection circuit (C-7) is provided in the DCS. This circuit senses the rate of decrease in the turbine load as detected by the turbine impulse pressure. C-7 is an arming interlock which will unblock the dump valves when the rate of load rejection exceeds a preset value corresponding to a 10% step load decrease. Independence is accomplished by providing one of the turbine impulse pressure inputs to a second processor pair, CP05, to generate the C-7 permissive. If the turbine impulse pressure input to C-7 came from the same processor as Tref, a low failure of one processor could both arm the dump valves and actuate the trip outputs, opening all of the valves. Providing a redundant input to C-7 in a different processor prevents a failure of CP11 from causing all of the steam dump valves to open when at full load, resulting in a rapid depressurization of the main steam system. See Figure 6.

The basis for this design is the consideration of steam dump failures in two analyzed events: Excessive Load Increase (FSAR section 15.2.11) and Accidental Depressurization of Main Steam (FSAR section 15.2.13). These analyses assume the inadvertent opening of a steam dump, relief or safety valve. Maintaining functional independence between the C-7 loss-of-load interlock and Tref as described above ensures that the analyses remain bounding. These events are further described in reference 3.A sections 4.1.10 and 4.1.12.

5.6 Pressurizer Pressure

The pressurizer maintains reactor coolant system pressure during operation and can accommodate certain transients without reactor trip. The pressurizer controls are divided into two groups, identified as Pressurizer A (PRZA) and Pressurizer B (PRZB), which utilize separate processor pairs, CP12 and CP13. Each processor receives inputs from two of the four pressurizer pressure channels via isolated outputs from Eagle 21. An average of the two inputs in each CP is transmitted via the network to the other CP pair and a median signal is developed in each processor. The median signal in PRZA (CP12) is input to a master controller whose output is used for control of the pressurizer spray valves and the variable and backup heaters. Figure 7 is a simplified sketch of the principal pressurizer control features.

The spray valves controllers are assigned to different CPs to provide functional diversity. The spray valve controller in PRZB (CP13) receives its input from the master controller via both the network and a hardwired connection. The median signals from both CPs are used for redundant actuation of the pressurizer power-operated relief valves (PORVs).

The unit 1 configuration has the controllers for the spray valves and the variable heater driven from the master controller output so that failure of or loss of power to the master controller would result in loss of the automatic control of these functions. However the unit 1 spray valve control stations in the main control room (MCR) are independent of the master controller in the manual mode and are powered from a different power source. The unit 2 DCS hand-auto stations in the MCR, however, will not function if the CP fails. Placing one spray valve controller and associated hand-auto station in PRZB (CP13) maintains manual control capability for at least one spray valve if one of the pressurizer CPs fails. Both the variable and backup heaters can be operated independently of the DCS from the MCR. Diverse spray isolation valve controls are provided external to the DCS if needed.

The pressurizer PORVs limit system pressure during a large power mismatch to a value below the high pressure reactor trip setpoint for transients up to and including a 50% step load decrease with steam dump actuation. A coincident high pressure signal from two independent channels (one from each processor) is needed for the actuation of each PORV. The PORVs also limit undesirable opening of the pressurizer safety valves. Condenser steam dumps and atmospheric steam dumps are controlled by different processor pairs than the pressurizer PORVs.

A spurious high or low control signal resulting from failure of CP12 can cause both spray valves to open or close and heaters to turn on or off as described above. A spurious high signal can cause decreasing pressure by turning off the heaters and actuating spray. Failure of a single CP will not cause spurious opening of a PORV since coincident high pressure signals are required from both processors.

A spurious low signal can cause increasing pressure by turning on the heaters and turning off spray. The rate of pressure rise achievable with heaters is slow, and ample time and pressure alarms are provided to alert the operator of the need for appropriate action. In addition, operation of either PORV can maintain pressure below the high pressure trip setpoint for most transients. No credit is taken for the relief capability provided by the PORVs during a pressure surge.

Cold Overpressure Mitigation System (COMS)

Two independent sets of controls are provided for mitigation of RCS overpressure events (e.g., inadvertent ECCS actuation) during low temperature operation. Each of two processor pairs, CP12 and CP13, receives signals from redundant channels of wide range RCS pressure and temperature via isolated outputs from Eagle 21. Each processor provides an output to open one PORV if necessary to prevent pressure from exceeding allowable limits. The actuation logic is manually armed (unblocked) external to the DCS when plant operation is at a temperature below the arming setpoint.

Manual arming prevents a spurious PORV opening due to a processor failure whenever the RCS temperature is above the arming temperature. In lower modes COMS will open the PORVs. See Figure 8.

5.7 Pressurizer Level, Charging and Letdown Flow

RCS inventory is maintained by controlling charging and letdown flows to keep the pressurizer at programmed level as a function of the average reactor coolant temperature (Tavg). A portion of the charging flow is provided to the reactor coolant pump (RCP) seals.

Consistent with the unit 1 design, the unit 2 design for pressurizer level control incorporates redundancy for letdown isolation and pressurizer heater protection. Two processor pairs, CP12 and CP13, receive inputs from three pressurizer level channels via isolated outputs from Eagle 21. Two channels are input to CP13; the third is input to CP12. The third channel is then networked to CP13, where a median signal is developed. The median signal in CP13, with the programmed level input from auctioneered high Tavg (from CP06), provides the setpoint to the charging flow controller in CP13. A low level output from either CP12 or CP13 will close the letdown isolation valves and shutoff the heaters. See Figure 9. The controllers for pressurizer pressure and pressurizer level (via charging flow) are in different CPs, providing additional diversity.

A spurious high or low control signal resulting from failure of CP13 can cause an increase or decrease in charging flow and a slow change in pressurizer level. The high pressurizer level and high pressurizer pressure reactor trips prevent liquid discharge through the safety valves in the event of a level control failure. With redundant outputs from two pressurizer level control CPs, a single CP failure will not prevent letdown isolation nor result in the heaters being uncovered.

The Tavg signal (level demand) from CP06 is transmitted independently to CP13 by a hardwired connection and also over the network. The pressurizer programmed level setpoint is calculated in CP13 and is limited to the range of 25-60% (the no load and full load values). Failure of the Tavg level demand signal from CP06 would be less severe than failure of the CP13 outputs and similar to Tavg failure on unit 1.

Charging Flow

In the AUTO mode, the charging flow controller output is limited to a minimum flow of 55 gpm to the RCP seals and the regenerative heat exchanger. The limit does not apply in MANUAL mode. The redundant output field bus modules also have a fail-safe feature which will maintain the output at 55 gpm minimum flow on loss of communication with the processor. Thermal barrier cooling provides back up for cooling the RCP seals.

External to the DCS, the charging flow valve controls also include a high select pneumatic relay in series with the signal to the valve positioner to prevent the valve from closing completely due to a spurious control signal during an Appendix R fire

event. The relay ensures a minimum flow rate of 32 gpm is maintained to the RCP seals regardless of the status of the DCS.

Letdown

When the normal letdown path is out of service the excess letdown path can be used to maintain RCS inventory and ensure that the allowable backpressure on the RCP pump No. 1 seals is not exceeded. Controls for the letdown and excess letdown paths are in separate processors. The excess letdown path instrumentation is in CP12 while the normal letdown instrumentation is controlled from CP13.

5.8 Volume Control Tank Level

The two level channels governing the water inventory in the volume control tank are input into separate processor pairs, CP12 and CP13. The CP12 level signal is then networked and hardwired to CP13 where an average of the two level signals is developed for diversion valve control and auto makeup control. A redundant high level interlock is provided in CP12 for diverting letdown flow to the holdup tank. Independent indications and high and low level alarms are provided from each channel/CP so that operators are alerted to a CP failure and can take appropriate action.

Low-low level signals are provided from each CP for re-aligning charging flow suction to the Refueling Water Storage Tank. Since valve alignment to the RWST requires a low-low level signal from both channels, a high output failure from either CP will prevent the switchover to RWST. Operators are alerted by redundant low level alarms from each channel/CP with ample time for action to maintain water supply to the charging pumps.

Failure effects of VCT level controls are similar to unit 1 except that failure of one transmitter will not disable automatic makeup. See Figure 10.

5.9 BOP Turbine Runback

For conditions where the turbine-generator steam consumption exceeds the amount of feedwater being delivered to the steam generators, a decrease in turbine load is required to prevent a reactor trip due to low-low steam generator water level. The turbine runback is discussed here not because of a need for segmentation but because of its significance in preventing a trip. The changes which have been implemented for unit 2 will increase reliability, eliminate single point failures, and provide improved protection against certain failures.

One such condition is the loss of a main feedwater pump, which will initiate runback of the turbine to below 85% and start the Standby Main Feedwater Pump. The unit can be operated at 85% load with one MFP and the SBMFP in operation.

The load reference for the BOP turbine runback is turbine impulse pressure. On unit 1 the turbine impulse pressure input to turbine runback is derived from a single

transmitter and associated bistables. The unit 2 turbine runback functions will be implemented in DCS with the higher median turbine impulse pressure signal providing the load reference and the switch functions implemented with outputs to relay logic similar to unit 1. Implementing the unit 2 runback in the DCS provides increased reliability and less susceptibility to single point failures.

Another condition requiring runback involves the No. 3 heater drain tank (HDT). With all drains from the No. 3 HDT being bypassed to the condenser, the condensate and feedwater systems can deliver only 85% guaranteed flow to the steam generators. A turbine-generator load runback to less than 85% power will be initiated when all of the following conditions exist concurrently: Unit load greater than 85% (as indicated by turbine impulse pressure), No. 3 HDT pump discharge low flow, and No. 3 HDT high level.

As noted above the turbine load reference is provided by the higher median of four turbine impulse pressure inputs to the DCS (CP06). The No. 3 HDT pump discharge flow is the median of three redundant flow measurements with redundant low flow switch outputs. The No. 3 HDT level signal is also the median of three redundant level measurements. The No. 3 HDT flow and level signals are processed in CP08. Implementing these features in the DCS provides a significant reliability improvement. Having the load reference signal in a different processor than the No. 3 HDT flow and level signals also provides a degree of protection against a false runback from a single CP failure.

6.0 Conclusions

Review of the design and licensing basis for WBN unit 2 identified requirements for segmentation of control systems and functions important to safe plant operation and ensuring the safety analyses remain bounding. The WBN unit 2 DCS design incorporates the principal segmentation features described below.

Failure of a one control processor pair, with all outputs failing high, low or as is, will not cause:

1. The feedwater control valves in more than one loop (SG level control) to fail open.
2. The feedwater control valves in one loop to fail open concurrent with the main feedwater pump speed control to going to maximum speed.
3. All the condenser steam dump valves to fail open.
4. Both the condenser steam dump valves and atmospheric steam dump valves (SG PORVs) to fail open.
5. More than one SG PORV to fail open.
6. Both pressurizer PORVs to fail open or closed, including low power operation (COMS).
7. Both pressurizer spray valves to fail open or closed. Loss of charging flow to the Reactor Coolant Pump seals.

8. Loss of both reactor coolant letdown paths.
9. Complete loss of pressurizer heater control and protection.

These requirements are satisfied by segmentation of the controls into multiple processor pairs as shown in Table 1.

Based on this evaluation, the design of the WBN unit 2 DCS does not introduce new control system failures which could adversely impact the safety analyses as described in the FSAR. Functional diversity and independence are provided for the critical control systems as required by the design basis and in a manner consistent with the unit 1 design. The segmentation implemented for unit 2 eliminates the possibility of a single processor pair failure from disabling multiple control systems or redundant features of these systems.

APPENDIX A

FUNCTIONAL LOGIC SKETCHES

FIGURES 1-10

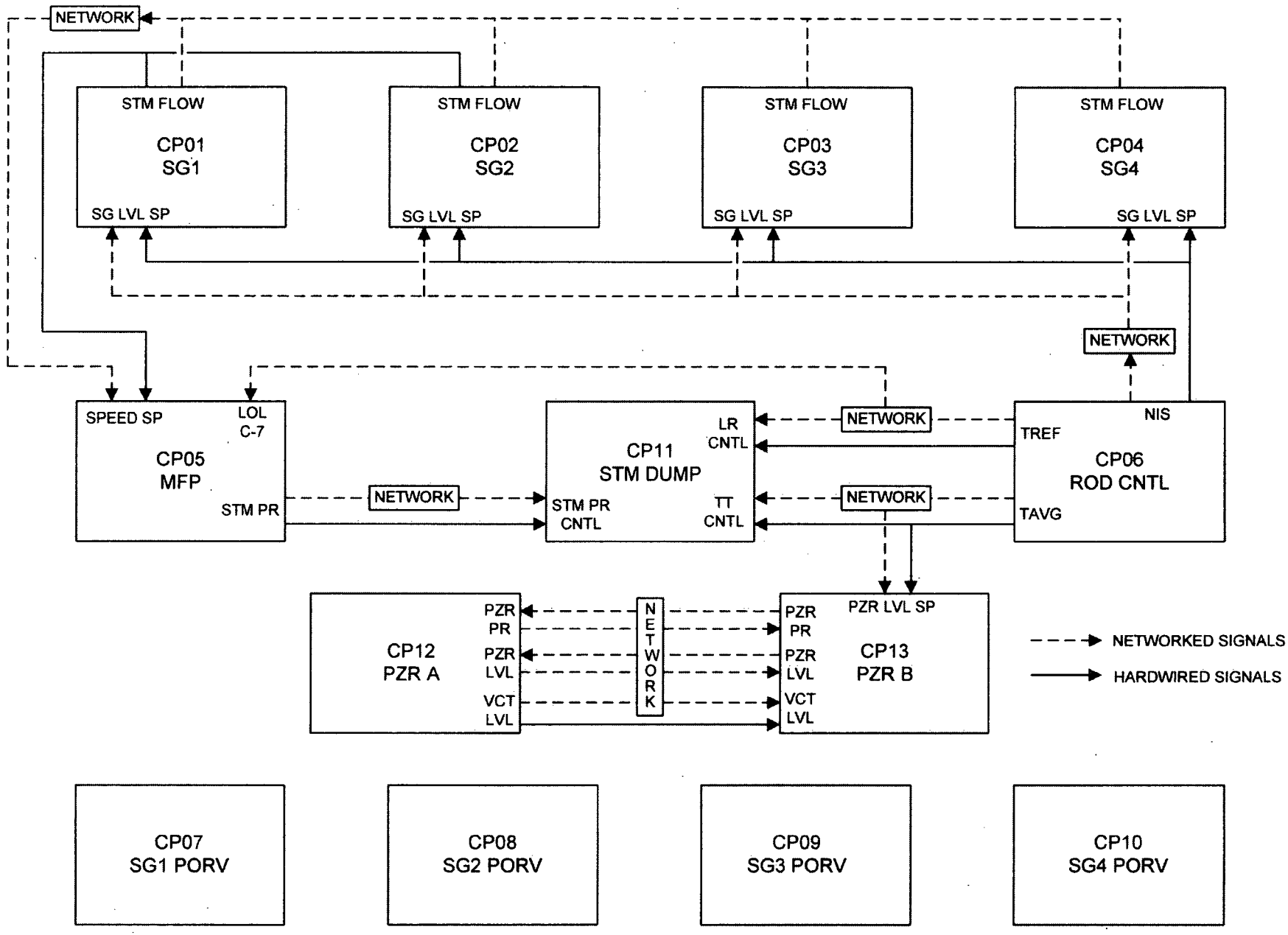

FIGURE 1

SHARED SIGNALS

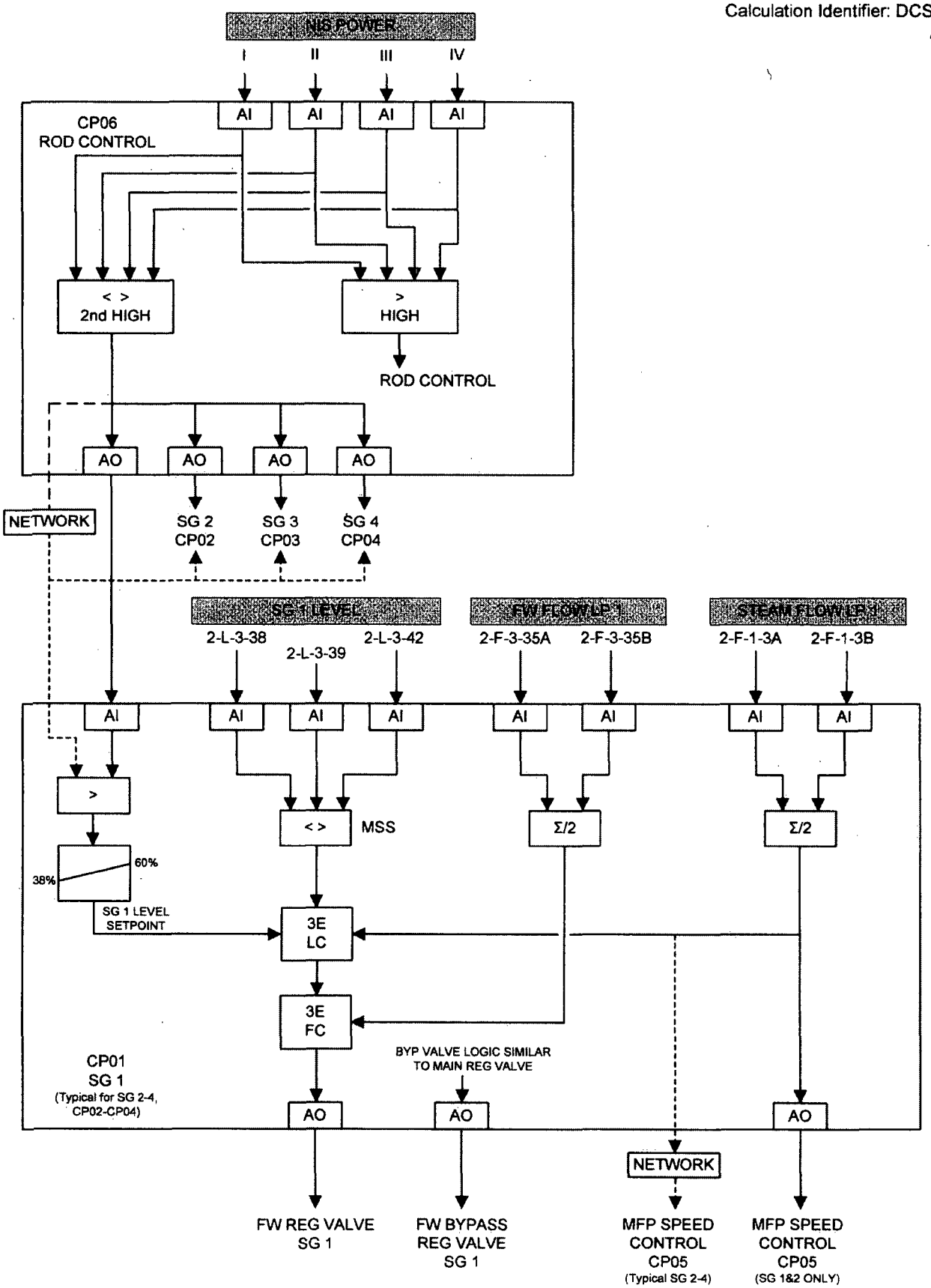

FIGURE 2

SG LEVEL CONTROL

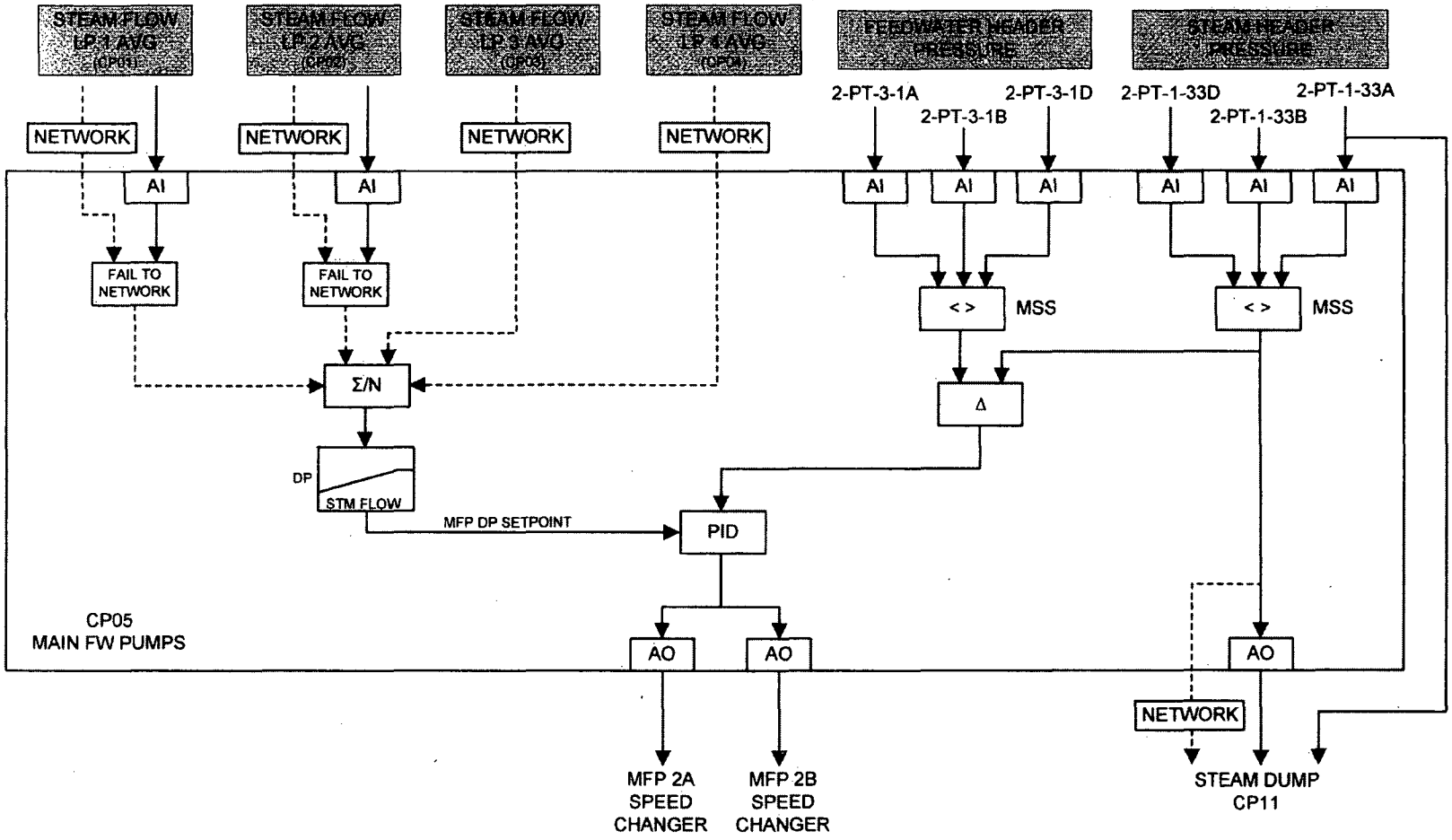

FIGURE 3

MAIN FEEDWATER PUMPS

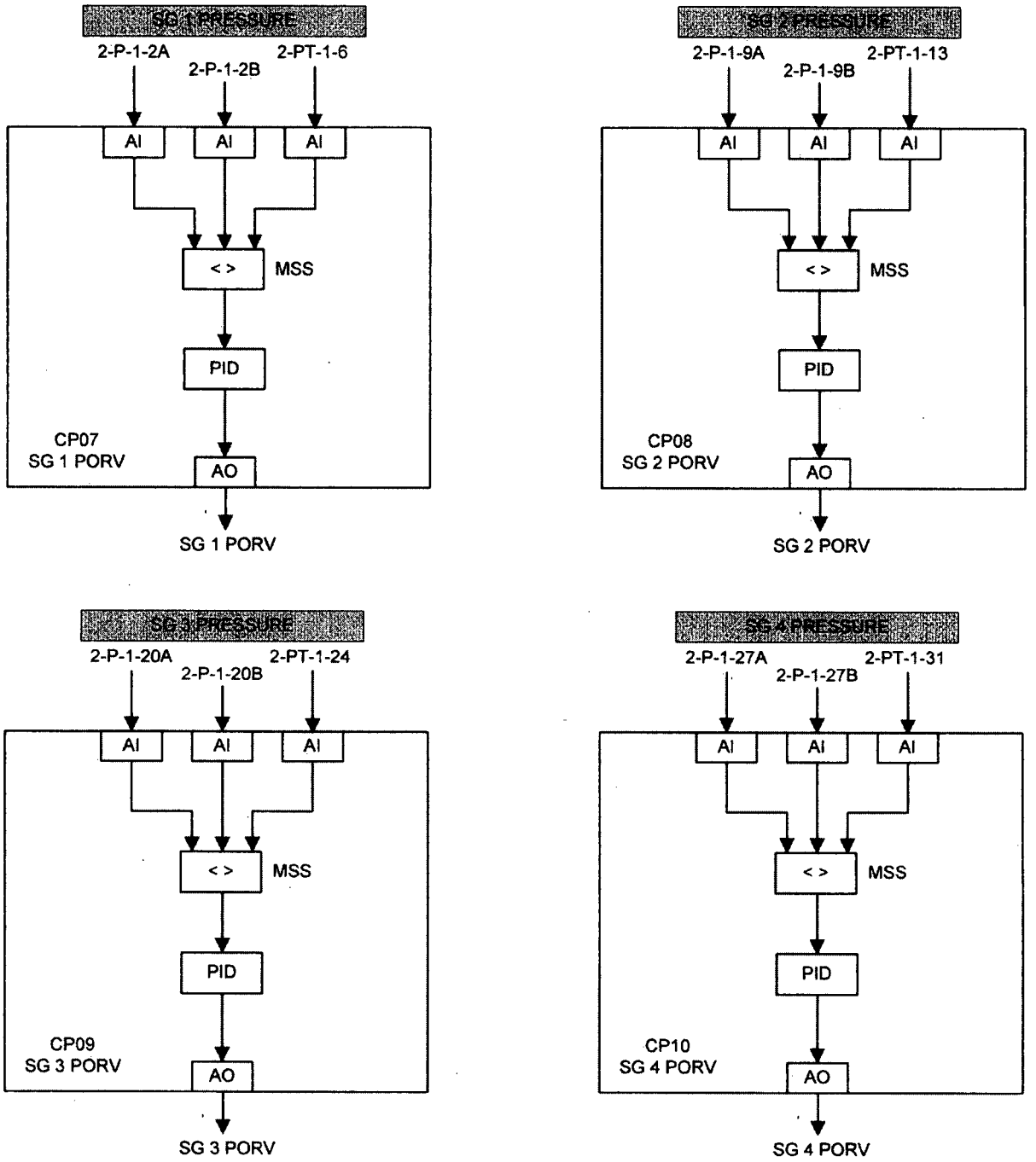

FIGURE 4

SG PORVs

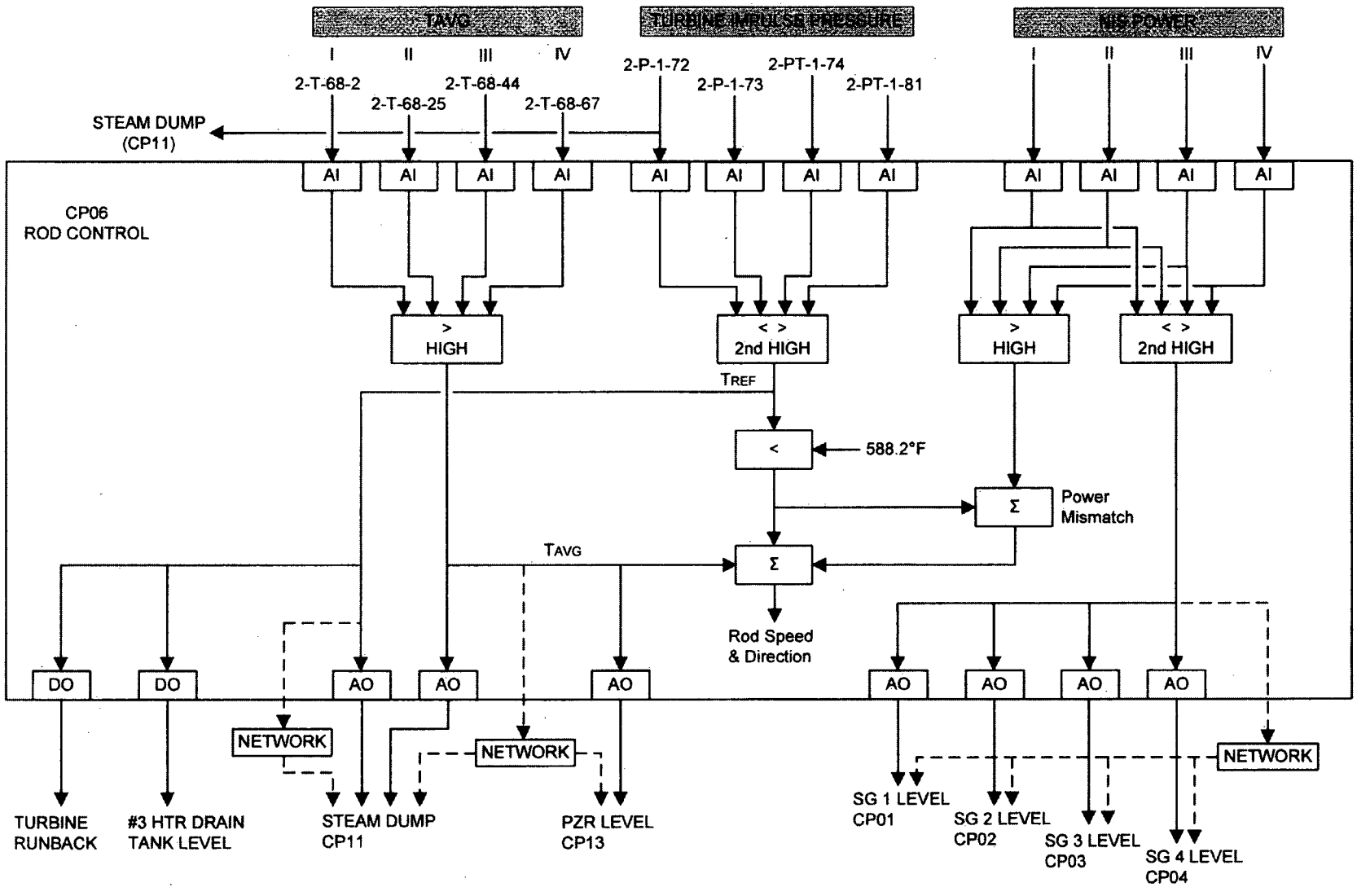

FIGURE 5

ROD CONTROL
TAVG/TREF/NIS

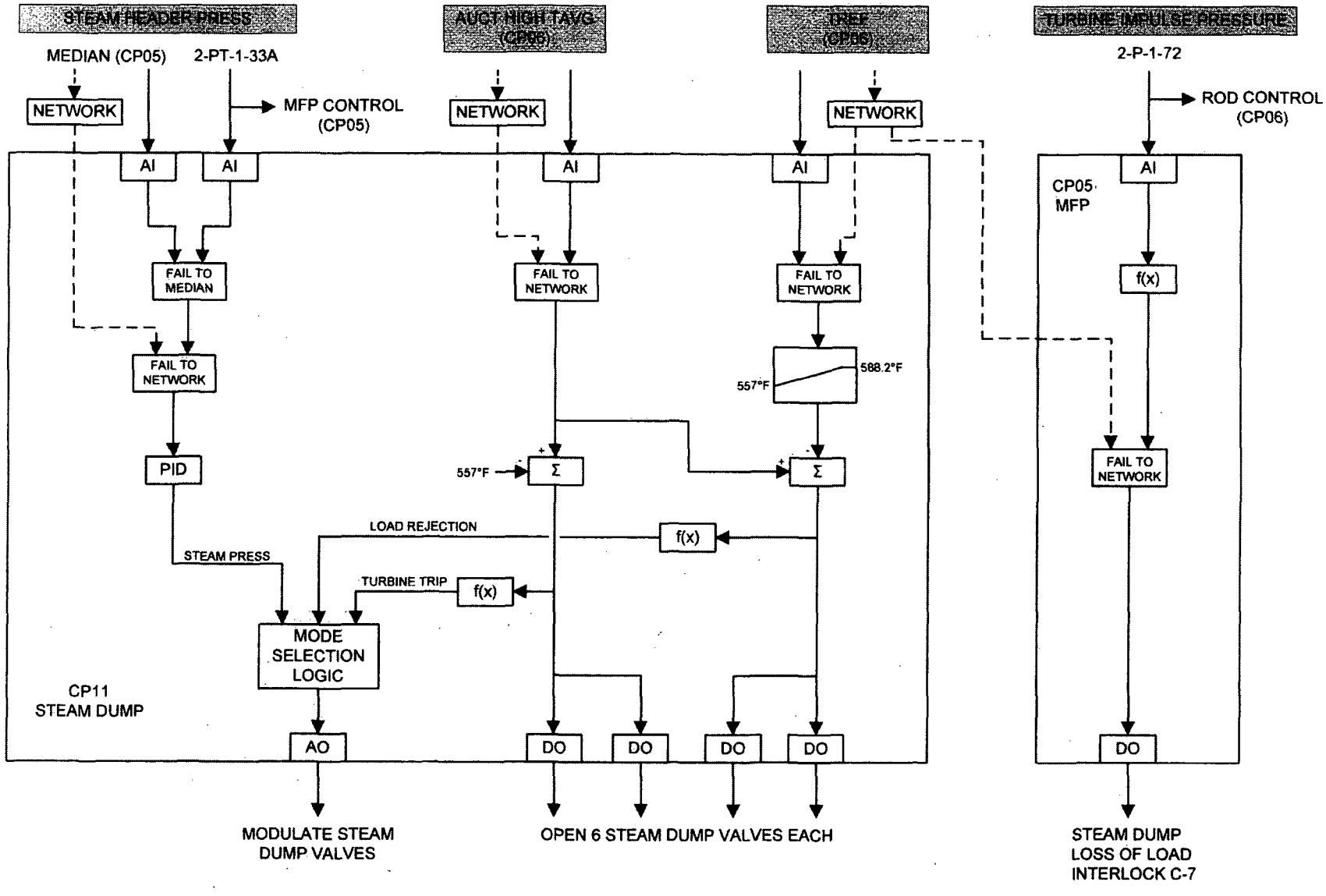

FIGURE 6

STEAM DUMP VALVES CONTROL

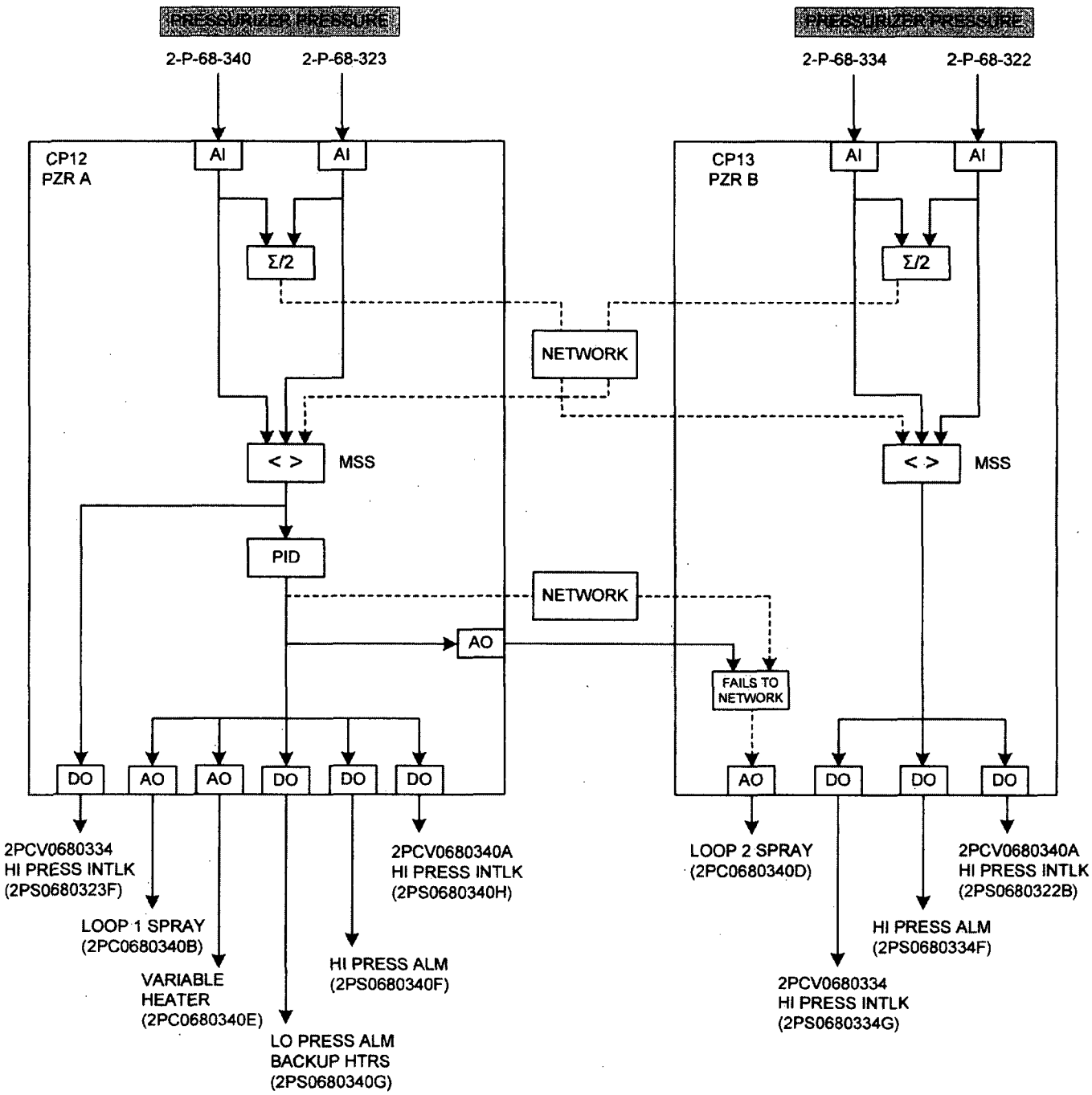

FIGURE 7

PRESSURIZER PRESSURE CONTROL

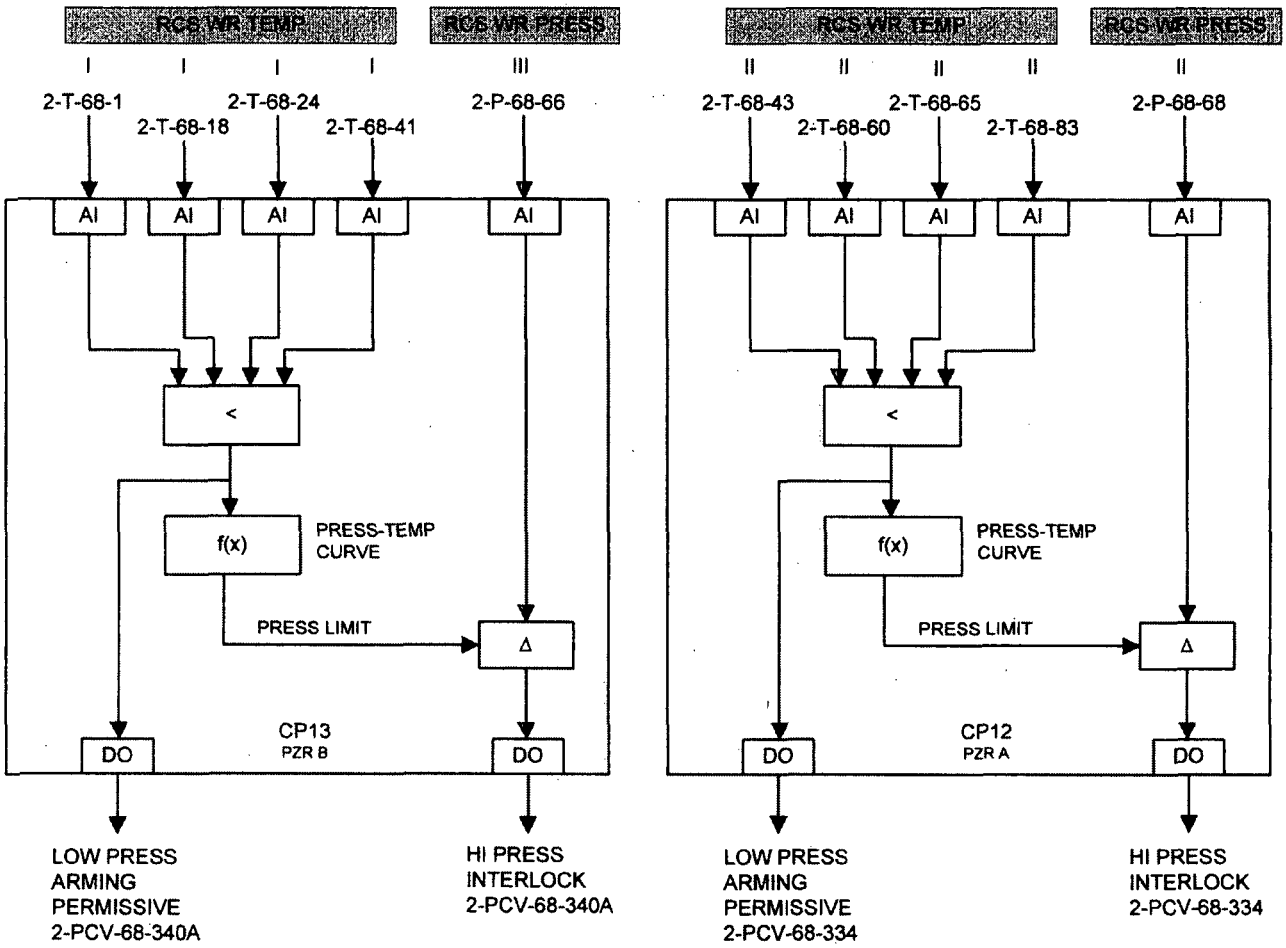

FIGURE 8

COLD OVERPRESSURE
MITIGATION SYSTEM
(PZR PORVS)

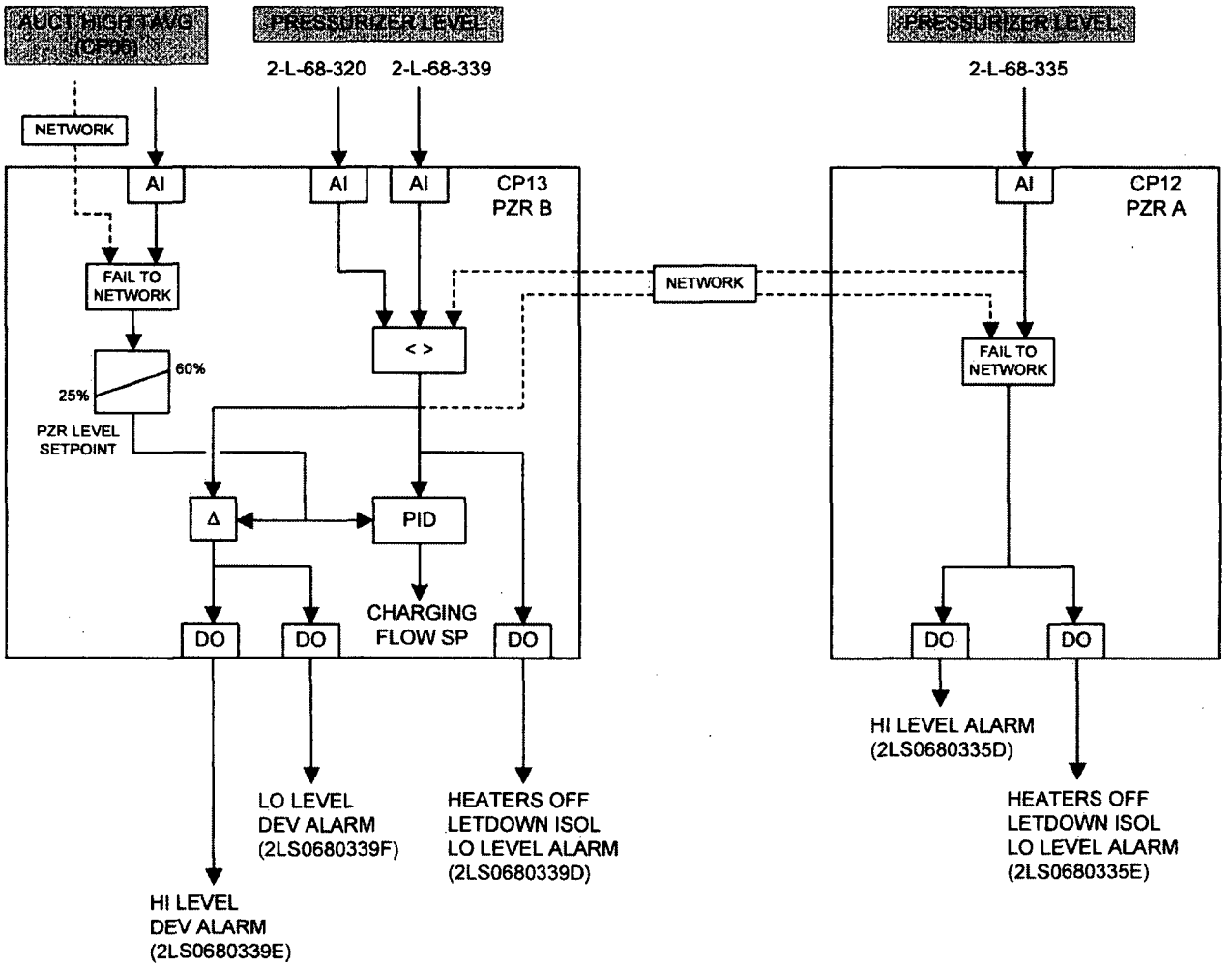

FIGURE 9

PRESSURIZER LEVEL CONTROL

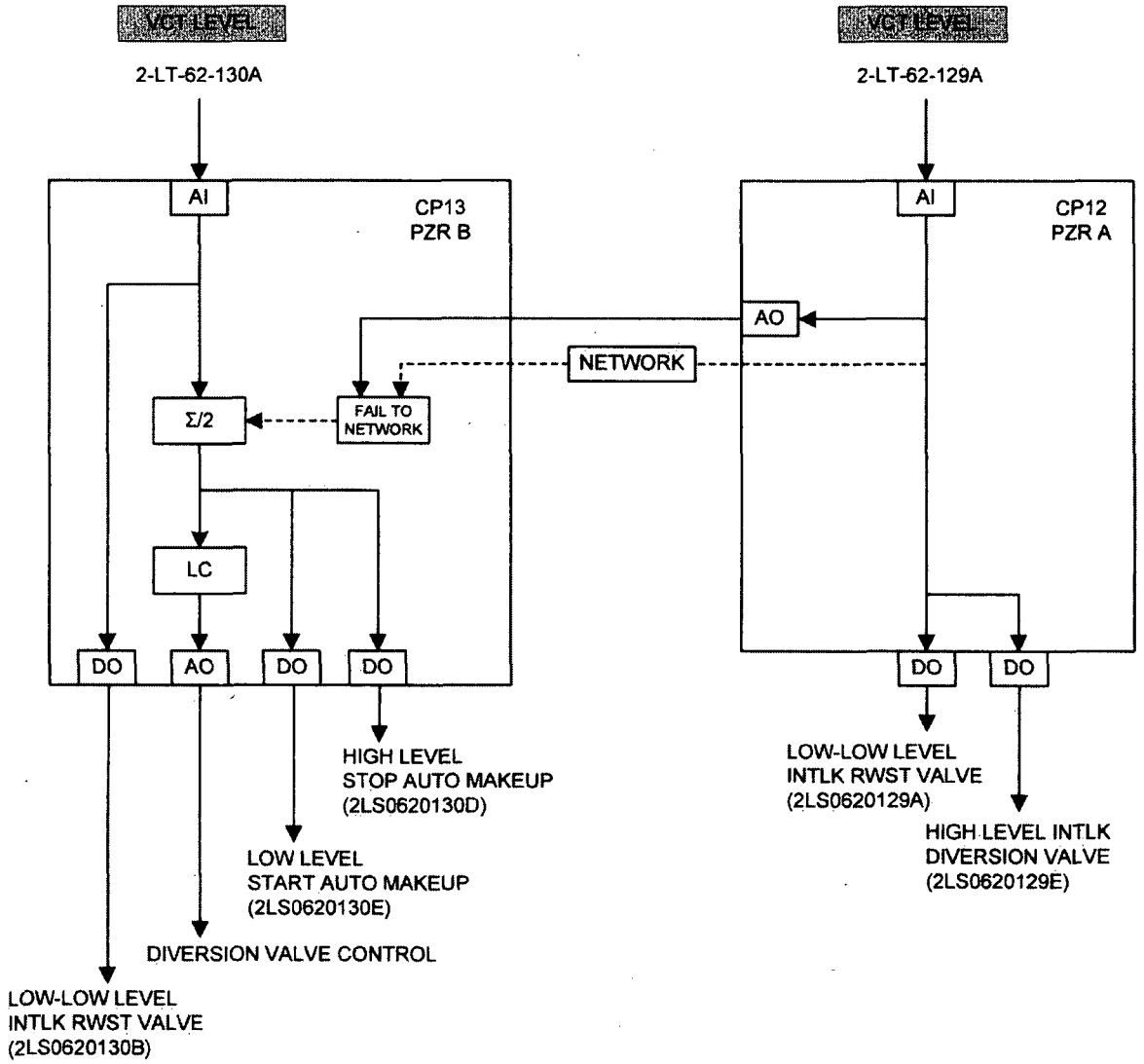

FIGURE 10

VOLUME CONTROL TANK
LEVEL CONTROL

APPENDIX B
SAFETY ANALYSIS REVIEW

The design basis accidents analyzed in the FSAR and WB-DC-40-70, Accident Analysis Parameter Checklist (AAPC), are listed in the following table. The modeling of the control systems for each event is described in the Plant Parameter List tables (item 6 of section 4.x.x.3) of the AAPC. Each analysis has been reviewed to verify that no new control system failures are introduced which could adversely impact the safety analyses. Typically, the control systems are assumed to function only if their operation results in more severe accident results. This does not imply that any segmentation requirements should be applied as a result of these assumptions. The principal aim of this review is to identify configurations wherein failure of a control processor pair could result in plant conditions which are more limiting than those analyzed. Segmentation configurations required to address such conditions are identified as well as those configurations which would enhance the availability of control systems/functions for transient response.

FSAR	AAPC	TITLE	EVENT ANALYSIS
15.2	**4.1**	**Condition II - Faults of Moderate Frequency**	
15.2.1	4.1.1	Uncontrolled Rod Cluster Control Assembly Bank Withdrawal From Subcritical	
		Pressurizer Pressure	NA
		Pressurizer Level	NA
		Steam Generator Level	NA
		Main Feedwater Pump Flow	NA
		Rod Control	NA. Rod control malfunction is an initiator.
		Steam Dump	NA
		Conclusion	Event is characterized by a power excursion and is terminated by high flux trips. No specific control systems segmentation implications.
15.2.2	4.1.2	Uncontrolled Rod Cluster Control Assembly Bank Withdrawal at Power	
		Pressurizer Pressure	PORVs and sprays are assumed to function.
		Pressurizer Level	Level control is not modeled; the high pressurizer water level reactor trip is not credited in the analysis for DNB or overpressure protection because the makeup and letdown functions of the CVCS inhibit the high pressurizer water level trip from being reached during a pressurizer fill event.
		Steam Generator Level	NA
		Main Feedwater Pump Flow	NA
		Rod Control	NA. Rod control malfunction is an initiator.
		Steam Dump	NA
		Conclusion	Rod control should be in different cp pair than pressurizer pressure (PORVs and spray valves), pressurizer level, and CVCS. PORV controls should be in different cp pairs so that a cp pair failure

APPENDIX B
SAFETY ANALYSIS REVIEW

FSAR	AAPC	TITLE	EVENT ANALYSIS
			does not disable both; similar for spray valves.
15.2.3	4.1.3	Rod Cluster Control Assembly Misalignment	
		Pressurizer Pressure	PORVs and sprays are assumed to function before and after reactor trip.
		Pressurizer Level	NA
		Steam Generator Level	NA
		Main Feedwater Pump Flow	NA
		Rod Control	NA. Rod control is assumed to be operating in AUTO.
		Steam Dump	NA
		Conclusion	Rod control should be in different cp pair than pressurizer pressure controls.
15.2.4	4.1.4	Uncontrolled Boron Dilution	
		Pressurizer Pressure	NA
		Pressurizer Level	NA
		Steam Generator Level	NA
		Main Feedwater Pump Flow	NA
		Rod Control	NA, but two cases implicitly assumed: AUTO rod control and MANUAL rod control. In AUTO, event will cause power and temperature increase and rod control system will insert rods.
		Steam Dump	NA
		Conclusion	Since failure of boric acid and primary makeup water controls in IA could initiate event, they should be in different cp than rod control. Mitigated by reactor trip or operator intervention. Event is bounded by other non-LOCA transients.
15.2.5	4.1.5	Partial Loss of Forced Reactor Coolant Flow	
		Pressurizer Pressure	NA
		Pressurizer Level	NA
		Steam Generator Level	NA
		Main Feedwater Pump Flow	NA
		Rod Control	NA. Rod control is assumed to be operating in MANUAL.
		Steam Dump	NA
		Conclusion	Control systems not modeled. Event terminated by reactor trip. No segmentation requirements.
15.2.6	4.1.6	Startup of an Inactive Reactor Coolant Loop	Not analyzed; N-1 RCP operation prohibited by Tech Specs.

APPENDIX B
SAFETY ANALYSIS REVIEW

FSAR	AAPC	TITLE	EVENT ANALYSIS
15.2.7	4.1.7	Loss of External Electrical Load and/or Turbine Trip	
		Pressurizer Pressure	Pressure control (PORVs and sprays) assumed in DNB analysis; no pressure control for over pressure analysis.
		Pressurizer Level	NA
		Steam Generator Level	NA
		Main Feedwater Pump Flow	NA
		Rod Control	NA. Rod control is assumed to be operating in MANUAL.
		Steam Dump	Not modeled, but desirable for steam dumps to be available to minimize pressure increase and remove decay heat.
		Conclusion	If condenser not available, atmospheric dump valves (SG PORVs) should be available. Rod control, pressurizer pressure and steam dump and SG PORVs should be in different cp pairs. Pzr PORV controls should be in different cp pairs; similar for spray valves and SG PORVs.
15.2.8	4.1.8	Loss of Normal Feedwater	
		Pressurizer Pressure	Pressure control (PORVs, sprays and heaters) assumed to function before and after reactor trip.
		Pressurizer Level	NA. Low level heater cutout assumed.
		Steam Generator Level	NA
		Main Feedwater Pump Flow	NA. MFP or reg valve controls malfunction could initiate.
		Rod Control	NA. Rod control is assumed to be operating in MANUAL.
		Steam Dump	NA
		Conclusion	Rod control and pressurizer pressure controls should be in different cp pairs. Pzr PORV controls should be in different cp pairs; similar for spray valves. Heater shutoff controls should also be in different cp pairs. Manual control of heaters is available outside the DCS. FW reg valves should be in different cp pairs, one per loop, with MFP control in another.
15.2.9		Loss Of Onsite and External (Offsite) Ac Power	Addressed in 15.2.7, 15.2.8 and 15.3.4.
15.2.10	4.1.9	Excessive Heat Removal Due to Feedwater System Malfunctions	
		Pressurizer Pressure	Pressure control (PORVs and sprays) assumed to function.
		Pressurizer Level	NA
		Steam Generator Level	Feedwater flow control malfunction, both single loop and multiple loops, is initiating event. Assumes feedwater control valves full open in one or all loops. TVA calc used as input assumed all 4 main reg valves wide open plus one bypass valve wide open. This analysis bounds the IA failure mode which is limited to a single CP failure which could cause both main and bypass valves in one loop to fail open while other valves continue to regulate.

APPENDIX B
SAFETY ANALYSIS REVIEW

FSAR	AAPC	TITLE	EVENT ANALYSIS
		Main Feedwater Pump Flow	NA
		Rod Control	Both AUTO and MANUAL rod control assumed.
		Steam Dump	NA
		Conclusion	Controls for feedwater reg valves should be in four different cp pairs, one per loop, with feedwater pump speed control in a fifth, to limit effects of a single cp pair failure. SG level control setpoint program for each loop should reside in different cp pair. MFP and reg valve controls, rod control and pressurizer pressure controls should be segregated. Pzr PORV controls should be in different cp pairs; similar for spray valves.
15.2.11	4.1.10	Excessive Load Increase Incident	
		Pressurizer Pressure	NA
		Pressurizer Level	NA
		Steam Generator Level	NA
		Main Feedwater Pump Flow	NA
		Rod Control	NA. Both AUTO and MANUAL rod control assumed.
		Steam Dump	NA. Steam dump control malfunction could be initiator. Analysis assumes that a single controller malfunction does not cause steam dump because of an interlock which blocks the opening of the valves unless a large turbine load decrease or turbine trip has occurred (the C-7 permissive derived from turbine impulse pressure loop 1-72)
		Conclusion	The C-7 loss of load permissive should be segregated from the steam dump controls so that a single cp failure does not result in opening of all steam dump valves.
15.2.12	4.1.11	Accidental Depressurization of the Reactor Coolant System	
		Pressurizer Pressure	Not modeled, but event initiator is inadvertent opening of pzr relief (PORV) or safety valve, with safety valve being more limiting.
		Pressurizer Level	NA
		Steam Generator Level	NA
		Main Feedwater Pump Flow	NA
		Rod Control	NA. MANUAL rod control assumed.
		Steam Dump	NA.
		Conclusion	Pzr PORV controls should be segregated so that a single cp failure does not open both PORVs.
15.2.13	4.1.12	Accidental Depressurization of the Main Steam System (Steamline Break Core Response)	
		Pressurizer Pressure	NA
		Pressurizer Level	NA

APPENDIX B
SAFETY ANALYSIS REVIEW

FSAR	AAPC	TITLE	EVENT ANALYSIS
		Steam Generator Level	NA
		Main Feedwater Pump Flow	NA
		Rod Control	NA. MANUAL rod control assumed.
		Steam Dump	Not modeled, but inadvertent opening of a single steam dump valve is one initiator. Analysis does not evaluate opening of all steam dumps.
		Conclusion	The C-7 loss of load permissive should be segregated from the steam dump controls so that a single cp failure does not result in opening of all steam dump valves.
15.2.14	4.1.13	Inadvertent Operation of the Emergency Core Cooling System	
		Pressurizer Pressure	For the minimum DNBR case, pressurizer heaters are assumed not available; the opposite is assumed for the pressurizer filling case. Sprays are assumed operable for both cases. The limiting case for pressurizer filling assumed PORVs are isolated and not available for pressure relief. In lower modes, cold overpressure mitigation system (COMS) provides protection by opening PORVs.
		Pressurizer Level	NA
		Steam Generator Level	NA
		Main Feedwater Pump Flow	NA
		Rod Control	NA. MANUAL rod control assumed.
		Steam Dump	NA.
		Conclusion	COMS controls for each PORV should be segregated.
15.3	**4.2**	**Condition III - Infrequent Faults**	
15.3.1	4.2.1	Small Break Loss of Coolant Accident	
		Pressurizer Pressure	NA
		Pressurizer Level	NA
		Steam Generator Level	NA
		Main Feedwater Pump Flow	NA
		Rod Control	NA
		Steam Dump	NA.
		Conclusion	No segmentation requirements.
15.3.4	4.2.2	Complete Loss of Forced (CLOF) Reactor Coolant Flow	
		Pressurizer Pressure	NA
		Pressurizer Level	NA

APPENDIX B
SAFETY ANALYSIS REVIEW

FSAR	AAPC	TITLE	EVENT ANALYSIS
		Steam Generator Level	NA
		Main Feedwater Pump Flow	NA
		Rod Control	NA. MANUAL rod control assumed.
		Steam Dump	NA.
		Conclusion	No segmentation requirements.
15.3.6	4.2.3	Single Rod Cluster Control Assembly Withdrawal at Full Power	
		Pressurizer Pressure	NA
		Pressurizer Level	NA
		Steam Generator Level	NA
		Main Feedwater Pump Flow	NA
		Rod Control	NA. Rod control malfunction is an initiator.
		Steam Dump	NA.
		Conclusion	No segmentation requirements.
15.4	**4.3**	**Condition IV - Limiting Faults**	
15.4.1	4.3.1	Large Break Loss of Coolant Accident	
		Pressurizer Pressure	NA
		Pressurizer Level	NA
		Steam Generator Level	NA
		Main Feedwater Pump Flow	NA
		Rod Control	NA.
		Steam Dump	NA.
		Conclusion	No segmentation requirements.
15.4.2.1	4.3.2	Major Rupture of a Main Steam System Pipe (Steamline Break Core Response)	
		Pressurizer Pressure	NA
		Pressurizer Level	NA
		Steam Generator Level	NA
		Main Feedwater Pump Flow	NA
		Rod Control	NA. MANUAL rod control assumed.
		Steam Dump	NA.

APPENDIX B
SAFETY ANALYSIS REVIEW

FSAR	AAPC	TITLE	EVENT ANALYSIS
		Conclusion	No segmentation requirements.
15.4.2.2	4.3.3	Major Rupture of a Main Feedwater Pipe	
		Pressurizer Pressure	Pressurizer PORVs are assumed to function.
		Pressurizer Level	NA
		Steam Generator Level	NA
		Main Feedwater Pump Flow	NA
		Rod Control	NA. MANUAL rod control assumed.
		Steam Dump	NA.
		Conclusion	No segmentation requirements.
15.4.3	4.3.4	Steam Generator Tube Rupture	
		Pressurizer Pressure	NA
		Pressurizer Level	NA
		Steam Generator Level	NA
		Main Feedwater Pump Flow	NA
		Rod Control	NA.
		Steam Dump	NA.
		Conclusion	No segmentation requirements.
15.4.4	4.3.5	Single Reactor Coolant Pump Locked Rotor	
		Pressurizer Pressure	NA
		Pressurizer Level	NA
		Steam Generator Level	NA
		Main Feedwater Pump Flow	NA
		Rod Control	NA. MANUAL rod control assumed.
		Steam Dump	NA.
		Conclusion	No segmentation requirements.
15.4.6	4.3.6	Rupture of a Control Rod Drive Mechanism Housing (Rod Cluster Control Assembly Ejection)	
		Pressurizer Pressure	NA
		Pressurizer Level	NA
		Steam Generator Level	NA
		Main Feedwater Pump Flow	NA

APPENDIX B
SAFETY ANALYSIS REVIEW

FSAR	AAPC	TITLE	EVENT ANALYSIS
		Rod Control	NA.
		Steam Dump	NA.
		Conclusion	No segmentation requirements.

NA – Not modeled or not applicable to analysis.

Attachment 1

Design Verification Report
WBN Unit 2 Calculation No. DCSSEGMENT

Design Verified (System, Structure, Component):	Method(s)	
System 098, non-safety related NSSS and BOP digital control system		Interdisciplinary Review
		Off-Project Design Review
	X	Individual Critical Review
		Alternate Calculation
		Qualification Testing

Document(s) Reviewed: **DCSSEGMENT, Rev. 0, Segmentation Analysis for WBN Unit 2 DCS**

Summary of Review (attach additional sheets if needed):

A design verification has been performed by the design review method in accordance with 25402-3DP-G04G-00027, Rev. 3.

Conclusions (attach additional sheets if needed)

Technical adequacy of this calculation was verified by determining that the methodology was adequate to ensure compliance with regulatory and design basis requirements, design inputs were appropriately addressed, and results and conclusions are valid.

Signature of Verifier	Organization	Position	Report Prepared by
J. T. Kepler J.T. Kepler 7/29/10	**WBN2 Engineering**	**I & C Engineer**	Name **J. T. Kepler**
			Signature J.T. Kepler
			Date 7/29/10

Attachment 1

Design Verification Checklist
(excerpted from ANSI N.45.2.11 [1974 Edition]
Name and Document Number (See Section 2.3.9.)

Yes	No	N/A	Design Verification Element Note: Any items checked "No" automatically imply the design is not verified.	Remarks *
X			Is the person performing the design verification qualified to originate the document?	
X			Is the design verification being performed by someone other than the supervisor of the originator? If the supervisor of the originator is performing design verification, mark the answer "N/A" and provide justification in the document (see section 2.3.7 for requirements).	
X			Do the collective results of the design input/output substantiate the concept and approach chosen to ensure the design activity provides an adequate, accurate, and workable solution to the problem/question being resolved?	
X			Were the design inputs correctly selected and incorporated into design?	
X			Are assumptions necessary to perform the design activity adequately described and reasonable? Where necessary, are assumptions identified for subsequent re-verifications when the detailed design activities are completed?	
X			Are the appropriate quality and quality assurance requirements specified?	
X			Are the applicable codes, standards and regulatory requirements including issue and addenda properly identified, and their requirements for design met?	
X			Have applicable construction and operating experiences been considered?	
		X	Have the design interface requirements been satisfied?	
X			Were appropriate design methods and computer programs used?	
X			Is the design output reasonable compared to design inputs?	
		X	Are the specified parts, equipment, and processes suitable for the required application? Are all applicable construction specifications referenced on the drawing(s)?	
		X	Are the specified materials compatible with each other and the design environmental conditions to which the material will be exposed?	
		X	Have adequate maintenance features and requirements been specified?	
		X	Are accessibility and other design provisions adequate for initial installation and for performing needed maintenance and repair?	
		X	Have adequate accessibility been provided to perform the in-service inspection expected to be required during the plant life?	
		X	Has the design properly considered radiation exposure to the public and plant personnel (e.g., ALARA)?	
X			Are the acceptance criteria incorporated in the design documents sufficient to allow verification that design requirements have been satisfactorily accomplished?	

Attachment 1

Design Verification Checklist (excerpted from ANSI N.45.2.11 [1974 Edition] Name and Document Number (See Section 2.3.9.)				
Yes	**No**	**N/A**	**Design Verification Element** Note: Any items checked "No" automatically imply the design is not verified.	**Remarks ***
X			Have adequate pre-operational and subsequent periodic test requirements been appropriately specified?	
		X	Have adequate handling, storage, cleaning, and shipping requirements been specified?	
X			Are adequate identification requirements specified?	
X			Are requirements for record preparation review, acceptance, retention, etc., adequately specified?	
		X	Has constructability been adequately considered?	

* It is encouraged that the verifier provide a brief explanation of the considerations utilized in performing the design verification activity in the "Remarks" column