

**ATTACHMENTS 3 AND 6 TRANSMITTED HERewith CONTAIN PROPRIETARY  
INFORMATION – WITHHOLD UNDER 10 CFR 2.390**

August 12, 2022

U.S. Nuclear Regulatory Commission  
Washington, DC 20555-0001  
ATTN: Document Control Desk

Limerick Generating Station, Units 1 and 2  
Renewed Facility Operating License Nos. NPF-39 and NPF-85  
NRC Docket Nos. 50-352 and 50-353

Subject: Review of Limerick Generating Station Defense in Depth and Diversity  
Common Cause Failure Coping Analysis, WNA-AR-01074-GLIM-P, Revision  
2, July 2022, and the Licensing Technical Report for the Limerick Generating  
Station Units 1&2 Digital Modernization Project, WCAP-18598-P, Revision 0,  
July 2022

- References:
1. Constellation Energy Generation, LLC letter to the U.S. Nuclear  
Regulatory Commission, Limerick Generating Station, Units 1 and 2,  
“Review of Limerick Generating Station Defense in Depth and Diversity  
Common Cause Failure Coping Analysis, WNA-AR-01074-GLIM-P, Rev  
1, February 2022, dated February 14, 2022” (ADAMS Accession No.  
ML22046A003)
  2. Constellation Energy Generation, LLC letter to the U.S. Nuclear  
Regulatory Commission, Limerick Generating Station, Units 1 and 2,  
“Supplement to Review of Limerick Generating Station Defense in Depth  
and Diversity Common Cause Failure Coping Analysis, WNA-AR-01074-  
GLIM-P, Rev 1, February 2022,” dated March 25, 2022 (ADAMS  
Accession No. ML22084A114)
  3. Meeting Between NRC Staff and Constellation Energy Generation, LLC  
on the Review of the Defense in Depth and Diversity Coping Analysis  
Supporting the Digital Upgrade of Instrumentation and Controls at  
Limerick Generating Station, Units 1 and 2 ADAMS Accession No.  
ML22203A084), conducted on July 22, 2022

In Reference 1, Constellation Energy Generation, LLC (CEG) submitted the Limerick  
Generating Station Defense in Depth and Diversity Common Cause Failure Coping  
Analysis, WNA-AR-01074-GLIM-P, Rev 0, February 2022, requesting NRC review by  
August 14, 2022.

**ATTACHMENTS 3 and 6 HERewith CONTAIN  
PROPRIETARY INFORMATION – WITHHOLD UNDER 10 CFR 2.390.  
When separated from Attachments 3 and 6 this cover letter is decontrolled.**



**ATTACHMENTS 3 AND 6 TRANSMITTED HERewith CONTAIN PROPRIETARY  
INFORMATION – WITHHOLD UNDER 10 CFR 2.390**

Review of LGS D3 Coping Analysis  
LGS Digital Modernization Project  
Docket Nos. 50-352 and 50-353  
August 12, 2022  
Page 2

In Reference 2, CEG withdrew the request to complete the review of the D3 Coping Analysis by August 14, 2022, and modified the request such that a separate Safety Evaluation Report (SER) and approval would not be necessary. CEG acknowledged that the D3 Coping Analysis was part of the Limerick Digital Modernization Project LAR review and that the NRC could continue to review the D3 Coping Analysis and provide timely feedback to CEG without requiring D3 Coping Analysis approval.

Subsequent to the Reference 2 submittal, NRC had identified several potential issues associated with the scope of the proprietary mark-ups associated with Revision 1 of the D3 Coping Analysis, and CEG agreed to correct and revise as Revision 2. In addition, CEG found that the level 8 reactor water level trip is independent of the Plant Protection System (PPS), but it is using a programable logic controller which is not considered sufficiently diverse to be credited in the analysis. This diversity issue was also addressed and corrected and is included in Revision 2 of the D3 Coping Analysis.

Attachment 1 contains the Westinghouse Electric Company (WEC) affidavit, which establishes the basis upon which the information contained in the D3 Coping Analysis Revision 2 may be withheld from public disclosure. Attachment 2 contains the non-proprietary version of the D3 Coping Analysis, Revision 2. Attachment 3 contains the proprietary version of the D3 Coping Analysis, Revision 2.

In Reference 3, during a scheduled D3 Coping Analysis Audit meeting on July 22, 2022, a discussion regarding the completed WEC Licensing Technical Report (LTR) arose. Feedback was provided that the LTR, which contained additional PPS technical and system architectural information, may be useful to facilitate the ongoing D3 Coping Analysis Audit and that early submittal of this document might provide additional information to facilitate timely resolution of Audit Open Item Summary List Questions.

Accordingly, Attachment 4 contains the WEC affidavit, which establishes the basis upon which the information contained in the WEC LTR Revision 0 may be withheld from public disclosure. Attachment 5 contains the non-proprietary version of the WEC LTR Revision 0. Attachment 6 contains the proprietary version of the WEC LTR Revision 0.

The D3 Coping Analysis Revision 2 provided in Attachment 3 and the WEC LTR Revision 0 provided in Attachment 6 contain information proprietary to WEC. Attachments 1 and 4 include affidavits signed by WEC, the owner of the proprietary information. The affidavits set forth the basis upon which the information may be withheld from public disclosure by the NRC, and it addresses with specificity the considerations listed in paragraph (b)(4) of 10 CFR 2.390 of the NRC's regulations. WEC requests that the WEC proprietary information in Attachments 3 and 6 be withheld from public disclosure in accordance with 10 CFR 2.390. Future correspondence with respect to the proprietary aspects of the application for

**ATTACHMENTS 3 and 6 HERewith CONTAIN  
PROPRIETARY INFORMATION – WITHHOLD UNDER 10 CFR 2.390.  
When separated from Attachments 3 and 6 this cover letter is decontrolled.**



**ATTACHMENTS 3 AND 6 TRANSMITTED HERewith CONTAIN PROPRIETARY  
INFORMATION – WITHHOLD UNDER 10 CFR 2.390**

Review of LGS D3 Coping Analysis  
LGS Digital Modernization Project  
Docket Nos. 50-352 and 50-353  
August 12, 2022  
Page 3

withholding related to the WEC proprietary information or the WEC affidavit provided in Attachments 1 and 3 should reference this request letter.

There are no regulatory commitments contained in this review request.

If you have any questions regarding this submittal, please contact Frank Mascitelli at 610-765-5512.

I declare under penalty of perjury that the foregoing is true and correct. Executed on this 12th day of August 2022.

Respectfully,



---

David P. Helker  
Sr. Manager - Licensing  
Constellation Energy Generation, LLC

Attachment 1: Affidavit CAW-22-038

Attachment 2: Limerick Generating Station Defense in Depth and Diversity Common Cause Failure Coping Analysis, WNA-AR-01074-GLIM-NP, Revision 2

Attachment 3: Limerick Generating Station Defense in Depth and Diversity Common Cause Failure Coping Analysis, WNA-AR-01074-GLIM-P, Revision 2

Attachment 4: Affidavit CAW-22-028

Attachment 5: Licensing Technical Report for the Limerick Generating Station Units 1&2 Digital Modernization Project, WCAP-18598-NP, Revision 0

Attachment 6: Licensing Technical Report for the Limerick Generating Station Units 1&2 Digital Modernization Project, WCAP-18598-P, Revision 0

cc:	Regional Administrator - NRC Region I	w/ attachments
		1, 2, 4 & 5
	NRC Senior Resident Inspector - Limerick Generating Station	"
	Director, Bureau of Radiation Protection - Pennsylvania Department of Environmental Protection	"
	NRC Project Manager, NRR - Limerick Generating Station	w/ attachments
		1, 2, 3, 4, 5, 6

**ATTACHMENTS 3 and 6 HERewith CONTAIN  
PROPRIETARY INFORMATION – WITHHOLD UNDER 10 CFR 2.390.  
When separated from Attachments 3 and 6 this cover letter is decontrolled.**



**ATTACHMENTS 3 AND 6 TRANSMITTED HERewith CONTAIN PROPRIETARY  
INFORMATION – WITHHOLD UNDER 10 CFR 2.390**

Review of LGS D3 Coping Analysis  
LGS Digital Modernization Project  
Docket Nos. 50-352 and 50-353  
August 12, 2022  
Page 4

bcc: Senior Vice President – MidAtlantic Operations w/o attachments “  
Vice President – Governance and Oversight ”  
Vice President - Nuclear Security, Licensing and Regulatory Affairs ”  
Site Vice President - LGS ”  
Plant Manager - LGS ”  
Director, Operations - LGS ”  
Director, Site Engineering - LGS ”  
Director, Site Training - LGS ”  
Director, Licensing and Regulatory Affairs ”  
Manager, Regulatory Assurance - LGS “  
Sr. Manager, Licensing – KSA ”  
Sr. Manager, Risk Management – KSA ”  
Manager, Engineering – KSA ”  
J. R. Berg – LGS “  
G. J. Bonanni – LGS “  
G. Budock – LGS “  
K. P. Cawley – LGS :  
J. R. Connelly – Cantera “  
M. S. Foote – Braidwood “  
Z. L. Gavin – LGS “  
J. R. George Jr - LGS “  
P. Golub – Sargent & Lundy “  
S. R. Hesse – PBAPS “  
P. Krueger – LGS “  
K. L. Marriner – LGS “  
F. J. Mascitelli – KSA “  
D. L. Molteni – LGS “  
S. Patel – LGS “  
A. Rickey – KSA “  
M. Samselski – LGS “  
G. P. Segner – LGS “  
S. Schumacher – LGS “  
PA DEP BRP Inspector - LGS, SSB2-4 ”  
Commitment Coordinator - KSA ”  
Licensing Records - KSA ”

**ATTACHMENTS 3 and 6 HERewith CONTAIN  
PROPRIETARY INFORMATION – WITHHOLD UNDER 10 CFR 2.390.  
When separated from Attachments 3 and 6 this cover letter is decontrolled.**



**ATTACHMENT 1**

**Limerick Generating Station, Units 1 and 2  
NRC Docket Nos. 50-352 and 50-353**

**Affidavit CAW-22-038**



Commonwealth of Pennsylvania:

County of Butler:

- (1) I, Zachary Harper, Manager, Licensing Engineering, have been specifically delegated and authorized to apply for withholding and execute this Affidavit on behalf of Westinghouse Electric Company LLC (Westinghouse).
- (2) I am requesting the proprietary portions of WNA-AR-01074-GLIM-P, Revision 2 be withheld from public disclosure under 10 CFR 2.390.
- (3) I have personal knowledge of the criteria and procedures utilized by Westinghouse in designating information as a trade secret, privileged, or as confidential commercial or financial information.
- (4) Pursuant to 10 CFR 2.390, the following is furnished for consideration by the Commission in determining whether the information sought to be withheld from public disclosure should be withheld.
  - (i) The information sought to be withheld from public disclosure is owned and has been held in confidence by Westinghouse and is not customarily disclosed to the public.
  - (ii) The information sought to be withheld is being transmitted to the Commission in confidence and, to Westinghouse's knowledge, is not available in public sources.
  - (iii) Westinghouse notes that a showing of substantial harm is no longer an applicable criterion for analyzing whether a document should be withheld from public disclosure. Nevertheless, public disclosure of this proprietary information is likely to cause substantial harm to the competitive position of Westinghouse because it would enhance the ability of competitors to provide similar technical evaluation justifications and licensing defense services for commercial power reactors without commensurate expenses. Also, public disclosure of the information would enable others to use the information to meet NRC requirements for licensing documentation without purchasing the right to use the information.

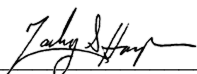


- (5) Westinghouse has policies in place to identify proprietary information. Under that system, information is held in confidence if it falls in one or more of several types, the release of which might result in the loss of an existing or potential competitive advantage, as follows:
- (a) The information reveals the distinguishing aspects of a process (or component, structure, tool, method, etc.) where prevention of its use by any of Westinghouse's competitors without license from Westinghouse constitutes a competitive economic advantage over other companies.
  - (b) It consists of supporting data, including test data, relative to a process (or component, structure, tool, method, etc.), the application of which data secures a competitive economic advantage (e.g., by optimization or improved marketability).
  - (c) Its use by a competitor would reduce his expenditure of resources or improve his competitive position in the design, manufacture, shipment, installation, assurance of quality, or licensing a similar product.
  - (d) It reveals cost or price information, production capacities, budget levels, or commercial strategies of Westinghouse, its customers or suppliers.
  - (e) It reveals aspects of past, present, or future Westinghouse or customer funded development plans and programs of potential commercial value to Westinghouse.
  - (f) It contains patentable ideas, for which patent protection may be desirable.
- (6) The attached documents are bracketed and marked to indicate the bases for withholding. The justification for withholding is indicated in both versions by means of lower-case letters (a) through (f) located as a superscript immediately following the brackets enclosing each item of information being identified as proprietary or in the margin opposite such information. These lower-case letters refer to the types of information Westinghouse customarily holds in confidence identified in Sections (5)(a) through (f) of this Affidavit.



I declare that the averments of fact set forth in this Affidavit are true and correct to the best of my knowledge, information, and belief. I declare under penalty of perjury that the foregoing is true and correct.

Executed on: 8/5/2022

A handwritten signature in black ink, appearing to read "Zachary Harper", is written over a horizontal line.

Signed electronically by

Zachary Harper



\*\*This page was added to the quality record by the PRIME system upon its validation and shall not be considered in the page numbering of this document.\*\*

## Approval Information

Author Approval Harper Zachary S Aug-05-2022 09:53:22

Files approved on Aug-05-2022

\*\*\* This record was final approved on 8/5/2022, 9:53:22 AM. (This statement was added by the PRIME system upon its validation)



**Attachment 2**

**Limerick Generating Station, Units 1 and 2  
Docket Nos. 50-352 and 50-353**

**Limerick Generating Station Defense in Depth and Diversity Common Cause Failure  
Coping Analysis, WNA-AR-01074-GLIM-NP, Revision 2**





Westinghouse Non-Proprietary Class 3

## Limerick Generating Stations Units 1 & 2 Digital Modernization Project

### Defense in Depth and Diversity Common Cause Failure Coping Analysis

WNA-AR-01074-GLIM-NP,  
Rev. 2

## Nuclear Safety Related

August 2022

#### APPROVALS

Function	Name and Signature
Author	Calvin K. Tang* Technical Advisor, Plant Control Systems
Reviewers	Boyan A. Setchenski* Project Manager, Safety I&C
	Stephen Seaman* Fellow Engineer, Safety I&C
Verifiers	Matthew Solmos* Principal Engineer, New Components and BWR
	Warren R. Odess-Gillett* Fellow Engineer, I&C Licensing
Approver	William G. Pantis* Manager, Plant Control Systems

\*Electronically approved records are authenticated in the electronic document management system.



**LIST OF CONTRIBUTORS**

<b>Revision</b>	<b>Name and Title</b>
A, 0, 1, 2	Paul Krueger, Limerick Operations Support - Senior Operations Specialist, Exelon Nuclear
A, 0	Cynthia L. Olesky, Production Control Coordinator, Major Projects I&C



## REVISION HISTORY

### RECORD OF CHANGES

Revision	Author	Description	Completed
A	Calvin K. Tang	Initial release for review	10/26/2021
0	Calvin K. Tang	Incorporation of review and verification comments	01/20/2022
1	Calvin K. Tang	Incorporation of Exelon Owner's Acceptance Review comments on Rev. 0.  Proprietary brackets were added. As such, the Proprietary version is now WNA-AR-01074-GLIM-P and the Non-Proprietary version is WNA-AR-01074-GLIM-NP.	02/10/2022
2	Calvin K. Tang	Proprietary markings were updated.  Typographical errors were corrected, and editorial changes were made.  Incorporated responses to NRC Open Items.	See PRIME

### DOCUMENT TRACEABILITY & COMPLIANCE

Created to Support the Following Document(s)	Document Number	Revision

### OPEN ITEMS

Item	Description	Status
None		



## TABLE OF CONTENTS

Section	Title	Page
	LIST OF CONTRIBUTORS .....	i
	REVISION HISTORY .....	ii
	TABLE OF CONTENTS.....	iii
	LIST OF TABLES.....	xiv
	LIST OF FIGURES .....	xiv
	ACRONYMS AND TRADEMARKS.....	xv
	GLOSSARY OF TERMS .....	xviii
	REFERENCES .....	xix
SECTION 1	INTRODUCTION .....	1-1
1.1	PURPOSE.....	1-1
1.2	SCOPE .....	1-1
SECTION 2	PLANT PROTECTION SYSTEM ARCHITECTURE.....	2-1
2.1	PPS ARCHITECTURE .....	2-1
2.2	PPS ARCHITECTURE CCF VULNERABILITIES.....	2-4
2.2.1	CIM Diversity .....	2-4
2.2.2	CIM Extensive Testing .....	2-10
2.2.3	PPS Diversity .....	2-14
2.2.4	[ ] <sup>a,c</sup> .....	2-14
SECTION 3	D3 CCF COPING ANALYSIS .....	3-1
3.1	EVENT: 15.1.1 LOSS OF FEEDWATER HEATING.....	3-3
3.1.1	Sequence of Events (UFSAR Table 15.1-2).....	3-3
3.1.2	Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS .....	3-3
3.1.3	EOP Entry Conditions .....	3-4
3.1.4	Operator Actions per RPV Control EOP with postulated PPS CCF.....	3-4
3.1.5	Summary of Diverse Features from PPS .....	3-4
3.1.6	Conclusion .....	3-4
3.2	EVENT: 15.1.2 FEEDWATER CONTROL FAILURE – MAXIMUM DEMAND (WITHOUT TURBINE BYPASS) .....	3-4
3.2.1	Sequence of Events (UFSAR Table 15.1-3).....	3-5
3.2.2	Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS .....	3-5
3.2.3	EOP Entry Conditions .....	3-5
3.2.4	Operator Actions per RPV Control EOP with postulated PPS CCF.....	3-5
3.2.5	Summary of Diverse Features from PPS .....	3-6
3.2.6	Conclusion .....	3-6



3.3	EVENT: 15.1.2 FEEDWATER CONTROL FAILURE – MAXIMUM DEMAND (WITH BYPASS).....	3-6
3.3.1	Sequence of Events (UFSAR Table 15.1-3):.....	3-6
3.3.2	Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS .....	3-7
3.3.3	EOP Entry Conditions .....	3-7
3.3.4	Operator Actions per RPV Control EOPs with postulated PPS CCF .....	3-7
3.3.5	Summary of Diverse Features from PPS .....	3-7
3.3.6	Conclusion .....	3-8
3.4	EVENT: 15.1.3 PRESSURE REGULATOR FAILURE-OPEN .....	3-8
3.4.1	Sequence of Events (UFSAR Table 15.1-4) .....	3-8
3.4.2	Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS .....	3-9
3.4.3	EOP Entry Conditions .....	3-9
3.4.4	Operator Actions per RPV Control EOPs with postulated PPS CCF .....	3-9
3.4.5	Summary of Diverse Features from PPS .....	3-9
3.4.6	Conclusion .....	3-10
3.5	EVENT: 15.1.4 INADVERTENT MAIN STEAM RELIEF VALVE OPENING.....	3-10
3.5.1	Sequence of Events (UFSAR Table 15.1-5) .....	3-10
3.5.2	Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS .....	3-10
3.5.3	EOP Entry Conditions .....	3-11
3.5.4	Operator Actions per EOPs with postulated PPS CCF .....	3-11
3.5.5	Summary of Diverse Features from PPS .....	3-11
3.5.6	Conclusion .....	3-12
3.6	EVENT: 15.1.6 INADVERTENT RHR SHUTDOWN COOLING OPERATION.....	3-12
3.6.1	Sequence of Events (UFSAR Table 15.1-1) .....	3-12
3.6.2	Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS .....	3-12
3.6.3	EOP Entry Conditions .....	3-12
3.6.4	Operator Actions .....	3-12
3.6.5	Summary of Diverse Features from PPS .....	3-13
3.6.6	Conclusion .....	3-13
3.7	EVENT: 15.2.1 PRESSURE REGULATOR FAILURE – CLOSED .....	3-13
3.7.1	Sequence of Events.....	3-13
3.7.2	Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS .....	3-13
3.7.3	EOP Entry Conditions .....	3-14
3.7.4	Operator Actions.....	3-14
3.7.5	Summary of Diverse Features from PPS .....	3-14
3.7.6	Conclusion .....	3-14
3.8	EVENT: 15.2.2 GENERATOR LOAD REJECTION WITH BYPASS FAILURE.....	3-14
3.8.1	Sequence of Events (UFSAR Table 15.2-2) .....	3-14



3.8.2	Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS .....	3-15
3.8.3	EOP Entry Conditions .....	3-15
3.8.4	Operator Actions per RPV Control / Primary Containment Control EOP with postulated PPS CCF .....	3-15
3.8.5	Summary of Diverse Features from PPS .....	3-16
3.8.6	Conclusion .....	3-16
3.9	EVENT: 15.2.2 GENERATOR LOAD REJECTION WITH BYPASS .....	3-16
3.9.1	Sequence of Events (UFSAR Table 15.2-1) .....	3-16
3.9.2	Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS .....	3-17
3.9.3	EOP Entry Conditions .....	3-17
3.9.4	Operator Actions per RPV Control / Primary Containment Control EOP with postulated PPS CCF .....	3-17
3.9.5	Summary of Diverse Features from PPS .....	3-17
3.9.6	Conclusion .....	3-18
3.10	EVENT: 15.2.3 TURBINE TRIP WITHOUT BYPASS .....	3-18
3.10.1	Sequence of Events (UFSAR Table 15.2-4) .....	3-18
3.10.2	Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS .....	3-18
3.10.3	EOP Entry Conditions .....	3-19
3.10.4	Operator Actions per RPV Control EOP with postulated PPS CCF .....	3-19
3.10.5	Summary of Diverse Features from PPS .....	3-19
3.10.6	Conclusion .....	3-19
3.11	EVENT: 15.2.3 TURBINE TRIP WITH BYPASS .....	3-20
3.11.1	Sequence of Events (UFSAR Table 15.2-3) .....	3-20
3.11.2	Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS .....	3-20
3.11.3	EOP Entry Conditions .....	3-20
3.11.4	Operator Actions per RPV Control EOP with postulated PPS CCF .....	3-21
3.11.5	Summary of Diverse Features from PPS .....	3-21
3.11.6	Conclusion .....	3-21
3.12	EVENT: 15.2.4 MSIV CLOSURE .....	3-21
3.12.1	Sequence of Events (UFSAR Table 15.2-5) .....	3-21
3.12.2	Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS .....	3-22
3.12.3	EOP Entry Conditions .....	3-22
3.12.4	Operator Actions per RPV Control EOP with postulated PPS CCF .....	3-22
3.12.5	Summary of Diverse Features from PPS .....	3-23
3.12.6	Conclusion .....	3-23
3.13	EVENT: 15.2.5 LOSS OF CONDENSER VACUUM .....	3-23
3.13.1	Sequence of Events (UFSAR Table 15.2-7) .....	3-23
3.13.2	Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS .....	3-24
3.13.3	EOP Entry Conditions .....	3-24
3.13.4	Operator Actions per RPV Control EOP with postulated PPS CCF .....	3-24



3.13.5	Summary of Diverse Features from PPS .....	3-25
3.13.6	Conclusion .....	3-25
3.14	EVENT: 15.2.6 LOSS OF ALL GRID CONNECTIONS .....	3-25
3.14.1	Sequence of Events (UFSAR Table 15.2-10) .....	3-25
3.14.2	Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS .....	3-26
3.14.3	EOP Entry Conditions .....	3-26
3.14.4	Operator Actions per RPV Control EOP with postulated PPS CCF .....	3-26
3.14.5	Summary of Diverse Features from PPS .....	3-27
3.14.6	Conclusion .....	3-27
3.15	EVENT: 15.2.7 LOSS OF FEEDWATER .....	3-27
3.15.1	Sequence of Events (UFSAR Table 15.2-11) .....	3-28
3.15.2	Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS .....	3-28
3.15.3	EOP Entry Conditions .....	3-28
3.15.4	Operator Actions per RPV Control EOP with postulated PPS CCF .....	3-28
3.15.5	Summary of Diverse Features from PPS .....	3-29
3.15.6	Conclusion .....	3-29
3.16	EVENT: 15.2.9 LOSS OF SHUTDOWN COOLING .....	3-29
3.16.1	Sequence of Events (UFSAR Table 15.2-12) .....	3-30
3.16.2	Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS .....	3-30
3.16.3	EOP Entry Conditions .....	3-30
3.16.4	Operator Actions .....	3-30
3.16.5	Summary of Diverse Features from PPS .....	3-31
3.16.6	Conclusion .....	3-31
3.17	EVENT: 15.2.10 LOSS OF STATOR COOLING .....	3-31
3.17.1	Sequence of Events (UFSAR Table 15.2-15) .....	3-31
3.17.2	Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS .....	3-31
3.17.3	EOP Entry Conditions .....	3-32
3.17.4	Operator Actions per RPV Control EOP with postulated PPS CCF .....	3-32
3.17.5	Summary of Diverse Features from PPS .....	3-32
3.17.6	Conclusion .....	3-32
3.18	EVENT: 15.3.1 TRIP OF ONE RECIRCULATION PUMP MOTOR .....	3-33
3.18.1	Sequence of Events (UFSAR Table 15.3-1) .....	3-33
3.18.2	Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS .....	3-33
3.18.3	EOP Entry Conditions .....	3-33
3.18.4	Operator Actions per EOPs with postulated PPS CCF .....	3-33
3.18.5	Summary of Diverse Features from PPS .....	3-33
3.18.6	Conclusion .....	3-34
3.19	EVENT: 15.3.1 TRIP OF TWO RECIRCULATION PUMPS .....	3-34
3.19.1	Sequence of Events (UFSAR Table 15.3-2) .....	3-34
3.19.2	Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS .....	3-34



3.19.3	EOP Entry Conditions .....	3-34
3.19.4	Operator Actions per RPV Control EOP with postulated PPS CCF.....	3-34
3.19.5	Summary of Diverse Features from PPS .....	3-35
3.19.6	Conclusion .....	3-35
3.20	EVENT: 15.3.2 RECIRCULATION FLOW CONTROL FAILURE- DECREASING FLOW .....	3-35
3.21	EVENT: 15.3.3 RECIRCULATION PUMP SEIZURE .....	3-35
3.21.1	Sequence of Events (UFSAR Table 15.3-3) .....	3-36
3.21.2	Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS .....	3-36
3.21.3	EOP Entry Conditions .....	3-36
3.21.4	Operator Actions per RPV Control EOPs with postulated PPS CCF .....	3-36
3.21.5	Summary of Diverse Features from PPS .....	3-36
3.21.6	Conclusion .....	3-36
3.22	EVENT: 15.3.4 RECIRCULATION PUMP SHAFT BREAK .....	3-37
3.22.1	Sequence of Events .....	3-37
3.22.2	Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS .....	3-37
3.22.3	EOP Entry Conditions .....	3-37
3.22.4	Operator Actions.....	3-37
3.22.5	Summary of Diverse Features from PPS .....	3-37
3.22.6	Conclusion .....	3-37
3.23	EVENT: 15.4.1 ROD WITHDRAWAL ERROR - LOW POWER .....	3-38
3.23.1	Sequence of Events.....	3-38
3.23.2	Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS .....	3-38
3.23.3	EOP Entry Conditions .....	3-38
3.23.4	Operator Actions.....	3-39
3.23.5	Summary of Diverse Features from PPS .....	3-39
3.23.6	Conclusion .....	3-39
3.24	EVENT: 15.4.2 ROD WITHDRAWAL ERROR – AT POWER .....	3-39
3.24.1	Sequence of Events (UFSAR Table 15.4-1) .....	3-39
3.24.2	Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS .....	3-39
3.24.3	EOP Entry Conditions .....	3-39
3.24.4	Operator Actions.....	3-40
3.24.5	Summary of Diverse Features from PPS .....	3-40
3.24.6	Conclusion .....	3-40
3.25	EVENT: 15.4.3 CONTROL ROD MALOPERATION (SYSTEM MALFUNCTION OR OPERATOR ERROR) .....	3-40
3.26	EVENT: 15.4.4 ABNORMAL STARTUP OF IDLE RECIRCULATION PUMP .....	3-40
3.26.1	Sequence of Events (UFSAR Table 15.4-3) .....	3-40
3.26.2	Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS .....	3-40
3.26.3	EOP Entry Conditions .....	3-41



3.26.4	Operator Actions.....	3-41
3.26.5	Summary of Diverse Features from PPS .....	3-41
3.26.6	Conclusion .....	3-41
3.27	EVENT: 15.4.5 RECIRCULATION FLOW CONTROL FAILURE WITH INCREASING FLOW .....	3-41
3.27.1	Sequence of Events (UFSAR Table 15.4-4) .....	3-41
3.27.2	Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS .....	3-42
3.27.3	EOP Entry Conditions .....	3-42
3.27.4	Operator Actions per RPV Control EOP with postulated PPS CCF.....	3-42
3.27.5	Summary of Diverse Features from PPS .....	3-42
3.27.6	Conclusion .....	3-43
3.28	EVENT: 15.4.7 MISPLACED BUNDLE ACCIDENT .....	3-43
3.28.1	Sequence of Events (UFSAR Table 15.4-5) .....	3-43
3.28.2	Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS .....	3-43
3.28.3	EOP Entry Conditions .....	3-44
3.28.4	Operator Actions.....	3-44
3.28.5	Summary of Diverse Features from PPS .....	3-44
3.28.6	Conclusion .....	3-44
3.29	EVENT: 15.4.9 CONTROL ROD DROP ACCIDENT .....	3-44
3.29.1	Sequence of Events (GESTAR II, NEDO-24011-A-31-US (Reference 8), Table S.2.2.3.1.1).....	3-44
3.29.2	Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS .....	3-45
3.29.3	EOP Entry Conditions .....	3-45
3.29.4	Operator Actions.....	3-45
3.29.5	Summary of Diverse Features from PPS .....	3-46
3.29.6	Conclusion .....	3-46
3.30	EVENT: 15.5.1 INADVERTENT HPCI START .....	3-46
3.31	EVENT: 15.6.2 INSTRUMENT LINE BREAK .....	3-46
3.31.1	Sequence of Events (UFSAR Table 15.6-1) .....	3-46
3.31.2	Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS .....	3-47
3.31.3	EOP Entry Conditions .....	3-47
3.31.4	Operator Actions with postulated PPS CCF .....	3-47
3.31.5	Summary of Diverse Features from PPS .....	3-47
3.31.6	Conclusion .....	3-47
3.32	EVENT: 15.6.4 STEAM SYSTEM PIPE BREAK OUTSIDE PRIMARY CONTAINMENT .....	3-48
3.32.1	Sequence of Events (UFSAR Table 15.6-8) .....	3-48
3.32.2	Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS .....	3-48
3.32.3	EOP Entry Conditions .....	3-49
3.32.4	Summary of Relevant Operator Actions per EOPs with postulated PPS CCF .....	3-49
3.32.5	Summary of Diverse Features from PPS .....	3-50



3.32.6	Conclusion .....	3-50
3.33	EVENT: 15.6.5 LOCA INSIDE CONTAINMENT .....	3-51
3.33.1	Sequence of Events (UFSAR Table 6.3-2) .....	3-51
3.33.2	Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS .....	3-52
3.33.3	EOP Entry Conditions .....	3-52
3.33.4	Summary of Relevant Operator Actions per RPV Control and Primary Containment Control EOPs with postulated PPS CCF .....	3-52
3.33.5	Summary of Diverse Features from PPS .....	3-53
3.33.6	Conclusion .....	3-54
3.34	EVENT: 15.6.5 LOCA INSIDE CONTAINMENT-MAIN STEAM LINE BREAK .....	3-54
3.34.1	Sequence of Events (UFSAR Table 6.2-16) .....	3-55
3.34.2	Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS .....	3-55
3.34.3	EOP Entry Conditions .....	3-55
3.34.4	Summary of Relevant Operator Actions per RPV Control and Primary Containment Control EOPs with postulated PPS CCF .....	3-56
3.34.5	Summary of Diverse Features from PPS .....	3-56
3.34.6	Conclusion .....	3-57
3.35	EVENT: 15.6.6 FEEDWATER LINE BREAK OUTSIDE PRIMARY CONTAINMENT .....	3-58
3.35.1	Sequence of Events (UFSAR Table 15.6-23) .....	3-58
3.35.2	Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS .....	3-58
3.35.3	EOP Entry Conditions .....	3-58
3.35.4	Summary of Relevant Operator Actions per RPV Control and Secondary Containment Control EOPs with postulated PPS CCF .....	3-59
3.35.5	Summary of Diverse Features from PPS .....	3-59
3.35.6	Conclusion .....	3-60
3.36	EVENT: 15.7.1.1 MAIN CONDENSER OFFGAS TREATMENT SYSTEM FAILURE .....	3-60
3.36.1	Sequence of Events (UFSAR Table 15.7-1) .....	3-60
3.36.2	Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS .....	3-61
3.36.3	EOP Entry Conditions .....	3-61
3.36.4	Operator Actions per RPV Control EOPs with postulated PPS CCF .....	3-61
3.36.5	Summary of Diverse Features from PPS .....	3-61
3.36.6	Conclusion .....	3-61
3.37	EVENT: 15.7.1.2 MALFUNCTION OF MAIN TURBINE GLAND SEALING SYSTEM .....	3-61
3.37.1	Sequence of Events .....	3-62
3.37.2	Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS .....	3-62
3.37.3	EOP Entry Conditions .....	3-62
3.37.4	Operator Actions .....	3-62



3.37.5	Summary of Diverse Features from PPS .....	3-62
3.37.6	Conclusion .....	3-62
3.38	EVENT: 15.7.1.3 FAILURE OF STEAM JET AIR EJECTOR LINES .....	3-62
3.38.1	Sequence of Events .....	3-63
3.38.2	Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS .....	3-63
3.38.3	EOP Entry Conditions .....	3-63
3.38.4	Operator Actions .....	3-63
3.38.5	Summary of Diverse Features from PPS .....	3-63
3.38.6	Conclusion .....	3-63
3.39	EVENT: 15.7.2 LIQUID RADIOACTIVE WASTE SYSTEM FAILURE .....	3-63
3.40	EVENT: 15.7.3 POSTULATED RADIOACTIVE RELEASES DUE TO LIQUID RADWASTE TANK FAILURE .....	3-63
3.41	EVENT: 15.7.4 FUEL HANDLING ACCIDENT .....	3-64
3.41.1	Sequence of Events (UFSAR Table 15.7-15) .....	3-64
3.41.2	Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS .....	3-64
3.41.3	EOP Entry Conditions .....	3-64
3.41.4	Operator Actions .....	3-64
3.41.5	Summary of Diverse Features from PPS .....	3-65
3.41.6	Conclusion .....	3-65
3.42	EVENT: 15.7.5 SPENT FUEL CASK-DROP ACCIDENT .....	3-65
3.43	EVENT: 15.7.6 MOVEMENT OF LOADS WITHOUT SECONDARY CONTAINMENT .....	3-65
3.44	EVENT: 15.7.8 ANTICIPATED TRANSIENTS WITHOUT SCRAM .....	3-65
3.45	SUMMARY OF REQUIRED DPS CONTROLS .....	3-66
3.46	SUMMARY OF DIVERSE INDICATIONS WITH PLANT IDENTIFIERS .....	3-70
SECTION 4	BTP 7-19 POSITION 4 DISPLAYS AND CONTROLS .....	4-1
4.1	REACTIVITY CONTROL .....	4-1
4.1.1	Position 4 Controls .....	4-1
4.1.2	Position 4 Displays .....	4-2
4.2	CORE HEAT REMOVAL .....	4-2
4.2.1	Position 4 Controls .....	4-2
4.2.2	Position 4 Displays .....	4-3
4.3	REACTOR COOLANT INVENTORY .....	4-3
4.3.1	Position 4 Controls .....	4-4
4.3.2	Position 4 Displays .....	4-4
4.4	CONTAINMENT ISOLATION .....	4-4
4.4.1	Position 4 Controls – Primary Containment .....	4-4
4.4.2	Position 4 Controls – Secondary Containment (Reactor Enclosure) .....	4-5
4.4.3	Position 4 Displays .....	4-5
4.5	CONTAINMENT INTEGRITY .....	4-6
4.5.1	Position 4 Controls .....	4-6
4.5.2	Position 4 Displays .....	4-6



4.6	SUMMARY OF POSITION 4 DIVERSE CONTROLS.....	4-6
4.7	SUMMARY OF DIVERSE POSITION 4 DISPLAYS.....	4-8
4.8	CONCLUSION.....	4-9
SECTION 5	CCF SPURIOUS ACTUATION ANALYSIS.....	5-1
5.1	[ ] <sup>a,c</sup> .....	5-3
5.1.1	[ ] <sup>a,c</sup> .....	5-3
5.1.2	[ ] <sup>a,c</sup> .....	5-3
5.1.3	[ ] <sup>a,c</sup> .....	5-3
5.1.4	[ ] <sup>a,c</sup> .....	5-3
5.1.5	[ ] <sup>a,c</sup> .....	5-4
5.1.6	Conclusion .....	5-4
5.2	[ ] <sup>a,c</sup> .....	5-4
5.2.1	[ ] <sup>a,c</sup> .....	5-4
5.2.2	[ ] <sup>a,c</sup> .....	5-4
5.2.3	[ ] <sup>a,c</sup> .....	5-4
5.2.4	[ ] <sup>a,c</sup> .....	5-5
5.2.5	[ ] <sup>a,c</sup> .....	5-5
5.2.6	Conclusion .....	5-5
5.3	[ ] <sup>a,c</sup> .....	5-5
5.3.1	[ ] <sup>a,c</sup> .....	5-5
5.3.2	[ ] <sup>a,c</sup> .....	5-5
5.3.3	[ ] <sup>a,c</sup> .....	5-6
5.3.4	[ ] <sup>a,c</sup> .....	5-6
5.3.5	[ ] <sup>a,c</sup> .....	5-7
5.3.6	Conclusion .....	5-7
5.4	[ ] <sup>a,c</sup> .....	5-7
5.4.1	[ ] <sup>a,c</sup> .....	5-7
5.4.2	[ ] <sup>a,c</sup> .....	5-7
5.4.3	[ ] <sup>a,c</sup> .....	5-8
5.4.4	[ ] <sup>a,c</sup> .....	5-8
5.4.5	[ ] <sup>a,c</sup> .....	5-8
5.4.6	Conclusion .....	5-8
5.5	[ ] <sup>a,c</sup> .....	5-9
5.5.1	[ ] <sup>a,c</sup> .....	5-9
5.5.2	[ ] <sup>a,c</sup> .....	5-9
5.5.3	[ ] <sup>a,c</sup> .....	5-9
5.5.4	[ ] <sup>a,c</sup> .....	5-10
5.5.5	[ ] <sup>a,c</sup> .....	5-10
5.5.6	Conclusion .....	5-10
5.6	[ ] <sup>a,c</sup> .....	5-11
5.6.1	[ ] <sup>a,c</sup> .....	5-11
5.6.2	[ ] <sup>a,c</sup> .....	5-11



5.6.3	[	] <sup>a,c</sup>	.....	5-12
5.6.4	[		] <sup>a,c</sup> .....	5-12
5.6.5	[	] <sup>a,c</sup>	.....	5-12
5.6.6	Conclusion .....			5-13
5.7	[	] <sup>a,c</sup>	.....	5-13
5.7.1	[	] <sup>a,c</sup>	.....	5-13
5.7.2	[	] <sup>a,c</sup>	.....	5-13
5.7.3	[	] <sup>a,c</sup>	.....	5-14
5.7.4	[		] <sup>a,c</sup> .....	5-14
5.7.5	[	] <sup>a,c</sup>	.....	5-14
5.7.6	Conclusion .....			5-15
5.8	[	] <sup>a,c</sup>	.....	5-15
5.8.1	[	] <sup>a,c</sup>	.....	5-15
5.8.2	[	] <sup>a,c</sup>	.....	5-15
5.8.3	[	] <sup>a,c</sup>	.....	5-16
5.8.4	[		] <sup>a,c</sup> .....	5-16
5.8.5	[	] <sup>a,c</sup>	.....	5-16
5.8.6	Conclusion .....			5-16
5.9	[	] <sup>a,c</sup>	.....	5-17
5.9.1	[	] <sup>a,c</sup>	.....	5-17
5.9.2	[	] <sup>a,c</sup>	.....	5-17
5.9.3	[	] <sup>a,c</sup>	.....	5-17
5.9.4	[		] <sup>a,c</sup> .....	5-17
5.9.5	[	] <sup>a,c</sup>	.....	5-17
5.9.6	Conclusion .....			5-18
5.10	[	] <sup>a,c</sup>	.....	5-18
5.10.1	[	] <sup>a,c</sup>	.....	5-18
5.10.2	[	] <sup>a,c</sup>	.....	5-18
5.10.3	[	] <sup>a,c</sup>	.....	5-18
5.10.4	[		] <sup>a,c</sup> .....	5-19
5.10.5	[	] <sup>a,c</sup>	.....	5-19
5.10.6	Conclusion .....			5-19
5.11	[	] <sup>a,c</sup>	.....	5-19
5.12	[	] <sup>a,c</sup>	.....	5-20

**SECTION 6 DIVERSITY ATTRIBUTES BETWEEN PPS, DCS, AND OTHER  
CREDITED SYSTEMS.....6-1**

6.1	HUMAN DIVERSITY .....	6-1
6.2	DESIGN DIVERSITY .....	6-2
6.3	SOFTWARE DIVERSITY .....	6-4
6.4	FUNCTIONAL DIVERSITY .....	6-4
6.5	SIGNAL DIVERSITY .....	6-4
6.6	EQUIPMENT DIVERSITY .....	6-4



6.7	DIVERSITY ATTRIBUTES OF EXISTING CONTROL AND MONITORING SYSTEMS.....	6-4
-----	---	-----



**TABLE OF CONTENTS (cont.)**

**LIST OF TABLES**

<b>Table</b>	<b>Title</b>	<b>Page</b>
Table 2-1. [	] <sup>a,c</sup> .....	2-9
Table 2-2. Comparison of BTP 7-19 Test Criteria to CIM Testing .....		2-12
Table 3-1. Summary of Required DPS Controls.....		3-67
Table 3-2. Diverse Indications Summary .....		3-70
Table 3-3. Diverse Sensors for DPS Automatic Functions.....		3-76

**LIST OF FIGURES**

<b>Figure</b>	<b>Title</b>	<b>Page</b>
Figure 2-1. PPS Architecture .....		2-3
Figure 2-2. CIM-SRNC Subsystem .....		2-6
Figure 2-3. CIM Safety Path Testing.....		2-11
Figure 5-1. [	] <sup>a,c</sup> .....	5-2
Figure 6-1. PPS and DCS Architectures .....		6-3



## **ACRONYMS AND TRADEMARKS**

Acronyms used in the document are defined in WNA-PS-00016-GEN, “Standard Acronyms and Definitions” (Reference 40), or included below to ensure unambiguous understanding of their use within this document.

<b>Acronym</b>	<b>Definition</b>
ABB	Asea Brown Boveri
ADS	Automatic Depressurization System
AOO	Anticipated Operational Occurrence
APRM	Average Power Range Monitor
ARI	Alternate Rod Insertion
ASD	Adjustable Speed Drive
ATWS	Anticipated Transient Without Scram
BPL	Bistable Processing Logic
BPWS	Banked Position Withdrawal Sequence
CCF	Common Cause Failure
CIM	Component Interface Module
CRD	Control Rod Drive
CRDA	Control Rod Drop Accident
CREFAS	Control Room Emergency Fresh Air Supply System
CS	Core Spray
CST	Condensate Storage Tank
DBA	Design Basis Accident
DCS	Distributed Control System
DEHC	Digital Electro-Hydraulic Control System
DFWLCS	Digital Feedwater and Level Control System
DWCW	Drywell Chilled Water System
DPS	Diverse Protection System
EAB	Exclusion Area Boundary
ECCS	Emergency Core Cooling System
EOP	Emergency Operating Procedure
FPGA	Field Programmable Gate Array
FZ	Fuel Zone
HARP	High Amperage Relay Panel
HMI	Human Machine Interface
HPCI	High Pressure Coolant Injection (system)
HSL	High Speed Link
HVAC	Heating, Ventilation, and Air Conditioning
ILP	Integrated Logic Processor
IRM	Intermediate Range Monitor
ITP	Interface and Test Processor
IV&V	Independent Verification and Validation
LCL	Local Coincidence Logic
LGS	Limerick Generating Station



<b>Acronym</b>	<b>Definition</b>
LOCA	Loss of Coolant Accident
LOOP	Loss of Offsite Power
LPCI	Low Pressure Core Injection (system)
LPZ	Low Population Zone
MCR	Main Control Room
MSCRWL	Minimal Steam Cooling Reactor Water Level
MSIV	Main Steam Isolation Valve
MSRV	Main Steam Relief Valve
MTP	Maintenance and Test Panel
NBI	Nuclear Boiler Instrumentation
NMS	Neutron Monitoring System
NR	Narrow Range
NSSSS	Nuclear Steam Supply Shutoff System
PA	Postulated Accident
PPC	Plant Process Computer
PPS	Plant Protection System
PRS	Plant Reference Simulator
PSP	Pressure Suppression Pressure
PSTG	Plant Specific Technical Guidelines
RCIC	Reactor Core Isolation Cooling (system)
RCPB	Reactor Coolant Pressure Boundary
RAW	Risk Achievement Worth
RBM	Rod Block Monitor
RECW	Reactor Enclosure Cooling Water System
RERS	Reactor Enclosure Recirculation System
RFCS	Recirculation Flow Control System
RHR	Residual Heat Removal
RHRSW	RHR Service Water
RMCS	Reactor Manual Control System
RNI	Remote Node Interface
RPS	Reactor Protection System
RPT	Recirculation Pump Trip
RPV	Reactor Pressure Vessel
RRCS	Redundant Reactivity Control System
RSP	Remote Shutdown Panel
RTL	Register-Transfer Level
RWCU	Reactor Water Cleanup
RWM	Rod Worth Minimizer
SD	Safety Display
SDC	Shutdown Cooling
SGTS	Standby Gas Treatment System
SRNC	Safety Remote Node Controller
SRV	Safety Relief Valve
TAF	Top of Active Fuel



<b>Acronym</b>	<b>Definition</b>
TEDE	Total Effective Dose Equivalent
TU	Termination Unit
UFSAR	Updated Final Safety Analysis Report
WR	Wide Range

All other product and corporate names used in this document may be trademarks or registered trademarks of other companies, and are used only for explanation and to the owners' benefit, without intent to infringe.



## **GLOSSARY OF TERMS**

Standard terms used in the document are defined in WNA-PS-00016-GEN, “Standard Acronyms and Definitions” (Reference 40), or included below to ensure unambiguous understanding of their use within this document.

<b>Term</b>	<b>Definition</b>
-------------	-------------------

N/A	
-----	--



## **REFERENCES**

Following is a list of references used throughout this document.

1. WCAP-16097-P-A, Revision 5, “Common Qualified Platform Topical Report,” Westinghouse Electric Company LLC
2. ML20339A647, Revision 8, Branch Technical Position 7-19, “Guidance For Evaluation Of Defense In Depth And Diversity To Address Common-Cause Failure Due To Latent Design Defects In Digital Safety Systems,” U.S. Nuclear Regulatory Commission
3. ML083310185, Revision 1, DI&C-ISG-04, “Digital Instrumentation and Controls Highly-Integrated Control Rooms – Communication Issues (HICRc),” U.S. Nuclear Regulatory Commission
4. WNA-LI-00096-GEN, Revision 0, “Evaluation of Common Cause Failure Susceptibility of Component Interface Module,” Westinghouse Electric Company LLC
5. WNA-AR-01054-GEN, Revision 0, “CIM Diversity Analysis,” Westinghouse Electric Company LLC
6. ML0906103170, “Wolf Creek Generating Station -Issuance Of Amendment Re: Modification of the Main Steam And Feedwater Isolation System Controls (TAC NO. MD4839)”
7. Limerick Generating Station Updated Final Safety Analysis Report (UFSAR), Revision 19
8. NEDO-24011-A-31-US, Revision 31, “Supplement to General Electric Standard Application for Reactor Fuel, GESTAR II, Base Document NEDO-24011-P-A,” General Electric November 2020
9. OT-101, Revisions 39, “High Drywell Pressure”
10. OT-104, Revision 58, “Unexpected/Unexplained Positive or Negative Reactivity Insertion”
11. OT-110, Revision 34, “Reactor High Level”
12. OT-117, Revision 12, “RPS Failures”
13. ON-113, Revision 28, “Loss of RECW”
14. T-101, Revision 28, “ RPV Control RC/L, RC/P (Flowchart)”
15. T-102, Revision 28, “Primary Containment Control SP/T, SP/L, PC/P, DW/T, PC/H (Flowchart)”
16. T-103, Revision 25, “Secondary Containment Control SCC/T, SCC/RAD, SCC/L (Flowchart)”
17. T-121, Revision 0, “RPV Control – Opcon 4 RC/L, RC/T (Flowchart)”



18. T-131, Revision 0, “Decay Heat Control – Opcon 5 DH/L, DH/T (Flowchart)”
19. NUREG-6303, “Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems,” U.S. Nuclear Regulatory Commission
20. Wolf Creek Nuclear Operating Corporation Wolf Creek Generating Station Docket No. 50-482 Amendment to Renewed Facility Operating License, March 31, 2009, US Nuclear Regulatory Commission (ML090610317)
21. 6002-00031, Revision 0, “ALS Diversity Analysis,” CS Innovations, LLC
22. Deleted
23. WCAP-17179, Revision 6, “AP1000 Component Interface Module Technical Report,” Westinghouse Electric Company LLC
24. Southern Nuclear Operating Company Vogtle Electric Generating Plant Unit 4, Resubmittal of ITAAC Closure Notification on Completion of ITAAC 2.5.02.14 [Index Number 553], ND-17-0824, 22 May 2017 (ML17143A244), Southern Company
25. ITAAC 2.5.01.14 Closure Verification Evaluation Form, September 22, 2017 (ML17268A064) U.S. Nuclear Regulatory Commission
26. Deleted
27. 6105-00021, Revision 5, “CIM SRNC ISE Specification,” Westinghouse Electric Company LLC
28. WNA-TP-04019-GEN, Revision 2, “CIM SRNC Subsystem Test Procedure,” Westinghouse Electric Company LLC
29. APP-PMS-T1P-080, Revision 0, “AP1000 PMS System Integration Test CIM Priority Test Procedure,” Westinghouse Electric Company LLC
30. 6105-60136, Revision 1, “CIM-SRNC ISE Test Task Report,” Westinghouse Electric Company LLC
31. WNA-TR-02718-GEN, Revision 4, “CIM SRNC Subsystem Test Report,” Westinghouse Electric Company LLC
32. APP-PMS-T2R-080, Revision 1, “AP1000 Protection and Safety Monitoring System - System Integration Test CIM Priority Test Report,” Westinghouse Electric Company LLC
33. WNA-DS-02904-GEN, Revision 0, “CIM-SRNC Test Tool Design Specification,” Westinghouse Electric Company LLC



34. WNA-RL-03374-VS3, Revision 2, "V.C. Summer Unit 3 AP1000 Protection and Safety Monitoring System Hardware Configuration Management Release Report," Westinghouse Electric Company LLC
35. LG-MISC-041, "Limerick Generating Station - Primary Containment Isolation Valve Risk Ranking," Revision 0, Constellation
36. NEDO-24222, "Assessment of BWR Mitigation of ATWS, Volume II (NUREG 0460 Alternate No. 3," Non-Proprietary version, General Electric, February 1981
37. Generic Letter 89-19, "Request for Action Related to Resolution of Unresolved Safety Issue A-47 Safety Implication of Control Systems in LWR Nuclear Power Plants, Pursuant to 10 CFR 50.54(f)," Nuclear Regulatory Agency, September 20, 1989
38. SE-10, Revision 65, "LOCA"
39. LM-0642, "Suppression Pool pH Calculation for Alternate Source Terms," Constellation
40. WNA-PS-00016-GEN, Revision 8, "Standard Acronyms and Definitions," Westinghouse Electric Company LLC
41. TP18-1-008, Revision 4, "Emergency Procedures Committee EPG/SAG Rev 4 and the TSG Rev 1," BWROG, June 1, 2018
42. TP18-1-008, Revision 4, "BWROG Emergency Procedure and Severe Accident Guidelines Appendix B Technical Basis, Volume I: Introduction and References," June 1, 2018
43. WCAP-18461-P-A, Revision 1, "Common Qualified Platform and Component Interface Module System, Elimination of Technical Specification Surveillance Requirements," Westinghouse Electric Company LLC
44. OT-116, Revision 46, "Loss of Condenser Vacuum"
45. ON-121, Revision 34, "Loss of Shutdown Cooling"
46. OT-112, Revision 65, "Unexpected/Unexplained Change in Core Flow"
47. OT-100, Revision 38, "Reactor Low Level"
48. OT-102, Revision 31, "High Reactor Pressure"
49. ON-120, Revision 31, "Fuel Handling Problems"

(Last Page of Front Matter)



## SECTION 1 INTRODUCTION

### 1.1 PURPOSE

The purpose of this document is to perform three analyses relative to the Limerick Generating Station (LGS) Plant Protection System (PPS) being implemented as part of the LGS Digital Modernization Project. The PPS will be implemented using the Common Qualified (Common Q) Platform, which is a digital platform that has been reviewed and approved by the NRC for use for safety-related systems (see Reference 1). The three analyses are:

1. CCF Coping Analysis that evaluates, for each LGS UFSAR Chapter 15 event, the plant coping ability with the assumption that the Common Q portion of the PPS is not available due to a CCF. This analysis will define the Diverse Protection System (DPS) functions needed to meet acceptance criteria. Refer to Section 3 for this analysis, which considered the guidelines of NUREG/CR-6303 (Reference 19); [ ]<sup>a,c</sup> of creating a block diagram as described in NUREG/CR-6303 identifying which aspects of the architecture are susceptible to a CCF, this analysis identifies which portions of the architecture are susceptible to a CCF, [ ]<sup>a,c</sup>. Refer to Section 2 for descriptions of the PPS architecture and its diversity features.
2. CCF Spurious Actuation Analysis [ ]<sup>a,c</sup> Refer to Section 4 for this analysis.
3. An analysis defining the set of displays and controls located in the main control room for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls will be independent and diverse from the PPS Common Q system. Refer to Section 5 for this analysis.

These analyses will identify required functionality of the DPS. Following these analyses, this document will compare the diversity attributes between the Common Q digital platform and the Emerson Ovation platform that will implement the DPS functions.

### 1.2 SCOPE

This document addresses the expected analyses from the NRC Standard Review Plan (SRP), NUREG-0800, Chapter 7, Branch Technical Position (BTP) 7-19 (Reference 2). The scope of the analysis is the PPS. The PPS functions include RPS, HPCI, ADS, RHR, CS, NSSSS, and RCIC. Because manual SLC is a safe shutdown system, it is also included as a function of PPS, although its automatic initiation for ATWS mitigation is a function of RRCS implemented in the DCS.

(Last Page of Section 1)



## SECTION 2 PLANT PROTECTION SYSTEM ARCHITECTURE

### 2.1 PPS ARCHITECTURE

For the purposes of this analysis, Figure 2-1 is used to analyze the potential vulnerabilities to CCF in the PPS architecture. The architecture is made up of four channels labeled A – D, and four divisions labeled 1-4. Each channel shares power and an AF100 bus with a division:

- Channel A shares power and an AF100 bus with Division 1
- Channel B shares power and an AF100 bus with Division 2
- Channel C shares power and an AF100 bus with Division 3
- Channel D shares power and an AF100 bus with Division 4

For each Channel/Division pair, there are three levels to the PPS architecture:

- Level 1 – the Bistable Processing Logic (BPL) that is considered the Channel portion of the architecture. It reads sensor inputs, compares those inputs to setpoints, and sends a trip signal to the Level 2 in all Divisions to support the Reactor Protection System (RPS), Nuclear Steam Supply Shutoff System (NSSSS), and Emergency Core Cooling System (ECCS) functions. These signals are transmitted via the Common Q High Speed Link (HSL). This part of the architecture utilizes the Common Q AC160 digital platform. Some sensors are shared between the PPS and the DCS that performs the functions of DPS and RRCS. This is indicated as “optional” in Figure 2-1 because not all PPS inputs are shared with the non-safety DCS (i.e., DPS/RRCS). When PPS and DCS share an input, a qualified isolator (e.g., fiber optic cable) will be installed to prevent any failures occurring on the DCS adversely affecting the PPS input side.
- Level 2 – the Local Coincidence Logic (LCL) that is considered the first level of the Division portion of the architecture. LCL is implemented using the Common Q AC160 digital platform. It receives the trip signals from the BPLs from the four channels and performs coincidence logic and initiates either a reactor trip signal, an NSSSS isolation signal, or an ECCS actuation signal. NSSSS and ECCS actuation signals from the LCL are sent to Level 3 of the architecture.

For each division, the RPS reactor trip signal feeds into its divisional RPS TU (Termination Unit). The RPS TU includes the HARP (High Amperage Relay Panel) assembly which consists of interposing solid state relays utilized to interface with the scram pilot solenoids requiring high amperage output capability. [ ]<sup>a,c</sup> The HARP responds to the RPS trip outputs. The HARP solid-state relays are coil-to-contact. The coil side is powered by the PPS cabinet power supply system, and the contact side is powered by the same plant power used for the actuating component.

A trip signal from RPS Division 1 TU or a Division 3 TU will de-energize the “A” scram pilot solenoids of all groups of control rods, and a trip signal from Division 2 or Division 4 will de-energize the “B” scram pilot solenoids of all groups of control rods. De-energization of both the



“A” and “B” scram pilot solenoids will result in a reactor scram. The manual scram push button trips are directly hardwired [ ]<sup>a,c</sup>

- Level 3 – Level 3 of the architecture is made up of two parts: The Integrated Logic Processor (ILP) and the Component Interface Module (CIM). The ILP receives the LCL system level actuation signal and fans out the component actuation signals to the CIM using the HSL. The ILP reads the manual component control signals from the Safety Displays and sends them to the CIM. The CIM provides actuating component feedback to the ILP. The ILP also reads permissive and interlock signals to facilitate manual component control. The CIM receives the component actuation signals via the Safety Remote Node Controller (SRNC) for distribution to the correct CIM for component actuation. The ILPs receive both analog and digital inputs from field sensors and feedbacks from components. This information is used in component control logic (as actuating signals or interlocks) and these signals are provided over the AF100 for display on the MTP and SD. The ILP is implemented using the Common Q AC160 digital platform. The CIM is a Field Programmable Gate Array (FPGA) component utilized as a priority module as described in NRC Interim Staff Guidance DI&C-ISG-04 (Reference 3), Part 2 Command Prioritization. As stated in Reference 3, Section 2, “safety-related commands that direct a component to a safe state must always have the highest priority and must override all other commands”. [ ]<sup>a,c</sup>

There are also two Safety Displays (SDs), one Maintenance and Test Panel (MTP), and one Interface and Test Processor (ITP) per Channel/Division. The MTP and ITP support maintenance and test activities for the PPS. The MTP is a Common Q Flat Panel Display System as described in the Common Q topical Report (Reference 1). The ITP utilizes the Common Q AC160 digital platform. The MTP and ITP do not perform any protective functions in the PPS. The SDs are located in the control room and allow the operator to observe PPS status. The three safety-related functions the SD performs are:

1. Displays Post Accident Monitoring variables.
2. Allows the operator to manually initiate NSSSS and ECCS system level actuation functions [ ]<sup>a,c</sup>
3. Allows the operator to manually control individual PPS actuating components [ ]<sup>a,c</sup>



a,c

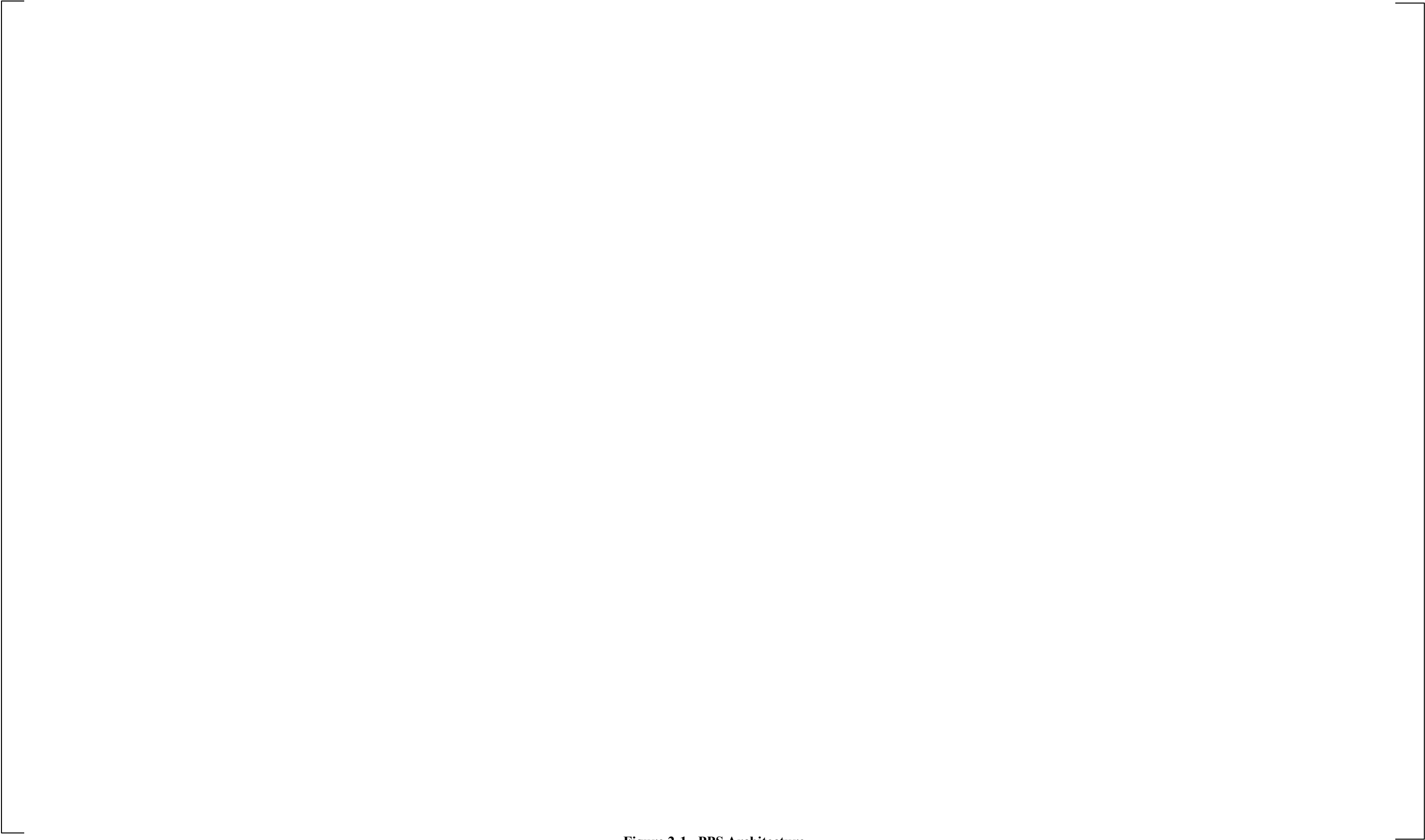


Figure 2-1. PPS Architecture



## 2.2 PPS ARCHITECTURE CCF VULNERABILITIES

[  
] <sup>a,c</sup> While performing the D3 CCF coping analysis (the first analysis listed in Section 1.1) these subsystems will be assumed to be unavailable for each UFSAR Chapter 15 event analyzed, along with the SDs.

The CIM, due to its design, is still considered available and not susceptible to a CCF. There are two legs to the safety case for this conclusion. The first is the extensive testing performed on the CIM. This testing is compared to the testing criteria in BTP 7-19 (Reference 2), Section B.3.1.2 in WNA-LI-00096-GEN, “Evaluation of Common Cause Failure Susceptibility of Component Interface Module” (Reference 4), and correlates the CIM tests to the BTP 7-19 criteria.

The second leg of the CIM safety case regarding CCF is the similarity in design attributes and process to the Main Steam Isolation and Feedwater Isolation System (MSFIS) implemented at Wolf Creek (Reference 6). WNA-AR-01054-GEN, “CIM Diversity Analysis” (Reference 5) provides the evaluation of the key design features of the CIM that are used to address the risk of CCF and eliminating CCF vulnerabilities from further consideration.

These two safety case arguments together (extensive testing and diverse design attributes) provide the holistic argument that the CIM does not need to be considered vulnerable to a CCF for this analysis.

### 2.2.1 CIM Diversity

The CIM is an FPGA-based qualified nuclear Class 1E safety grade module. It provides an interface between the PPS and the field devices through discrete component output commands for valves, pumps, etc. based on the command inputs and component status feedbacks.

The CIM subsystem was designed and qualified as a generic assembly. The CIM subsystem consists of the following primary components:

- Component Interface Module (CIM)
- CIM Base Plate Assembly
- Safety Remote Node Controller (SRNC)
- SRNC Base Plate Assembly
- Double Width Transition Panel (DWTP)
- Single Width Transition Panel (SWTP)
- Branch Terminating Device

Figure 2-2 shows the configuration of the CIM Subsystem. Referring to the figure:

- [ ] <sup>a,c</sup>
- The CIM provides discrete component output commands for valves, pumps, etc.



- The CIM receives commands and transmit status on three ports to/from interfacing systems:
  - [ ]<sup>a,c</sup> (collectively referenced as Port X) are interfacing with the safety system through SRNC.
  - Port Y is interfacing with the non-safety system through a Remote Node Interface (RNI).
  - Port Z is an additional port that can be used for the highest priority remote inputs.
- The CIM priority logic function arbitrates between demands as follows: [ ]<sup>a,c</sup>





**Figure 2-2. CIM-SRNC Subsystem**

The three major functions of the CIM are:

1. Priority Logic
2. Component Control Logic
3. Diagnostics

#### CIM Priority Logic

CIM Priority Logic establishes which demand signals are to be used in the component control logic in the event multiple signals are sent to the CIM.



[

] <sup>a,c</sup>

#### CIM Component Control Logic

The CIM is capable of performing the following functions. The design documentation will specify the CIM functions that will be employed: [

] <sup>a,c</sup>

None of the listed functions except for the Anti-coincidence Logic function will be used for the LGS PPS. [

] <sup>a,c</sup>

#### CIM Diagnostics

The CIM contains several on-board self-diagnostics features, described in detail in WCAP-18461-P-A (Reference 43), that can detect the following faults: [

] <sup>a,c</sup>



[  
] <sup>a,c</sup>

#### Diversity Features and Comparison to Wolf Creek Main Steam and Feedwater Isolation System (MSFIS)

The first generation of the Westinghouse Advanced Logic System (ALS) was installed as an upgrade to the MSFIS system at the Wolf Creek Generating Station. The NRC review of this modification included a review of the ALS platform, and this review included an argument that the features of the ALS platform adequately address CCF for the MSFIS application (Reference 20). The CIM was designed to be consistent with the approach that was used for the MSFIS application.

#### *Summary of the NRC MSFIS Review of ALS*

The methodology that was used to address CCF is included in 6002-00031, “ALS Diversity Analysis” (Reference 21), and this formed the basis for the NRC review. As stated in MSFIS SER (Reference 20),

“The NRC staff also took into consideration the low level of complexity of the MSFIS. The MSFIS is not a full trip or actuation system, but receives the trip signal from the SSPS, and upon receipt of that signal, provides opening signals to the individual valves. In addition, the MSFIS receives valve control signals from the operator control panel, and provides open or close signals to the individual valves. The received signals are binary (on/off) and not complex digital data.”

The NRC then concluded:

“The NRC staff has determined that due to the MSFIS use of two diverse cores in each FPGA and the ability to examine the resultant circuitry to determine the actual diversity, there is reasonable assurance the programmable nature of FPGAs as used in the MSFIS does not add any additional vulnerability over that found in non-programmable systems.”

#### *Comparison of CIM to MSFIS Designs*

The development of the CIM used the same processes and implemented the same architectural features that were used to develop the MSFIS design. Diversity is built into the architecture of the FPGA design, and is validated in every step of the FPGA design process. The NRC approval of the MSFIS design is based on three areas:

- Design Features

[

] <sup>a,c</sup>



[

] <sup>a,c</sup>

- Lifecycle Processes used in development and verification

In July 2010, Revision 2 of the CIM Technical Report, WCAP-17179 (ML102170259) was docketed as part of the AP1000 PMS design. It is a Tier 2\* document incorporated by reference in the Vogtle 3&4 UFSAR in accordance with 10 CFR 52. The NRC review included a review of the logic included in the design and the complete lifecycle (design, development, verification, and testing). During the review, a few areas were identified that resulted in some minor changes to the CIM. This resulted in an update to the CIM Technical Report and the changes are captured in Revision 6 of WCAP-17179 (Reference 23). These same changes were captured in license amendment LAR 16-021 for Vogtle Units 3 and 4 (ML16293A033). All changes to the CIM are included in Appendix 7A in the Vogtle 3&4 UFSAR.

An additional review of the CIM development life cycle was performed as part of the AP1000 ITAAC process (ITAAC number 2.5.02.14). The results of the NRC inspection are summarized in the Southern Nuclear “Notification on the Completion of ITAAC 2.5.02.14,” (Reference 24), and the NRC Closure Form for ITAAC 2.5.02.14 (Reference 25).

- Simplicity of the Design

As stated in MSFIS SER (Reference 20), the NRC considered the low level of complexity of the design as part of their safety evaluation. [

] <sup>a,c</sup>

**Table 2-1. [**

**] <sup>a,c</sup>**

**a,c**



The CIM Diversity Analysis (Reference 5) provides the same diversity analysis that was provided to the NRC for the ALS MSFIS (Reference 21) to allow the NRC to reach the safety conclusion that CCF was adequately addressed for MSFIS.

### **2.2.2 CIM Extensive Testing**

The second argument to the safety case that the CIM is not vulnerable to a CCF is the extensive testing performed on the CIM. BTP 7-19, Section 3.1.2 defines acceptance criteria for level of extensive testing to adequately address CCF. The Evaluation of CCF Susceptibility of the CIM (Reference 4) compares the extensive testing performed on the CIM to the test acceptance criteria in BTP 7-19. [

] <sup>a,c</sup>





**Figure 2-3. CIM Safety Path Testing**



The Reference 4 document summarizes the evaluation to the BTP 7-19 criteria as follows:

**Table 2-2. Comparison of BTP 7-19 Test Criteria to CIM Testing**

BTP 7-19 Test Criteria	CIM Testing Evaluation Results
a. Testing covers the expected performance of the proposed I&C system in each of its functional modes of operation and for all transitions between modes. For this purpose, testing may include the following:	
1) every possible combination of inputs, including every possible sequence of inputs (if the system has unused inputs, and the system can force them to a defined safe state (e.g., during a system failure), then those inputs need not meet this criterion))	[  ] <sup>a,c</sup> Component-level ISE Tests (Reference 27) Subsystem-level SIOS Tests (Reference 28) CIM Priority Logic Type Test (Reference 29)
2) for systems with analog inputs, every combination of inputs over the entire operational range of the analog inputs, including defined over-range and under-range conditions	[  ] <sup>a,c</sup>
3) every possible executable logic path (includes nonsequential logic paths)	[  ] <sup>a,c</sup> Component-level ISE Tests (Reference 27)
4) every functional state transition among all modes of operation	[        ] <sup>a,c</sup> Subsystem-level SIOS Tests (Reference 28) CIM Priority Logic Type Test (Reference 29)



BTP 7-19 Test Criteria	CIM Testing Evaluation Results
<p>5) testing results that conform to preestablished test cases to monitor for correctness of all outputs for every case</p>	<p>[</p> <p style="text-align: right;">] <sup>a,c</sup></p> <p>ISE Test Task Report (Reference 30) CIM-SRNC Subsystem Test Report (Reference 31) CIM Priority Test Report (Reference 32)</p>
<p>b. Testing for latent design defects was conducted on a system that accurately represents the system to be installed, guaranteeing that the system installed will perform the same functions as the system tested.</p>	<p>[</p> <p style="text-align: right;">] <sup>a,c</sup></p> <p>CIM-SRNC Test Tool Design Spec (Reference 33) VC Summer Unit 3 AP1000 PMS Hardware Configuration Management Release Report (Reference 34)</p>



BTP 7-19 Test Criteria	CIM Testing Evaluation Results
<p>c. Testing results account for potential spurious operations.</p>	<p>[</p> <p style="text-align: right;">] <sup>a,c</sup></p> <p>Component-level ISE Tests (Reference 27) - Section 8 “Test Case Specifications” identifies the action that will be performed for each featured test.</p>

### 2.2.3 PPS Diversity

The manual scram inputs, indicated in Figure 2-1, are provided by the hardware scram push buttons located at the operator control console (Panel tag number 10-C603 for Unit 1 and 20-C603 for Unit 2) and are directly hardwired to the RPS TU, bypassing all PPS software. These push buttons provide a diverse means of initiating a reactor scram. The RPS TU consists of solid state relays and contacts for switching power to the scram pilot solenoids.

### 2.2.4 [ ]<sup>a,c</sup>

[

 $\top_{a,c}$



### SECTION 3 D3 CCF COPING ANALYSIS

As described in Section 1, this is the first of three analyses to assess the adequacy of the LGS plant defense in depth and diversity to cope with a PPS CCF. The UFSAR describes some differences between the two units in fuel cycle parameters used for the Chapter 15 event analyses. The analyses are applicable for both LGS Units 1 and 2 because there are no differences between the two units in terms of functions, sequences of events, control, and protection actions. This first analysis takes each event in Chapter 15 of the LGS UFSAR and with best-estimate techniques, determines:

1. Is there sufficient LGS plant diversity to cope with the Chapter 15 event assuming the PPS (excluding the CIM) is not available to protect the plant.
2. Any functions necessary to be included in the DPS to adequately cope with the event when the PPS is not available to protect the plant.

All PPS functions stated in Section 1.2 are postulated to be inoperable due to a PPS CCF.

The format for the coping analysis for each event is as follows:

1. The event time sequence with \*\* ... \*\* indicates a sequence that is inoperable due to a PPS CCF.
2. The diverse automatic controls that will be initiated as a result of the event without the PPS. *Text in this format* indicates an additional diverse automatic actuation that is needed from the DPS.
3. Diverse indications available to the operator as a result of the event plus the PPS CCF; and the Emergency Operating Procedures (EOPs) that these indications will lead the operator to follow to mitigate the event. The systems that provide the diverse indications for each analysis are summarized in Table 3-2. The diverse systems and the basis for their diversity from PPS are discussed in Section 6. Any additional diverse indications needed will be indicated *with text in this format*.
4. Manual operator actuations directed by the EOP. *Text in this format* indicates additional diverse manual actuations needed to cope with the CCF scenario.
5. Summary of diverse indications and controls available in the current plant design. *Text in this format* indicates additional diverse indications and controls needed. For diverse control functions identified, any diverse parameters needed for its control logic will be specified in the DPS Functional Requirements Specification.
6. Scenario summary

The LGS design basis assumes manual actuations are not required for 10 minutes after a postulated accident (PA) commences (e.g., LGS UFSAR Chapter 7.5.2.4.1, Initial Accident Event). The LGS Plant Reference Simulator (PRS) was used as a tool to guide the analysis for necessary manual operator actions



and estimates for time available for these actions. The Limerick operations staffs were used to help assess the acceptability of the coping actions and the timing required for adequate results. A separate HFE evaluation is conducted to evaluate the adequacy of the required diverse manual actions using the acceptance criteria in NUREG-0800, Chapter 18, Attachment A as a guide.

For analyses where RPS is assumed to fail due to a PPS CCF, the Redundant Reactivity Control System (RRCS, Section 6.2) will automatically initiate the following functions upon Reactor Pressure Vessel (RPV) Pressure-High or RPV Water Level-Low (with 9-second time for RPT actuation) conditions: Alternate Rod Insertion (ARI), Standby Liquid Control (SLC) Actuation, and Recirculation Pump Trip (RPT). NEDO-24222, Assessment of BWR Mitigation of Anticipated Transients Without Scram (Reference 36), analyzed the ATWS transients assuming RPS failure and operability of ARI and RPT, and concluded that the results satisfied all applicable criteria for reactor coolant pressure boundary (RCPB), containment integrity, adequate core cooling, and allowable radioactivity release limits.

Manual operator actions are assumed to be performed for most of the events analyzed, in accordance with the Limerick EOPs, developed in accordance with the BWROG generic guidelines in Reference 41.

BTP 7-19, Section B, Branch Technical Position, Section 3.3 states that the consequences of a Common-Cause Failure may be acceptable if the following acceptance criteria are met:

- b. "For each AOO in the design basis that occurs concurrently with the CCF, the plant response, calculated using realistic or conservative assumptions, does not result in radiation release exceeding 10 percent of the applicable siting dose guideline values, or in violation of the integrity of the primary coolant pressure boundary."*
- c. "For each PA in the design basis that occurs concurrently with each single postulated CCF, the plant response, calculated using realistic or conservative assumptions, does not result in radiation release exceeding the applicable siting dose guideline values, in violation of the integrity of the primary coolant pressure boundary, or in violation of the integrity of the containment."*

In Limerick UFSAR, Chapter 15, Section 15.0.3.1, an analyzed event is classified according to the following:

- a. Incidents of moderate frequency - These are accidents that may occur from once during a calendar year to once per 20 years for a particular plant. These events are referred to as "anticipated (expected) operational transients."*
- b. Infrequent incidents - These are accidents that may occur occasionally during the life of a particular plant, ranging in time from once in 20 years to once in 100 years. These events are referred to as "abnormal (unexpected) operational transients."*
- c. Limiting faults - These are accidents that are not expected to happen, but are postulated because they may result in the release of significant amounts of radioactive material. These events are referred to as "design basis (postulated) accidents."*

Thus, BTP 7-19 reference to an anticipated operational occurrence (AOO), is an "anticipated (expected) operational transient" classified as an incident of moderate frequency, or an "abnormal (unexpected) operational transient" classified as an infrequent incident. A postulated accident (PA) is referred to as a



Limiting Fault. The frequency classification for each transient or accident is indicated for coping analysis. Furthermore, in the Conclusion section of each event, qualitative statements are made regarding the satisfaction of applicable acceptance criteria in BTP 7-19. When the use of the term, “adequate cooling”, or “the core is adequately cooled” is included in the Conclusion statements, these statements are to mean that heat removal from the reactor is sufficient to prevent rupturing the fuel cladding. This conclusion is based upon consideration of the three viable mechanisms for establishing adequate core cooling: core submergence, spray cooling, and steam cooling (Reference 42):

- a. Submergence is the preferred method for cooling the core. The core is adequately cooled by submergence when it can be determined that RPV water level is at or above the top of the active fuel (TAF, -161”). All fuel nodes are then assumed to be covered with water and heat is removed by boiling heat transfer.
- b. Adequate spray cooling is provided, assuming a bounding axial power shape, when design spray flow requirements (one CS loop flow of 6250 gpm) are satisfied and RPV water level is at or above the elevation of the jet pump suctions. The covered portion of the core is then cooled by submergence while the uncovered portion is cooled by the spray flow.
- c. Steam cooling is relied upon only if RPV water level cannot be restored and maintained above the top of the active fuel, cannot be determined, or must be intentionally lowered below the top of the active fuel. The core is adequately cooled by steam if the steam flow across the uncovered length of each fuel bundle is sufficient to maintain the hottest peak clad temperature below the appropriate limits. The covered portion of the core remains cooled by boiling heat transfer and generates the steam which cools the uncovered portion.

### **3.1 EVENT: 15.1.1 LOSS OF FEEDWATER HEATING**

Feedwater heating is assumed to be lost, resulting in a maximum reactor inlet feedwater temperature decrease of 100°F. This event is classified as an incident of moderate frequency.

#### **3.1.1 Sequence of Events (UFSAR Table 15.1-2)**

<u>TIME (sec)</u>	<u>EVENT</u>
0	Initiate a 100°F temperature reduction into the feedwater system.
25 (approx.)	Initial effect of unheated feedwater to raise core power level and steam flow.
65 (approx.)	Bypass valves open to accommodate the increasing steam flow.
120.0 (approx.)	New higher power, steady-state conditions reached.

#### **3.1.2 Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS**

1. Pressure control system maintains normal pressure control.
2. DFWLCS maintains normal level control.



### 3.1.3 EOP Entry Conditions

No EOP Entry Conditions.

### 3.1.4 Operator Actions per RPV Control EOP with postulated PPS CCF

None. However, operator will take action to reduce reactor power to within the limits with feedwater heaters out of service in accordance with plant operating procedure OT-104, “Unexpected/Unexplained Positive or Negative Reactivity Insertion” (Reference 10).

Estimated Time Available for Operator Actions: N/A. Operator action not required.

### 3.1.5 Summary of Diverse Features from PPS

The following diverse features are available to the operator for this scenario:

1. Reactor water level Narrow Range (NR) indication
2. Reactor pressure indication
3. Average Power Range Monitor (APRM)
4. DFWLCS (Digital Feed Water and Level Control System)
5. DEHC (Digital Electrohydraulic Control system)

### 3.1.6 Conclusion

For the postulated event of Loss of Feedwater Heating, concurrent with a postulated CCF of PPS, sufficient automatic control functions and indications that are diverse and independent of the PPS, are available to monitor and mitigate the event. The reactor core remains in a quasi-steady state and is adequately cooled and Reactor Coolant Pressure Boundary (RCPB) integrity is maintained. Since this transient does not result in any fuel failures or any release of primary coolant to either the secondary containment or the environment, there are no radiological consequences associated with this transient. Thus, BTP 7-19 3.3(b) Acceptance Criteria for this AOO are satisfied.

## 3.2 EVENT: 15.1.2 FEEDWATER CONTROL FAILURE – MAXIMUM DEMAND (WITHOUT TURBINE BYPASS)

Feedwater controller demand (DFWLCS) is postulated to fail upscale that results in maximum feedwater injection into the Reactor Pressure Vessel (RPV), resulting in a rapid water level rise and a trip of the main turbine and the turbine-driven feedwater pump turbines when water level reaches the Level 8 trip setpoint. It is further assumed that the turbine bypass valves failed upon a turbine trip. This event is considered to be an incident of moderate frequency.



### 3.2.1 Sequence of Events (UFSAR Table 15.1-3)

<u>TIME (sec)</u>	<u>EVENT</u> (2) (WITHOUT TURBINE BYPASS)
0	Initiate simulated failure of feedwater controller to upper limit on feedwater flow.
8.3	**Level 8 vessel level setpoint trips main turbine and feedwater pumps.**
8.3(est)	**Reactor scram trip actuated from main turbine stop valve position switches.**
8.3	**Recirculation Pump Trip (RPT) actuated by stop valve position switches.**
8.5	Turbine bypass valves fail to open.
8.5	**Main turbine stop valves closed.**
8.6	**Recirculation pump motor circuit breakers open causing recirculation drive flow to coast-down.**
10.5	First groups 1 to 3 actuated due to high pressure.

### 3.2.2 Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS

1. Reactor feedpump “C” trips on low suction pressure, with feedpumps “A” and “B” injecting water at their maximum rate of approximately 16 Mlb/hr. (Note: Feedpump turbine “C” trips after a 5-second delay, “A” and “B” do not trip on low suction pressure due to time delays of 15 and 10 seconds, respectively.)
2. DEHC fully opens the turbine control valves, with postulated failure of the turbine bypass valves, resulting in reactor pressure, power, and water level operating at higher values. However, RPV water level did not reach Level 8.

### 3.2.3 EOP Entry Conditions

No EOP entry conditions.

### 3.2.4 Operator Actions per RPV Control EOP with postulated PPS CCF

No entry into the EOPs for operator action for mitigating this event. However, upon recognition of unexpected increase in reactivity, operator will take action to reduce reactor power or shutdown the reactor in accordance with procedure OT-104 (Reference 10) and OT-102, "High Reactor Pressure" (Reference 48). Upon recognition of a reactor feedpump trip, operator may also take action in accordance with procedure OT-100, "Reactor Low Level" (Reference 47) to reduce reactor power to less than 85%. Because automatic level control is lost, the operator may initiate a reactor scram. Because of the postulated failure of the turbine bypass valves, ADS SRVs may be used for reactor depressurization.

Required operator response time for manual actions >10 minutes from initiation of event.



### 3.2.5 Summary of Diverse Features from PPS

Based upon the analysis for this event, the following diverse features are available, for the postulated CCF of the PPS:

1. Reactor water level NR & WR indication
2. Reactor pressure
3. Reactor Pressure High alarm
4. Reactor power (APRM)
5. APRM Not Downscale indication
6. Turbine Trip Status
7. Control rod position
8. Reactor feedpump turbine trip circuits - low suction pressures
9. DEHC
10. Woodward turbine speed control system
11. Manual scram pushbuttons
12. Manual Control of ADS SRVs

### 3.2.6 Conclusion

For the postulated event of Feedwater Controller Failure – Maximum Demand (without Turbine Bypass), concurrent with a postulated CCF of PPS, sufficient automatic control functions and information that are/will be independent of the PPS are available to mitigate the event with the addition of the diverse manual control of individual ADS SRVs. The reactor core is adequately cooled and RCPB integrity is maintained. Since this transient does not result in any fuel failures or any release of primary coolant to either the secondary containment or the environment, there are no radiological consequences associated with this transient. Thus, BTP 7-19 3.3(b) Acceptance Criteria for this AOO are satisfied.

## 3.3 EVENT: 15.1.2 FEEDWATER CONTROL FAILURE – MAXIMUM DEMAND (WITH BYPASS)

Feedwater controller demand is postulated to fail upscale that results in maximum feedwater injection into the RPV, resulting in a rapid water level rise and a trip of the main turbine and the turbine-driven feedpump turbines when water level reaches the Level 8 trip setpoint. This event is considered to be an incident of moderate frequency.

### 3.3.1 Sequence of Events (UFSAR Table 15.1-3):

<u>TIME (sec)</u>	<u>EVENT (1) (WITH TURBINE BYPASS)</u>
0	Initiate simulated failure of feedwater controller to upper limit on feedwater flow.
8.4	**Level 8 vessel level setpoint trips main turbine and feedwater pumps.**
8.4	**Reactor scram trip actuated from main turbine stop valve position switches.**



<u>TIME (sec)</u>	<u>EVENT (1) (WITH TURBINE BYPASS)</u>
8.4	**RPT actuated by stop valve position switches.**
8.6	**Main turbine stop valves closed and turbine bypass valves start to open.**
8.6	**Recirculation pump motor circuit breakers open causing recirculation drive flow to start to coast down.**
11.2	First group of SRVs open due to high pressure.

### 3.3.2 Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS

1. Reactor feedpump “C” trips on low suction pressure, with feedpumps “A” and “B” injecting water at their maximum rate of approximately 16 Mlb/hr. (Note: Feedpump turbine “C” trips after a 5-second delay, “A” and “B” do not trip on low suction pressure due to time delays of 15 and 10 seconds, respectively. However, RPV water level did not reached Level 8)
2. DEHC modulates the turbine control and bypass valves to control pressure.

### 3.3.3 EOP Entry Conditions

No EOP entry conditions

### 3.3.4 Operator Actions per RPV Control EOPs with postulated PPS CCF

No entry into the EOPs for operator action for mitigating this event. However, upon recognition of unexpected increase in reactivity, operator will take action to reduce reactor power or shutdown the reactor in accordance with procedure OT-104 (Reference 10) and OT-102 (Reference 48). Upon recognition of a reactor feedpump trip, operator may also take action in accordance with procedure OT-100 (Reference 47), to reduce reactor power to less than 85%. Because automatic level control is lost, the operator may initiate a reactor scram.

Estimated Time Available for Operator Actions: >10 minutes.

### 3.3.5 Summary of Diverse Features from PPS

Based upon the analysis for this event, the following diverse indications are available, for the postulated CCF of the PPS:

1. Reactor water level NR & WR indication
2. Reactor pressure
3. Reactor power (APRM)
4. APRM Not Downscale indication
5. Turbine Trip Status
6. Control rod position
7. Reactor feedpump turbine trip circuits - low suction pressures



8. DEHC
9. Woodward turbine speed control system
10. Manual scram pushbuttons

### 3.3.6 Conclusion

For the postulated event of Feedwater Controller Failure – Maximum Demand, with Bypass, concurrent with a postulated CCF of PPS, sufficient automatic and manual control functions, and information that are independent of the PPS are available to mitigate the event. The reactor core is adequately cooled and RCPB integrity is maintained. Since this transient does not result in any fuel failures or any release of primary coolant to either the secondary containment or the environment, there are no radiological consequences associated with this transient. Thus, BTP 7-19 3.3(b) Acceptance Criteria for this AOO are satisfied.

## 3.4 EVENT: 15.1.3 PRESSURE REGULATOR FAILURE-OPEN

If the controlling regulator fails, the backup controller will take over control with a “bumpless” switchover. If both controllers fail to the open position, the turbine control valves can be fully opened, and the turbine bypass valves can be partially or fully opened until the maximum steam flow is established. This event is categorized as an incident of moderate frequency.

### 3.4.1 Sequence of Events (UFSAR Table 15.1-4)

<u>TIME (sec)</u>	<u>EVENT</u>
0.0	Simulate maximum limit flow to main turbine.
0.4	Main turbine bypass valves open.
4.7	**Vessel water level (Level 8) trip initiates main turbine and feedwater turbine trips.**
4.7	**Main turbine stop valve position initiates reactor scram and RPT.**
4.8	**Turbine stop valves closed.**
4.9	**Recirculation pump motor circuit breakers open causing decrease in core flow to natural circulation.**
46.8	**Main steam line isolation on low turbine inlet pressure.**
51.8	**MSIVs closed**. Bypass valves remain open, exhausting steam in steam lines downstream of isolation valves.
52.0	**RCIC and HPCI systems initiation on low level (Level 2).**
>100.0	Group 1 Main Steam Relief Valves (MSRVs) actuate and cycle.



### 3.4.2 Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS

1. MSIVs isolate on Main Steam Line Pressure – Low. (Note: Needed to avoid uncontrolled blowdown of RPV.)
2. After MSIVs are closed, main turbine trips on reverse power, and steam to the feedpump turbines is shut off.
3. Redundant Reactivity Control System (RRCS) initiates on High Reactor RPV Pressure resulting in reactor scram, and Recirculation Pump Trip (RPT actuation).

### 3.4.3 EOP Entry Conditions

The operator will promptly enter T-101, “RPV Control RC/L, RC/P (Flowchart) (Reference 14), upon recognition of any of the following entry conditions:

1. RPV water level below +12.5 inches (Level 3)
2. RPV pressure above 1096 psig
3. A reactor scram condition with APRM above 4%

### 3.4.4 Operator Actions per RPV Control EOPs with postulated PPS CCF

1. Enter T-101 (Reference 14). Monitor RPV water level, pressure, power, control rod positions.
2. If reactor scram has not initiated, initiate a reactor scram.
3. Stabilize RPV pressure at a pressure below 1096 psig using ADS SRVs.
4. Depressurize the RPV using ADS SRVs to the desired pressure, at a cooldown rate below 100°F/hr.
5. Restore and maintain RPV water level between +12.5 inches and +54 inches using condensate pumps when RPV pressure decreases below pump shutoff head (approximately 680 psig).

Estimated Time Available for Operator Actions: >10 minutes from initiation of event.

### 3.4.5 Summary of Diverse Features from PPS

Based upon the analysis for this event, the following diverse features are available, for the postulated CCF of the PPS:

1. Reactor water level NR, WR, and FZ indications
2. Reactor Water Level Low (Level 3) alarm
3. Reactor pressure



4. Reactor power (APRM)
5. APRM Not Downscale indication
6. Control rod position indications
7. RRCS
8. Manual control of ADS SRVs
9. Auto MSIV isolation on Main Steam Line Pressure- Low
10. Manual controls of feedwater injection using the condensate pumps
11. Main steam line pressure
12. Manual scram pushbuttons

### 3.4.6 Conclusion

For the postulated event of Pressure Regulator Failure - Open, concurrent with a postulated CCF of PPS, sufficient automatic control functions, indications that are /will be independent of the PPS, and operator actions, will be available to mitigate the event with the added DPS functions. The reactor core is adequately cooled and RCPB integrity is maintained. Since this transient does not result in any fuel failures or any release of primary coolant to either the secondary containment or the environment, there are no radiological consequences associated with this transient. Thus, BTP 7-19 3.3(b) Acceptance Criteria for this AOO are satisfied.

## 3.5 EVENT: 15.1.4 INADVERTENT MAIN STEAM RELIEF VALVE OPENING

Cause of inadvertent MSR/V opening is attributed to malfunction of the valve or an operator initiated opening. Opening and closing circuitry at the individual valve level (as opposed to groups of valves) is subject to a single failure event. It is therefore simply postulated that a failure occurs, and the transient is analyzed accordingly. This event is categorized as an infrequent incident but is analyzed as an incident of moderate frequency.

### 3.5.1 Sequence of Events (UFSAR Table 15.1-5)

<u>TIME (sec)</u>	<u>EVENT</u>
0	Initiate opening of one MSR/V.
0.5(est)	MSRV flow reaches full flow.
15.0(est)	System establishes new steady-state operation.

### 3.5.2 Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS

1. DEHC (pressure regulator) closes the turbine control valves slightly to control pressure.
2. DFWLCS maintains normal level control.
3. No safety control action is needed. Reactor remains on-line with generator output reduced by the capacity of one SRV.



### 3.5.3 EOP Entry Conditions

The operator will promptly enter the T-102, “Primary Containment Control SP/T, SP/L, PC/P, DW/T, PC/H (Flowchart)” (Reference 15), upon recognition of the following entry conditions:

1. Suppression pool temperature above 95°F (indication or alarm)

### 3.5.4 Operator Actions per EOPs with postulated PPS CCF

1. Enter T-102 (Reference 15).
  - a. Before suppression pool temperature reaches 110 ° F, enter T-101 (Reference 14) concurrently and initiate a manual scram.
2. Enter T-101 (Reference 14) from 1(a) above.
  - a. Monitor RPV water level, pressure, power, control rod positions.
  - b. Restore and maintain RPV water level between +12.5 inches and +54 inches using DFWLCS.
  - c. Stabilize RPV pressure at a pressure below 1096 psig using the turbine bypass valves.

Estimated Time Available for Operator Actions: >10 minutes, based upon the following:

UFSAR Section 15.1.4.2.1 states: “If it is assumed that the suppression pool is at its maximum operating temperature (95°F) and minimum operating volume with no pool cooling systems in operation when the valve first opens, the operator will have more than 6 minutes before the pool scram temperature of 110°F is reached. If the above worst case assumptions were relaxed, the time for operator action would increase.

Delaying the reactor scram to 10 minutes after the valve sticks full open would have no adverse effect on plant safety. Even though the suppression pool temperature would approach 120°F at the time of scram, the maximum allowable suppression pool temperature limits would not be exceeded.”

### 3.5.5 Summary of Diverse Features from PPS

Based upon the analysis for this event, the following diverse features are available, for the postulated CCF of the PPS:

1. Suppression pool temperature indication
2. Suppression pool temperature high alarm
3. Reactor water level NR indication
4. Reactor pressure
5. Reactor power (APRM)
6. APRM Not Downscale indication
7. Control rod position indications
8. DFWLCS
9. DEHC
10. Manual scram pushbuttons



### 3.5.6 Conclusion

For the postulated event of Inadvertent Main Steam Relief Valve Opening, concurrent with a postulated CCF of PPS, sufficient automatic control functions, indications that are independent of the PPS, and operator actions, are available to mitigate the event. The reactor core is adequately cooled and RCPB integrity is maintained. Since this transient does not result in any release of primary coolant to either the secondary containment or the environment, there are no radiological consequences associated with this transient. Thus, BTP 7-19 3.3(b) Acceptance Criteria for this AOO are satisfied.

## 3.6 EVENT: 15.1.6 INADVERTENT RHR SHUTDOWN COOLING OPERATION

If the reactor were critical or near critical in a startup or cooldown condition, a slow increase in reactor power could result. A shutdown cooling malfunction leading to a moderator temperature decrease could result from mis-operation of the cooling water controls for the RHR heat exchangers. The resulting temperature decrease would cause a slow insertion of positive reactivity into the core. If the operator did not act to control the power level, a high neutron flux reactor scram would terminate the transient without violating fuel thermal limits and without any measurable increase in nuclear system pressure. This event is categorized as a transient of moderate frequency.

### 3.6.1 Sequence of Events (UFSAR Table 15.1-1)

<u>TIME (min)</u>	<u>EVENT</u>
0	Reactor at low power and low pressure when RHR shutdown cooling inadvertently activated.
0 – 10	Slow rise in reactor power.
+10	Operator may take action to limit power rise. **Flux scram will occur if no action is taken.**

### 3.6.2 Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS

1. DEHC (pressure regulator) maintains normal pressure control
2. DFWLCS maintains normal level control

### 3.6.3 EOP Entry Conditions

Assuming no operator action to limit power rise, the operator will promptly enter T-101 (Reference 14) with a reactor scram condition with APRM above 4%.

### 3.6.4 Operator Actions

Assuming that RHR shutdown cooling operation is in progress, and then a PPS CCF occurs rendering RHR controls inoperable, relevant operator actions are:



1. Isolate shutdown cooling
2. Insert control rods to limit rise in neutron flux
3. Enter T-101 (Reference 14), if applicable, and initiate a manual scram

Estimated Time Available for Operator Actions: >10 minutes

### 3.6.5 Summary of Diverse Features from PPS

1. Reactor water level NR indication
2. Neutron flux (IRM / APRM)
3. Rod control and position display
4. DFWLCS
5. DEHC
6. Isolation of RHR shutdown cooling (diverse isolation identified in Position 4 analysis)
7. Manual scram pushbuttons

### 3.6.6 Conclusion

For the postulated event of Inadvertent RHR Shutdown Cooling Operation, existing diverse displays and controls for reactivity are sufficient to mitigate the postulated event. Manual scram push buttons are hardwired in the PPS design and not susceptible to a CCF. The reactor core is adequately cooled and RCPB integrity is maintained. Since this transient does not result in any release of primary coolant to either the secondary containment or the environment, there are no radiological consequences associated with this transient. Thus, BTP 7-19 3.3(b) Acceptance Criteria for this AOO are satisfied.

## 3.7 EVENT: 15.2.1 PRESSURE REGULATOR FAILURE – CLOSED

It is assumed, for the purposes of this transient analysis that a single failure occurs, erroneously causes the controlling regulator processor to close the main turbine control valves. Failure of the primary controlling regulator processor results in the automatic “bumpless” transfer between the primary and the backup regulator controllers, thereby preventing an increase in reactor pressure. This event is treated as a moderate frequency event.

### 3.7.1 Sequence of Events

When a fault is detected with the controlling pressure regulator processor, as discussed in UFSAR Section 15.2.1.1.1, an automatic “bumpless” failover will occur to the back-up redundant regulator controller. The pressure increase will be small, if any. Both regulators receive the same setpoint value from the operator input via the Human Machine Interface (HMI), thus, pressure will be controlled at approximately the same value prior to the assumed failure.

### 3.7.2 Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS

1. Pressure control system (DEHC) maintains normal pressure control, an automatic “bumpless” failover will occur to the back-up redundant regulator controller. The pressure increase will be



small, if any. Pressure will be controlled at approximately the same value prior to the assumed failure.

2. DFWLCS maintains normal level control.

### 3.7.3 EOP Entry Conditions

No EOP Entry Conditions.

### 3.7.4 Operator Actions

None required to mitigate this event. No PPS action is required.

Estimated Time Available for Operator Actions: N/A. No operator action required.

### 3.7.5 Summary of Diverse Features from PPS

Based upon the analysis for this event, the following diverse features are required, for the postulated CCF of the PPS:

1. Reactor water level NR indication
2. Reactor pressure indication
3. DFWLCS
4. DEHC

### 3.7.6 Conclusion

For the postulated event of Pressure Regulator Failure-Closed, concurrent with a postulated CCF of PPS, sufficient automatic control functions and indications that are independent of the PPS, are available to monitor the reactor conditions. BTP 7-19 Acceptance Criteria are not applicable.

## 3.8 EVENT: 15.2.2 GENERATOR LOAD REJECTION WITH BYPASS FAILURE

A generator load rejection is assumed to occur with failure of the turbine steam bypass valves to open. This event is categorized as an incident of moderate frequency.

### 3.8.1 Sequence of Events (UFSAR Table 15.2-2)

<u>TIME (sec)</u>	<u>EVENT</u>
-0.015 (approx.)	Turbine-generator detection of loss of electrical load.
0.0	Turbine-generator power load unbalance devices trip to initiate turbine control valve fast closure.
0.0	Turbine bypass valves fail to operate.



0.0	**Fast control valve closure initiates scram trip.**
0.0	**Turbine control valve closure initiates a recirculation pump trip (RPT).**
0.08 (approx.)	Turbine control valve closed.
0.175	**Recirculation pump motor circuit breakers open causing the recirculation drive flow to begin to coast down.**
1.9	MSRV actuation initiated.
> 6	MSRV closed.

### 3.8.2 Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS

1. RRCS initiates ARI on high RPV pressure resulting in reactor scram, and RPT actuation
2. DFWLCS maintains normal level control
3. SRVs cycle to relief pressure as required

### 3.8.3 EOP Entry Conditions

The operator will promptly enter T-101 (Reference 14) upon recognition of any of the following entry conditions:

1. RPV water level below +12.5 inches (Level 3)
2. RPV pressure above 1096 psig
3. A reactor scram condition with APRM above 4%

### 3.8.4 Operator Actions per RPV Control / Primary Containment Control EOP with postulated PPS CCF

1. Enter T-101 (Reference 14). Monitor RPV water level, pressure, power, control rod positions
2. Restore and maintain RPV water level between +12.5 inches and +54 inches using DFWLCS
3. Stabilize RPV pressure at a pressure below 1096 psig using ADS SRVs

Estimated Time Available for Operator Actions: >10 minutes



### 3.8.5 Summary of Diverse Features from PPS

Based upon the analysis for this event, the following diverse features are required, for the postulated CCF of the PPS:

1. Reactor water level NR indication
2. Reactor pressure
3. Reactor power (APRM)
4. APRM Not Downscale indication
5. Control rod position indications
6. RRCS
7. DFWLCS
8. Manual control of ADS SRVs

### 3.8.6 Conclusion

For the postulated event of Generator Load Rejection With Bypass Failure, concurrent with a postulated CCF of PPS, sufficient automatic control functions, indications that are independent of the PPS, and operator actions, are/will be available to mitigate the event. The reactor core is adequately cooled and RCPB integrity is maintained. Since this transient does not result in any release of primary coolant to either the secondary containment or the environment, there are no radiological consequences associated with this transient. Thus, BTP 7-19 3.3(b) Acceptance Criteria for this AOO are satisfied.

## 3.9 EVENT: 15.2.2 GENERATOR LOAD REJECTION WITH BYPASS

A generator load rejection is assumed to occur with normal operation of the turbine steam bypass valves to open. This event is categorized as an incident of moderate frequency.

### 3.9.1 Sequence of Events (UFSAR Table 15.2-1)

<u>TIME (sec)</u>	<u>EVENT</u>
-0.015 (approx.)	Turbine-generator detection of loss of electrical load.
0.0	Turbine-generator power load unbalance devices trip to initiate turbine control valve fast closure.
0.0	Turbine-generator power load unbalance trip initiates main turbine bypass system operation.
0.0	**Fast turbine control valve closure initiates scram trip.**
0.0	**Turbine control valve closure initiates an RPT.**
0.07	Turbine control valve closed.
0.14	Turbine bypass valves start to open.



0.175	**Recirculation pump motor circuit breakers open causing the recirculation drive flow to begin to coast down.**
2.0	Group 1 MSRV actuated.
2.15	Group 2 MSRVs actuated.
2.40	Group 3 MSRVs actuated.
3.90	Group 1 MSRV close.

### 3.9.2 Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS

1. RRCS initiates ARI on high RPV pressure resulting in reactor scram, and RPT actuation
2. DFWLCS maintains normal level control
3. SRVs cycle to relief pressure as required
4. Pressure control system modulates turbine bypass valves to control pressure

### 3.9.3 EOP Entry Conditions

The operator will promptly enter T-101 (Reference 14) upon recognition of any of the following entry conditions:

1. RPV water level below +12.5 inches (Level 3)
2. RPV pressure above 1096 psig
3. A reactor scram condition with APRM above 4%

### 3.9.4 Operator Actions per RPV Control / Primary Containment Control EOP with postulated PPS CCF

1. Enter T-101 (Reference 14). Monitor RPV water level, pressure, power, control rod positions.
2. Restore and maintain RPV water level between +12.5 inches and +54 inches using DFWLCS.
3. Stabilize RPV pressure at a pressure below 1096 psig using the turbine bypass valves.

Estimated Time Available for Operator Actions: >10 minutes

### 3.9.5 Summary of Diverse Features from PPS

Based upon the analysis for this event, the following diverse features are required, for the postulated CCF of the PPS:

1. Reactor water level NR indication



2. Reactor pressure
3. Reactor power (APRM)
4. APRM Not Downscale indication
5. Control rod position indications
6. RRCS
7. DFWLCS
8. DEHC

### 3.9.6 Conclusion

For the postulated event of Generator Load Rejection with Bypass, concurrent with a postulated CCF of PPS, sufficient automatic control functions, indications that are independent of the PPS, and operator actions, are available to mitigate the event. The reactor core is adequately cooled and RCPB integrity is maintained. Since this transient does not result in any release of primary coolant to either the secondary containment or the environment, there are no radiological consequences associated with this transient. Thus, BTP 7-19 3.3(b) Acceptance Criteria for this AOO are satisfied.

### 3.10 EVENT: 15.2.3 TURBINE TRIP WITHOUT BYPASS

A main turbine trip is assumed to occur with failure of the turbine steam bypass valves to open. This event is categorized as an incident of moderate frequency.

#### 3.10.1 Sequence of Events (UFSAR Table 15.2-4)

<u>TIME (sec)</u>	<u>EVENT</u>
0.0	Turbine trip initiates closure of main stop valves.
0.0	Turbine bypass valves fail to operate.
0.01	**Main turbine stop valves reach 90% open position and initiate reactor scram trip.**
0.01	**Main turbine stop valves reach 90% open position and initiate an RPT.**
0.1	Turbine stop valves closed.
0.175	**Recirculation pump motor circuit breakers open causing the recirculation drive flows to coast down.**
~ 1.8	MSRV actuation initiated.
> 6	MSRVs closed.

#### 3.10.2 Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS

1. RRCS initiates ARI on high RPV pressure resulting in reactor scram, and RPT actuation



2. DFWLCS maintains normal level control of RPV water level
3. SRVs cycle to relief pressure as required

### 3.10.3 EOP Entry Conditions

The operator will promptly enter T-101 (Reference 14) upon recognition of any of the following entry conditions:

1. RPV water level below +12.5 inches (Level 3)
2. RPV pressure above 1096 psig
3. A reactor scram condition with APRM above 4%

### 3.10.4 Operator Actions per RPV Control EOP with postulated PPS CCF

1. Enter T-101 (Reference 14). Monitor RPV water level, pressure, power, control rod positions
2. Restore and maintain RPV water level between +12.5 inches and +54 inches using DFWLCS
3. Stabilize RPV pressure at a pressure below 1096 psig using ADS SRVs

Estimated Time Available for Operator Actions: >10 minutes

### 3.10.5 Summary of Diverse Features from PPS

Based upon the analysis for this event, the following diverse features are required, for the postulated CCF of the PPS:

1. Reactor Water Level NR indication
2. Reactor Water Level Low (Level 3) alarm
3. Reactor pressure indication
4. Reactor power (APRM)
5. APRM Not Downscale indication
6. Control rod position indications
7. RRCS
8. DFWLCS
9. Manual control of ADS SRVs

### 3.10.6 Conclusion

For the postulated event of Turbine Trip Without Bypass, concurrent with a postulated CCF of PPS, sufficient automatic control functions, indications that are independent of the PPS, and operator actions, are/will be available to mitigate the event. The reactor core is adequately cooled and RCPB integrity is maintained. Since this transient does not result in any release of primary coolant to either the secondary containment or the environment, there are no radiological consequences associated with this transient. Thus, BTP 7-19 3.3(b) Acceptance Criteria for this AOO are satisfied.



### 3.11 EVENT: 15.2.3 TURBINE TRIP WITH BYPASS

A main turbine trip is assumed to occur with normal operation of the turbine steam bypass valves to open. This event is categorized as an incident of moderate frequency.

#### 3.11.1 Sequence of Events (UFSAR Table 15.2-3)

<u>TIME (sec)</u>	<u>EVENT</u>
0.0	Turbine trip initiates closure of main stop valves.
0.0	Turbine trip initiates bypass operation.
0.01	**Main turbine stop valves reach 90% open position and initiates reactor scram trip.**
0.01	**Main turbine stop valves reach 90% open position and initiates an RPT.**
0.1	Turbine stop valves closed.
0.17	Turbine bypass valves start to open to regulate pressure.
2.5	Group 1 MSRVs actuated.
2.7	Group 2 MSRVs actuated.
2.9	Group 3 MSRVs actuated.
8.3	All MSRVs closed.

#### 3.11.2 Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS

1. RRCS initiates ARI on high RPV pressure resulting in reactor scram, and RPT actuation
2. DFWLCS maintains normal level control of RPV water level
3. SRVs cycle to relief pressure as required
4. Pressure control system modulates turbine bypass valves to control pressure

#### 3.11.3 EOP Entry Conditions

The operator will promptly enter T-101 (Reference 14) upon recognition of any of the following entry conditions:

1. RPV water level below +12.5 inches (Level 3)
2. RPV pressure above 1096 psig
3. A reactor scram condition with APRM above 4%



### 3.11.4 Operator Actions per RPV Control EOP with postulated PPS CCF

1. Enter T-101 (Reference 14). Monitor RPV water level, pressure, power, control rod positions.
2. Restore and maintain RPV water level between +12.5 inches and +54 inches using DFWLCS.
3. Stabilize RPV pressure at a pressure below 1096 psig using the turbine bypass valves.

Estimated Time Available for Operator Actions: >10 minutes

### 3.11.5 Summary of Diverse Features from PPS

Based upon the analysis for this event, the following diverse features are required, for the postulated CCF of the PPS:

1. Reactor water level NR indication
2. Reactor pressure
3. Reactor power (APRM)
4. APRM Not Downscale indication
5. Control rod position indications
6. RRCS
7. DFWLCS
8. DEHC

### 3.11.6 Conclusion

For the postulated event of Turbine Trip with Bypass, concurrent with a postulated CCF of PPS, sufficient automatic control functions, indications that are independent of the PPS, and operator actions, are available to mitigate the event. The reactor core is adequately cooled and RCPB integrity is maintained. Since this transient does not result in any release of primary coolant to either the secondary containment or the environment, there are no radiological consequences associated with this transient. Thus, BTP 7-19 3.3(b) Acceptance Criteria for this AOO are satisfied.

## 3.12 EVENT: 15.2.4 MSIV CLOSURE

An inadvertent closure of all MSIVs is assumed for this event. This event is categorized as an incident of moderate frequency. The closure of one MSIV is not quantitatively analyzed in UFSAR Section 15.2.4.

### 3.12.1 Sequence of Events (UFSAR Table 15.2-5)

<u>TIME (sec)</u>	<u>EVENT</u>
0.0	Initiate closure of all MSIVs.
0.3	**MSIV position trip scram initiated.**



- 2.9                    \*\*Recirculation pump drive motors are tripped.\*\*
- 3.1                    MSRVs open 3 groups due to pressure relief setpoint action.
- 14.6                  All MSRVs closed.
- 26.0                  \*\*Initiate HPCI and RCIC systems on low-low water level (Level 2).\*\*

### 3.12.2 Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS

1. RRCS initiates ARI on high RPV pressure resulting in reactor scram, and RPT actuation.
2. Feedpump turbines trip with steam flow cutoff by closure of MSIVs and depressurization of main steam lines.
3. SRVs cycle to relief pressure as required.
4. Rapid decrease in steam line pressure results in closure of turbine control valves by the Digital Electro-Hydraulic Control System (DEHC) pressure regulator and subsequent turbine trip on reverse power.

### 3.12.3 EOP Entry Conditions

The operator will promptly enter T-101 (Reference 14) upon recognition of any of the following entry conditions:

1. RPV water level below +12.5 inches (Level 3)
2. RPV pressure above 1096 psig
3. A reactor scram condition with APRM above 4%

### 3.12.4 Operator Actions per RPV Control EOP with postulated PPS CCF

1. Enter T-101 (Reference 14). Monitor RPV water level, pressure, power, control rod positions.
2. Stabilize RPV pressure at a pressure below 1096 psig using ADS SRVs.
3. Depressurize the RPV and maintain the cooldown rate below 100°F/hr using ADS SRVs.
4. Restore and maintain RPV water level between +12.5 inches and +54 inches using condensate pumps when RPV pressure decreases below pump shutoff head (approximately 680 psig).

Estimated Time Available for Operator Actions: >10 minutes



### 3.12.5 Summary of Diverse Features from PPS

Based upon the analysis for this event, the following diverse features are required, for the postulated CCF of the PPS:

1. Reactor water level NR and WR indication
2. Reactor Water Level Low (Level 3) alarm
3. Reactor pressure
4. Reactor power (APRM)
5. APRM Not Downscale indication
6. Control rod position indications
7. RRCS
8. DEHC
9. Manual control of ADS SRVs
10. Manual controls of feedwater injection using the condensate pumps

### 3.12.6 Conclusion

For the postulated event of MSIV Closure, concurrent with a postulated CCF of PPS, sufficient automatic control functions, indications that are independent of the PPS, and operator actions, are/will be available to mitigate the event. The reactor core is adequately cooled, RCPB and primary containment integrity are maintained. Thus, BTP-7-19 Acceptance Criteria are satisfied.

## 3.13 EVENT: 15.2.5 LOSS OF CONDENSER VACUUM

Condenser vacuum is assumed to be lost at a rate of approximately 2 inches Hg per second. This event is categorized as an incident of moderate frequency.

### 3.13.1 Sequence of Events (UFSAR Table 15.2-7)

<u>TIME (sec)</u>	<u>EVENT</u>
-3.0	Initiate simulated loss of condenser vacuum at 2 inches of Hg per second.
0.0 (est)	Low condenser vacuum main turbine trip actuated.
0.0 (est)	Low condenser vacuum feedwater trip actuated.
0.01	**Main turbine trip initiates reactor scram.**
0.01	**Main turbine trip initiates RPT.**
0.1	Turbine stop valves closed.
0.1	Bypass valves begin to open.
2.5	Group 1 MSRV setpoints actuated.



2.7	Group 2 MSRV setpoints actuated.
2.9	Group 3 MSRV setpoints actuated.
5.0	**Low condenser vacuum initiates MSIV closure.**
5.0	Low condenser vacuum initiates bypass valve closure.
13.3	All MSRVs close.
16.9	MSRV cyclic actuation on pressure demand.
50.6	**HPCI/RCIC system initiation on low level (Level 2)** (not included in simulation)

### 3.13.2 Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS

1. RRCS initiates ARI on high RPV pressure resulting in reactor scram, and RPT actuation
2. SRVs cycle to relief pressure as required
3. DEHC closes turbine bypass valves upon low vacuum

### 3.13.3 EOP Entry Conditions

The operator will promptly enter T-101 (Reference 14) upon recognition of any of the following entry conditions:

1. RPV water level below +12.5 inches (Level 3)
2. RPV pressure above 1096 psig
3. A reactor scram condition with APRM above 4%

### 3.13.4 Operator Actions per RPV Control EOP with postulated PPS CCF

1. Enter T-101 (Reference 14). Monitor RPV water level, pressure, power, control rod positions.
2. Stabilize RPV pressure at a pressure below 1096 psig using ADS SRVs.
3. Depressurize the RPV and maintain the cooldown rate below 100 ° F/hr using ADS SRVs.
4. Restore and maintain RPV water level between +12.5 inches and +54 inches using condensate pumps when RPV pressure decreases below pump shutoff head (approximately 680 psig).

Estimated Time Available for Operator Actions: >10 minutes



### 3.13.5 Summary of Diverse Features from PPS

Based upon the analysis for this event, the following diverse features are required, for the postulated CCF of the PPS:

1. Reactor water level NR and WR indication
2. Reactor Water Level Low (Level 3) alarm
3. Reactor pressure
4. Reactor power (APRM)
5. APRM Not Downscale indication
6. Control rod position indications
7. RRCS
8. Manual control of ADS SRVs
9. DEHC
10. Manual controls of feedwater injection using the condensate pumps

### 3.13.6 Conclusion

For the postulated event of Loss of Condenser Vacuum, concurrent with a postulated CCF of PPS, sufficient automatic control functions, indications that are independent of the PPS, and operator actions, are/will be available to mitigate the event. The reactor core is adequately cooled and RCPB integrity is maintained. Since this transient does not result in any release of primary coolant to either the secondary containment or the environment, there are no radiological consequences associated with this transient. Thus, BTP 7-19 3.3(b) Acceptance Criteria for this AOO are satisfied.

## 3.14 EVENT: 15.2.6 LOSS OF ALL GRID CONNECTIONS

Loss of all grid connections can result from major shifts in electrical loads, seismic events, loss of loads, lightning, storms, wind, etc., that contribute to electrical grid instabilities. These instabilities cause equipment damage if unchecked. Protective relay schemes automatically disconnect electrical sources and loads to mitigate damage and regain electrical grid stability. The loss of all grid connections causes the loss of all auxiliary power. This transient consists of a generator load rejection and recirculation pump trip at time t=0. This event is categorized as an incident of moderate frequency.

### 3.14.1 Sequence of Events (UFSAR Table 15.2-10)

<u>TIME (sec)</u>	<u>EVENT</u>
-0.015 (approx.)	Loss of grid causes turbine-generator to detect a loss of electrical load.
0.0	Turbine control valve fast closure is initiated.
0.0	Turbine-generator power load unbalance trip initiates main turbine bypass system operation.
0.0	Recirculation system pump motors are tripped.



0.0	**Turbine control valve fast closure initiates a reactor scram trip.**
0.07	Turbine control valves closed.
0.10	Turbine bypass valves begin to open.
2.0	Feedwater pumps trip on low suction pressure.
2.4	MSRVs open and cycle.
7.2	Initial SRVs closure.
49	**Low water Level 2 setpoint reached, HPCI/RCIC initiated** (not simulated).

### 3.14.2 Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS

1. RRCS initiates ARI on high RPV pressure resulting in reactor scram, and RPT actuation.
2. Pressure control system modulates turbine bypass valves to control pressure until inhibited by low condenser vacuum, or until the bypass valve accumulators are depleted.
3. SRVs cycle to relief pressure as required.
4. Initiate one loop of CS when RPV water level decreases below Level 1(-129 inches).\*

\*From 6.3.2.5 of UFSAR (Reference 7):

“Certain technical specification LCO periods are justified based on NEDO-24708A which states that for postulated LOCAs, one low pressure ECCS (one LPCI loop or one CS loop) and ADS to depressurize is adequate to reflood the vessel and maintain core cooling sufficient to preclude fuel damage. NEDC-30936P-A, specifically applicable to LGS references NEDO-24708A and reaffirms this conclusion, with the advisory regarding the possible necessity of an alternate cooling path following 2 hours of post large-break LOCA LPCI injection into the core shroud.” Due to its design simplicity, one CS loop is chosen to provide a diverse ECCS backup.

### 3.14.3 EOP Entry Conditions

The operator will promptly enter T-101 (Reference 14) upon recognition of any of the following entry conditions:

1. RPV water level below +12.5 inches (Level 3)
2. RPV pressure above 1096 psig
3. A reactor scram condition with APRM above 4%

### 3.14.4 Operator Actions per RPV Control EOP with postulated PPS CCF

1. Enter T-101 (Reference 14). Monitor RPV water level, pressure, power, control rod positions.



2. Stabilize RPV pressure at a pressure below 1096 psig using ADS SRVs.
3. Depressurize the RPV, using ADS SRVs and maintain the cooldown rate below 100°F/hr.
4. Before RPV level reaches -186 inches (MSCRWL), Emergency Depressurization is required (using ADS SRVs).
5. Restore and maintain RPV water level between +12.5 inches and +54 inches using one loop of CS when RPV pressure decreases below pump shutoff head (approximately 335 psig).

Estimate of Time Available for Operator Actions: >10 minutes

### 3.14.5 Summary of Diverse Features from PPS

Based upon the analysis for this event, the following diverse features are required, for the postulated CCF of the PPS:

1. Reactor water level NR, WR, and FZ indication
2. Reactor Water Level Low (Level 3) alarm
3. Reactor pressure
4. Reactor power (APRM)
5. APRM Not Downscale indication
6. Control rod position indications
7. RRCS
8. Auto initiation of CS Loop-A on Level 1(-129 inches)
9. CS Loop-A flow
10. CS Loop-A pressure
11. Manual control of ADS SRVs

### 3.14.6 Conclusion

For the postulated event of Loss of All Grid Connections, concurrent with a postulated CCF of PPS, 1) sufficient automatic control functions, 2) indications that are independent of the PPS, and 3) operator actions, are/will be available to mitigate the event. The reactor core is adequately cooled and RCPB integrity is maintained. Since this transient does not result in any release of primary coolant to either the secondary containment or the environment, there are no radiological consequences associated with this transient. Thus, BTP 7-19 3.3(b) Acceptance Criteria for this AOO are satisfied.

## 3.15 EVENT: 15.2.7 LOSS OF FEEDWATER

A total loss of feedwater flow could occur due to pump failures, feedwater controller failures, operator errors, or reactor system variables such as a high vessel water level (Level 8) trip signal. This event is categorized as an incident of moderate frequency.



### 3.15.1 Sequence of Events (UFSAR Table 15.2-11)

<u>TIME (sec)</u>	<u>EVENT</u>
0.0	Trip of all feedwater pumps initiated.
~6	**Vessel water level (Level 3) trip initiates scram trip.**
~19	**Vessel water level (Level 2) trip initiates RCIC (and HPCI) operation.**
~19	**Vessel water level (Level 2) trip initiates containment isolation.**
~19	**Vessel water level (Level 2) trip initiates recirculation pump trip.**
~74	**Rated RCIC flow is achieved.**
~800	Minimum Level is reached (444 inches above vessel zero), approx. 45.5 inches above Level 1 trip.

### 3.15.2 Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS

1. RRCS initiates upon condition of Reactor Water Level 2:
  - i. ARI initiation (Level 2)
  - ii. RPT actuation (Level 2 with 9 second delay)
2. Main turbine trips after reactor trip due to closure of turbine control valves on reverse power condition. Bypass valves open to control pressure as required.
3. Initiate one loop of CS when RPV water level decreases below Level 1(-129 inches).

### 3.15.3 EOP Entry Conditions

The operator will promptly enter T-101 (Reference 14) upon recognition of any of the following entry conditions:

1. RPV water level below +12.5 inches (Level 3)
2. RPV pressure above 1096 psig
3. A reactor scram condition with APRM above 4%

### 3.15.4 Operator Actions per RPV Control EOP with postulated PPS CCF

1. Enter T-101 (Reference 14). Monitor RPV water level, pressure, power, control rod positions.
2. Stabilize RPV pressure at a pressure below 1096 psig using the turbine bypass valves.



3. Depressurize the RPV to the desired pressure, using the turbine bypass valves and maintain the cooldown rate below 100°F/hr.
4. Before RPV level reaches -186 inches (MSCRWL), Emergency Depressurization is required (using ADS SRVs).
5. Restore and maintain RPV water level between +12.5 inches and +54 inches.

Estimated Available Time for Operator Actions: > 10 minutes

### 3.15.5 Summary of Diverse Features from PPS

Based upon the analysis for this event, the following diverse features are required, for the postulated CCF of the PPS:

1. Reactor water level NR, WR, and FZ indication
2. Reactor Water Level Low (Level 3) alarm
3. Reactor pressure
4. Reactor power (APRM)
5. APRM Not Downscale indication
6. Control rod position indications
7. RRCS
8. DEHC
9. Auto initiation of CS Loop-A on Level 1
10. CS Loop-A flow
11. CS Loop-A pressure
12. Manual control of ADS SRVs

### 3.15.6 Conclusion

For the postulated event of Loss of Feedwater, concurrent with a postulated CCF of PPS, sufficient automatic control functions, indications that are independent of the PPS, and operator actions, are/will be available to mitigate the event. The reactor core is adequately cooled and RCPB integrity is maintained. Since this transient does not result in any release of primary coolant to either the secondary containment or the environment, there are no radiological consequences associated with this transient. Thus, BTP 7-19 3.3(b) Acceptance Criteria for this AOO are satisfied. Performance of this scenario at the plant simulator demonstrated that the operator actions are appropriate and adequate to maintain the core covered and thus fuel clad temperature below its limit.

## 3.16 EVENT: 15.2.9 LOSS OF SHUTDOWN COOLING

For evaluation purposes, it is assumed that plant shutdown is initiated by a transient event (Loss of Offsite Power [LOOP]) that results in reactor isolation/scram and subsequent relief valve actuation and suppression pool heatup. After subsequent reactor trip and isolation, the reactor is depressurized to 75 psig at which pressure shutdown cooling can be initiated. The event is categorized as an incident of moderate frequency.



### 3.16.1 Sequence of Events (UFSAR Table 15.2-12)

<u>TIME (min)</u>	<u>EVENT</u>
0	Reactor is operating at 3528 MWt when LOOP occurs initiating plant shutdown.
0	Concurrently, loss of one division of power occurs.
10	Controlled depressurization initiated (100%) using selected MSRVs.
15	Suppression pool cooling initiated to prevent overheating from MSRV actuation.
157	Blowdown to approximately 75.0 psig completed.
157	Personnel are sent in to open RHR shutdown cooling suction valve; this fails.
187	**Actuate core spray into vessel and reopen ADS valves to establish alternate cooling path.**

### 3.16.2 Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS

Note that as a result of LOOP, MSIVs isolate resulting in reactor trip, loss of steam to drive the feedpump turbines, and main turbine trip and loss of main condenser heat sink. For the purposes of this analysis, the PPS is assumed to be functional and that at the point when RHR shutdown cooling suction valve fails (in the above sequence of events) PPS is postulated to have a CCF.

1. None, after time of discovery of RHR shutdown cooling suction valve failure in the above sequence of events.

### 3.16.3 EOP Entry Conditions

No EOP Entry Conditions.

### 3.16.4 Operator Actions

Upon recognition of loss of shutdown cooling, in accordance with ON-121, "Loss of Shutdown Cooling" (Reference 45):

1. **Open ADS SRVs.**
2. **Manually initiate one loop of CS** and flood the RPV to establish a flow path through the ADS SRVs, to the suppression pool, and
3. **Manually Initiate RHR suppression pool cooling**

Estimated Time Available for Operator Actions: >10 minutes



### 3.16.5 Summary of Diverse Features from PPS

1. Reactor water level NR, WR, Upset and Shutdown indication
2. Manual control of ADS SRVs
3. Manual control of CS Loop-A
4. CS Loop-A flow
5. CS Loop-A pressure
6. Manual control of RHR Loop-A suppression pool cooling mode

### 3.16.6 Conclusion

For the postulated event of Loss of Shutdown Cooling Operation, existing diverse displays with the addition of DPS diverse displays and controls identified in 3.16.5, and operator actions, are sufficient to mitigate the postulated event, concurrent with a postulated CCF of PPS. The reactor core is adequately cooled and RCPB integrity is maintained. Since this transient does not result in any release of primary coolant to either the secondary containment or the environment, there are no radiological consequences associated with this transient. Thus, BTP 7-19 3.3(b) Acceptance Criteria for this AOO are satisfied.

## 3.17 EVENT: 15.2.10 LOSS OF STATOR COOLING

Loss of generator stator cooling is assumed to occur. This event is a moderate frequency event and classified as an AOO.

### 3.17.1 Sequence of Events (UFSAR Table 15.2-15)

<u>TIME (sec)</u>	<u>EVENT</u>
0.0	Loss of Stator Cooling occurs.
0.0	Dual Recirculation Pump to 42% Speed is initiated.
0.0	Turbine-Generator Load Set Runback begins from 105% going to 20% over 140 seconds.
45 (approx.)	Turbine-Generator Load Set reaches Turbine Control Valve (TCV) position and starts causing the TCVs to close. Turbine Bypass Valves (TBV) begin to open in response to the TCV Closure.
75 (approx.)	TBVs open to their available capacity. Pressurization begins due to mismatch between steam flow coming from the vessel and the available TCV/TBV capacity.
95 (approx.)	**Reactor scrams on high pressure or neutron flux.**

### 3.17.2 Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS

1. RRCS initiates ARI on high RPV pressure resulting in reactor scram, and RPT actuation.



2. SRVs cycle to relief pressure as required.
3. DFWLCS maintains normal level control.
4. Main turbine-generator trips on reverse power.
5. Pressure control system modulates turbine bypass valves to control pressure.

### 3.17.3 EOP Entry Conditions

The operator will promptly enter T-101 (Reference 14) upon recognition of any of the following entry conditions:

1. RPV water level below +12.5 inches (Level 3)
2. RPV pressure above 1096 psig
3. A reactor scram condition with APRM above 4%

### 3.17.4 Operator Actions per RPV Control EOP with postulated PPS CCF

1. Enter T-101 (Reference 14). Monitor RPV water level, pressure, power, control rod positions
2. Restore and maintain RPV water level between +12.5 inches and +54 inches using DFWLCS
3. Stabilize RPV pressure at a pressure below 1096 psig using the turbine bypass valves

Estimated Time Available for Operator Actions: >10 minutes

### 3.17.5 Summary of Diverse Features from PPS

Based upon the analysis for this event, the following diverse features are required, for the postulated CCF of the PPS:

1. Reactor water level NR indication
2. **Reactor Water Level Low (Level 3) alarm**
3. Reactor pressure (WR)
4. Reactor power (APRM)
5. APRM Not Downscale indication
6. Control rod position indications
7. RRCS
8. DFWLCS
9. DEHC

### 3.17.6 Conclusion

For the postulated event of Loss of Stator Cooling, concurrent with a postulated CCF of PPS, sufficient automatic control functions, indications that are independent of the PPS, and operator actions, are available to mitigate the event. The reactor core is adequately cooled and RCPB integrity is maintained. Since this transient does not result in any release of primary coolant to either the secondary containment



or the environment, there are no radiological consequences associated with this transient. Thus, BTP 7-19 3.3(b) Acceptance Criteria for this AOO are satisfied.

### **3.18 EVENT: 15.3.1 TRIP OF ONE RECIRCULATION PUMP MOTOR**

Trip of one recirculation pump motor is assumed. This event is categorized as an incident of moderate frequency.

#### **3.18.1 Sequence of Events (UFSAR Table 15.3-1)**

<u>TIME (sec)</u>	<u>EVENT</u>
0	Trip of one recirculation pump initiated.
2.7	Diffuser flow decreases significantly in the tripped loop.
20.0	Core flow stabilizes at new equilibrium conditions.
40.0	Power level stabilizes at new equilibrium conditions.

#### **3.18.2 Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS**

1. Pressure regulator controls pressure by modulation of the turbine control valves.
2. DFWLCS controls RPV water level to setpoint.
3. No safety control action is needed. Reactor remains on-line.

#### **3.18.3 EOP Entry Conditions**

No EOP Entry Conditions.

#### **3.18.4 Operator Actions per EOPs with postulated PPS CCF**

None.

Operator should reduce the flow of the running recirculation pump to conform to the single pump flow criteria for single loop operation, and enter single loop operation per applicable plant procedure.

Estimated Time Available for Operator Actions: N/A. No operator actions required per EOPs.

#### **3.18.5 Summary of Diverse Features from PPS**

Based upon the analysis for this event, the following diverse features are required, for the postulated CCF of the PPS:

1. Reactor Water Level NR indication
2. DFWLCS



### 3. DEHC

#### 3.18.6 Conclusion

For the postulated event of Trip of One Recirculation Pump Motor, concurrent with a postulated CCF of PPS, no diverse features are identified because no PPS action is required. BTP 7-19 Acceptance Criteria are not applicable.

### 3.19 EVENT: 15.3.1 TRIP OF TWO RECIRCULATION PUMPS

Trip of two recirculation pump motors is assumed. The vessel water level swell due to rapid flow coast-down is expected to reach the high level trip, thereby shutting down the main turbine and feed pump turbines and scrambling the reactor. This event is categorized as an incident of moderate frequency.

#### 3.19.1 Sequence of Events (UFSAR Table 15.3-2)

<u>TIME (sec)</u>	<u>EVENT</u>
0.0	Trip of both recirculation pumps initiated.
5.2	**Vessel water level (Level 8) trip initiates turbine trip and feedwater pumps** trip.
5.2	**Turbine trip initiates bypass operation.**
5.2	**Turbine trip initiates reactor scram trip.**
9.9	Group 1 MSRVs open.
12.9	Group 1 MSRVs close.
43.5	**Level 2 vessel level setpoint initiates steam line isolation and HPCI/RCIC start.**

#### 3.19.2 Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS

1. DFWLCS maintains normal water level control.
2. Pressure regulator controls pressure by modulation of the turbine control valves

#### 3.19.3 EOP Entry Conditions

No EOP entry conditions.

#### 3.19.4 Operator Actions per RPV Control EOP with postulated PPS CCF

No entry into the EOPs for operator action for mitigating this event. Operator takes immediate action to manually scram the reactor in accordance with procedure OT-112, "Unexpected/Unexplained Change in



Core Flow” (Reference 46), to avoid operation in the reactor instability region after both recirculation pumps tripped.

Estimated Time Available for Operator Actions: >10 minutes

### **3.19.5 Summary of Diverse Features from PPS**

Based upon the analysis for this event, the following diverse features are required, for the postulated CCF of the PPS:

1. Reactor water level NR indication
2. Reactor pressure (WR)
3. Reactor power (APRM)
4. Control rod position indications
5. DFWLCS
6. DEHC
7. Manual scram pushbuttons

### **3.19.6 Conclusion**

For the postulated event of Trip of Both Recirculation Pumps, concurrent with a postulated CCF of PPS, sufficient automatic control functions, indications that are independent of the PPS, and operator actions, are available to mitigate the event. The reactor core is adequately cooled and RCPB integrity is maintained. Since this transient does not result in any release of primary coolant to either the secondary containment or the environment, there are no radiological consequences associated with this transient. Thus, BTP 7-19 3.3(b) Acceptance Criteria for this AOO are satisfied.

## **3.20 EVENT: 15.3.2 RECIRCULATION FLOW CONTROL FAILURE- DECREASING FLOW**

Some causes of recirculation flow control failure are malfunction of the active Adjustable Speed Drive (ASD) controller (one of two redundant controllers), malfunction of the PLC supplying command signals to the controllers, or corruption to the communication between these devices (one of two redundant channels). These malfunctions can result in a rapid flow decrease in only one recirculation loop.

No analyses are provided for failure of one recirculation flow controller or failure of both controllers that result in decreasing recirculation flow. Failure of one recirculation flow controller is bounded by Event 15.3.1 Trip of One Recirculation Pump. Failure of both recirculation flow controller is bounded by analysis of Event 15.3.1 for Trip of Two Recirculation Pumps. Plant operating procedure requires a manual reactor scram to avoid operation in the core instability region of the power-flow map.

## **3.21 EVENT: 15.3.3 RECIRCULATION PUMP SEIZURE**

The case of recirculation pump seizure represents the extremely unlikely event of instantaneous stoppage of the pump motor shaft of one recirculation pump. This accident produces a very rapid decrease of core



flow as the result of the large hydraulic resistance introduced by the stopped rotor. This event is categorized as a Design Basis Accident (DBA).

### 3.21.1 Sequence of Events (UFSAR Table 15.3-3)

<u>TIME (sec)</u>	<u>EVENT</u>
0.0	Single pump seizure was initiated.
0.7	Jet pump diffuser flow reverses in seized loop.
4.0	Core flow stabilizes at new equilibrium conditions.
40.0	Power stabilizes at new equilibrium conditions.

### 3.21.2 Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS

1. DFWLCS maintains normal level control
2. Pressure control system maintains normal pressure control by modulation of the turbine control valves

### 3.21.3 EOP Entry Conditions

No EOP Entry Conditions.

### 3.21.4 Operator Actions per RPV Control EOPs with postulated PPS CCF

No operator actions required.

Estimated Time Available for Operator Actions: N/A. No operator actions required.

### 3.21.5 Summary of Diverse Features from PPS

1. Reactor water level NR indication
2. Reactor pressure
3. Reactor power (APRM)
4. DFWLCS
5. DEHC
6. Recirculation loop flows

### 3.21.6 Conclusion

For the postulated event of Recirculation Pump Seizure, concurrent with a postulated CCF of PPS, sufficient indications that are independent of the PPS are available for operator monitoring of the progression of this event. No PPS actions are necessary for mitigation of this event. BTP 7-19 acceptance criteria are not applicable for this event.



### **3.22 EVENT: 15.3.4 RECIRCULATION PUMP SHAFT BREAK**

The case of recirculation pump shaft breaking represents the extremely unlikely event of instantaneous stoppage of the one recirculation pump motor and is considered as an accident. This accident produces a very rapid decrease of core flow as the result of the broken pump shaft. The event is bounded by the more limiting case of recirculation pump seizure in 15.3.3, and thus no quantitative results are presented. This event is considered to be a Limiting Fault.

#### **3.22.1 Sequence of Events**

A postulated instantaneous break of the motor shaft of one recirculation pump will cause the core flow to decrease rapidly and result in water level swell in the reactor vessel but no scram. The core flow and then reactor power stabilize at lower values within less than a minute of the failure.

#### **3.22.2 Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS**

1. DFWLCS maintains normal level control
2. Pressure control system maintains normal pressure control by modulation of the turbine control valves

#### **3.22.3 EOP Entry Conditions**

No EOP Entry Conditions.

#### **3.22.4 Operator Actions**

No entry into the EOPs for operator action for mitigating this event.

Estimated Time Available for Operator Actions: N/A. No operator actions required.

#### **3.22.5 Summary of Diverse Features from PPS**

1. Reactor water level NR indication
2. Reactor pressure
3. Reactor power (APRM)
4. DFWLCS
5. DEHC
6. Recirculation loop flows

#### **3.22.6 Conclusion**

For the postulated event of Recirculation Pump Shaft Break, concurrent with a postulated CCF of PPS, sufficient indications that are independent of the PPS are available for operator monitoring of the progression of this event. No PPS actions are necessary for mitigation of this event. BTP 7-19 acceptance criteria are not applicable.



### 3.23 EVENT: 15.4.1 ROD WITHDRAWAL ERROR - LOW POWER

The transient considered is inadvertent criticality due to the complete withdrawal or removal of the highest worth control rod during refueling operations. It is classified as an infrequent incident.

#### 3.23.1 Sequence of Events

Five sequences of events are considered:

1. Initial Control Rod Removal or Withdrawal: During refueling operations system interlocks provide assurance that inadvertent criticality does not occur because two control rods have been removed or withdrawn together.
2. Fuel Insertion with Control Rod Withdrawn: To minimize the possibility of loading fuel into a cell containing no control rod, all control rods must be fully inserted when fuel is being loaded into the core. This requirement is backed up by refueling interlocks on rod withdrawal and movement of the refueling platform. When the mode switch is in the REFUEL position, the interlocks prevent the platform from being moved over the core if a control rod is withdrawn and fuel is on the hoist. Likewise, if the refueling platform is over the core and fuel is on the hoist, control rod motion is blocked by the interlocks.
3. Second Control Rod Removal or Withdrawal: When the platform is not over the core (or fuel is not on the hoist) and the mode switch is in the REFUEL position, only one control rod can be withdrawn. Any attempt to withdraw a second rod results in a rod block by the refueling interlocks. Since the core is designed to meet shutdown requirements with the highest worth rod withdrawn, the core remains subcritical even with one rod withdrawn.
4. Control Rod Removal Without Fuel Removal: The design of the control rod, incorporating the velocity limiter, does not physically permit the upward removal of the control rod without prior or simultaneous removal of the four adjacent fuel bundles.
5. Continuous Rod Withdrawal During Reactor Startup: Control rod withdrawal errors are not considered credible in the startup and low power ranges. The Rod Worth Minimizer (RWM) system prevents the operator from selecting and withdrawing an out-of-sequence control rod.

#### 3.23.2 Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS

For sequences 1 through 3 above, the reactor manual rod control system and/or the refueling bridge interlocks enforce rod blocks using reactor mode switch Refuel position signals, separate from those provided to PPS. Sequence 5 is unlikely to occur due to the design of the RWM.

#### 3.23.3 EOP Entry Conditions

There are no EOP Entry Conditions.



### **3.23.4 Operator Actions**

No entry into the EOPs for operator action for mitigating these events.

Estimated Time Available for Operator Actions: N/A. No operator actions required.

### **3.23.5 Summary of Diverse Features from PPS**

1. RMCS
2. Reactor Mode Switch Refuel position signals to RMCS
3. Rod Worth Minimizer

### **3.23.6 Conclusion**

For the postulated events of inadvertent control rod withdrawal, concurrent with a postulated CCF of PPS, sufficient controls that are independent of the PPS are available for mitigating these postulated events. No PPS actions are necessary for mitigation of these events. No radioactive material is released from the fuel for these postulated events. BTP 7-19 acceptance criteria are not applicable.

## **3.24 EVENT: 15.4.2 ROD WITHDRAWAL ERROR – AT POWER**

The operator is assumed to make a procedural error and continuously withdraws a high worth control rod until the Rod Block Monitor (RBM) system inhibits further withdrawal. This transient is classified as an incident of moderate frequency.

### **3.24.1 Sequence of Events (UFSAR Table 15.4-1)**

1. Operator selects (the Rod Block Monitor (RBM) is automatically normalized) and withdraws high worth control rod.
2. The RBM system indicates excessive local peaking. Operator ignores the alarm and continues to withdraw control rod.
3. The RBM system initiates a rod block, inhibiting further withdrawal.
4. Operator verifies fuel thermal limits are satisfied before renormalizing RBM to further withdraw control rod.

### **3.24.2 Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS**

The RBM system initiates a rod block, inhibiting further withdrawal.

### **3.24.3 EOP Entry Conditions**

There are no EOP Entry Conditions.



### 3.24.4 Operator Actions

Operator verifies fuel thermal limits are satisfied before renormalizing RBM to further withdraw control rod.

Estimated Time Available for Operator Actions: No time requirement.

### 3.24.5 Summary of Diverse Features from PPS

1. Reactor Manual Control System (RMCS)
2. Rod Block Monitor (RBM) System

### 3.24.6 Conclusion

For the postulated event of Rod Withdrawal Error – At Power, concurrent with a postulated CCF of PPS, sufficient controls that are independent of the PPS are available for mitigating these postulated events. No PPS actions are necessary for mitigation of this event. No radioactive material is released from the fuel for this event. BTP 7-19 acceptance criteria are not applicable.

## 3.25 EVENT: 15.4.3 CONTROL ROD MALOPERATION (SYSTEM MALFUNCTION OR OPERATOR ERROR)

In accordance with UFSAR Section 15.4.3, this transient is covered by the evaluations in Sections 3.23 and 3.24.

## 3.26 EVENT: 15.4.4 ABNORMAL STARTUP OF IDLE RECIRCULATION PUMP

This action results directly from the operator's manual action to initiate pump operation. It assumes that the remaining loop is already operating. This event is categorized as an incident of moderate frequency.

### 3.26.1 Sequence of Events (UFSAR Table 15.4-3)

<u>TIME (sec)</u>	<u>EVENT</u>
0	Start pump motor.
9.0	Startup loop flow starts to increase significantly.
10.4	**APRM neutron flux upscale scram initiated.**
>50.0	Vessel level returning to normal and will stabilize quickly.

### 3.26.2 Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS

1. DFWLCS maintains normal level control
2. Pressure control system maintains normal pressure control



### 3.26.3 EOP Entry Conditions

No EOP Conditions.

### 3.26.4 Operator Actions

No entry into EOPs for operator action for mitigating this event.

Estimated Time Available for Operator Actions: N/A. No operator actions required.

### 3.26.5 Summary of Diverse Features from PPS

Based upon the analysis for this event, the following diverse features are required, for the postulated CCF of the PPS:

1. Reactor water level NR indication
2. Reactor pressure
3. Reactor power (APRM)
4. APRM high flux indication/alarm
5. DFWLCS
6. DEHC

### 3.26.6 Conclusion

For the postulated event of Abnormal Start of Idle Recirculation Pump, concurrent with a postulated CCF of PPS, sufficient automatic control functions and indications that are independent of the PPS, are available to mitigate the event. The reactor core is adequately cooled and RCPB integrity is maintained. Since this transient does not result in any release of primary coolant to either the secondary containment or the environment, there are no radiological consequences associated with this transient. Thus, BTP 7-19 3.3(b) Acceptance Criteria for this AOO are satisfied.

## 3.27 EVENT: 15.4.5 RECIRCULATION FLOW CONTROL FAILURE WITH INCREASING FLOW

Maximum change in recirculation pump ASD speed control occurs when both speed controllers failed such that ASD recirculation pumps increase to maximum speed. This event is categorized as an incident of moderate frequency.

### 3.27.1 Sequence of Events (UFSAR Table 15.4-4)

<u>TIME (sec)</u>	<u>EVENT</u>
0	Simulate failure of single-loop control.
1.7	**APRM neutron flux upscale scram trip initiated.**



<u>TIME (sec)</u>	<u>EVENT</u>
5.5	Turbine control valves start to close upon falling turbine pressure.
20.2	Feedwater decreases upon rising water level.
>100.0	Reactor variables settle into new steady-state.

### 3.27.2 Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS

1. DFWLCS maintains normal level control.
2. Pressure control system opens turbine control valves and modulates the turbine bypass valves to control pressure.

### 3.27.3 EOP Entry Conditions

The operator will promptly enter T-101 (Reference 14) upon recognition of any of the following entry conditions:

1. RPV water level below +12.5 inches (Level 3)
2. RPV pressure above 1096 psig
3. A reactor scram condition with APRM above 4%

### 3.27.4 Operator Actions per RPV Control EOP with postulated PPS CCF

1. Enter T-101 (Reference 14). Monitor RPV water level, pressure, power, control rod positions.
2. If reactor scram has not been initiated, initiate a reactor scram.
3. Restore and maintain RPV water level between +12.5 inches and +54 inches using DFWLCS.
4. Stabilize RPV pressure at a pressure below 1096 psig using the turbine bypass valves.

Estimated Time Available for Operator Actions: >10 minutes

### 3.27.5 Summary of Diverse Features from PPS

Based upon the analysis for this event, the following diverse features are required, for the postulated CCF of the PPS:

1. Reactor water level NR indication
2. Reactor pressure indication
3. Reactor power (APRM, Simulated Thermal Power)
4. APRM high flux indication/alarm
5. APRM Not Downscale indication
6. Control rod position indications



7. DFWLCS
8. DEHC
9. Manual scram push buttons

### **3.27.6 Conclusion**

For the postulated event of Recirculation Flow Control Failure With Increasing Flow, concurrent with a postulated CCF of PPS, sufficient automatic control functions, indications that are independent of the PPS, and operator actions, are available to mitigate the event. Sufficient time is available for operator to initiate a reactor scram to mitigate this event. The reactor core is adequately cooled and RCPB integrity is maintained. Since this transient does not result in any release of primary coolant to either the secondary containment or the environment, there are no radiological consequences associated with this transient. Thus, BTP 7-19 3.3(b) Acceptance Criteria for this AOO are satisfied.

## **3.28 EVENT: 15.4.7 MISPLACED BUNDLE ACCIDENT**

The accident discussed in this section is the improper loading of a fuel bundle and subsequent operation of the core. Three errors must occur for this accident to take place in the initial core loading. First, a bundle must be loaded into a wrong location in the core. Second, the bundle which was supposed to be loaded where the mis-location occurred would have to be overlooked and also put in an incorrect location. Third, the misplaced bundles would have to be overlooked during the core verification performed following initial core loading. This event is categorized as an infrequency incident.

### **3.28.1 Sequence of Events (UFSAR Table 15.4-5)**

1. During core loading operation, bundle is placed in the wrong location.
2. Subsequently, the bundle intended for this location is placed in the location of the previous bundle.
3. During core verification procedure, error is not observed.
4. Plant is brought to full power operation without detecting misplaced bundle.
5. Plant continues to operate.

### **3.28.2 Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS**

1. DFWLCS maintains normal level control
2. Pressure control system maintains normal pressure control by modulation of the turbine control valves

Fuel loading errors, undetected by in-core instrumentation following fueling operations, may result in undetected reductions in thermal margins during power operations. No detection is assumed per UFSAR



Section 15.4.7 and, therefore, no corrective operator action or automatic protection system functioning occurs.

### 3.28.3 EOP Entry Conditions

No EOP Entry Conditions.

### 3.28.4 Operator Actions

No entry into the EOPs for operator action for mitigating this event.

Estimated Time Available for Operator Actions: N/A. No operator actions required.

### 3.28.5 Summary of Diverse Features from PPS

Monitoring of important parameters for normal plant operation are:

1. Reactor water level NR indication
2. Reactor pressure indication (WR)
3. Reactor power (APRM)
4. DFWLCS
5. DEHC

### 3.28.6 Conclusion

For the postulated event of Misplaced Bundle Accident, concurrent with a postulated CCF of PPS, sufficient indications that are independent of the PPS are available for operator monitoring the operating condition of the reactor. No PPS actions are necessary for mitigation of this event. UFSAR Section 15.4.7.3 demonstrates acceptable fuel thermal margin is maintained for continuous power operations. BTP 7-19 acceptance criteria are not applicable.

## 3.29 EVENT: 15.4.9 CONTROL ROD DROP ACCIDENT

Causes of the control rod drop accident is described in the Sequence of Events table below. This event is classified as a Limiting Fault (DBA).

### 3.29.1 Sequence of Events (GESTAR II, NEDO-24011-A-31-US (Reference 8), Table S.2.2.3.1.1)

<u>Approximate Elapsed Time, seconds</u>	<u>Event</u>
-	Reactor is at a control rod pattern corresponding to maximum increment rod worth.



<u>Approximate Elapsed Time, seconds</u>	<u>Event</u>
-	Rod pattern control systems (Rod Worth Minimizer, Rod Sequence Control System, or Rod Pattern Controller) or operators are functioning within constraints of Banked Position Withdrawal Sequence (BPWS). The control rod that will result in the maximum incremental reactivity worth addition at any time in core life under any operating condition while employing the BPWS becomes decoupled from the control rod drive.
-	Operator selects and withdraws the drive of the decoupled rod – along with the other required control rods assigned to the Banked position group such that the proper core geometry for the maximum incremental rod worth exists.
-	Decoupled control rod sticks in the fully inserted position.
0	Control rod becomes unstuck and drops at the maximum velocity determined from experimental data (3.11 fps).
≤1	Reactor goes on a positive period and initial power burst is <1 sec. terminated by the Doppler reactivity feedback.
-	**APRM 120% power signal scrams reactor (conservative; in startup mode APRM scram would be operative + Intermediate Range Monitor [IRM]).**
≤5	**Scram terminates accident.**

### 3.29.2 Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS

1. DFWLCS maintains normal level control
2. Pressure control system maintains normal pressure control by modulation of the turbine control valves

### 3.29.3 EOP Entry Conditions

None. Operator will enter operating procedure OT-117, “RPS Failures” (Reference 12), upon recognition of IRM upscale condition and upscale alarm.

### 3.29.4 Operator Actions

None per the EOPs. However, upon recognition of IRM upscale condition operator will take action to initiate a reactor scram using the manual scram switches in accordance with plant operating procedure OT-117 (Reference 12).

Estimated Time Available for Operator Actions: >10 minutes



### 3.29.5 Summary of Diverse Features from PPS

Based upon the analysis for this event, the following diverse features are required, for the postulated CCF of the PPS:

1. Reactor water level NR indication
2. Reactor pressure indication (WR)
3. Reactor power (APRM / IRM)
4. IRM upscale alarm
5. Reactor manual scram push buttons

### 3.29.6 Conclusion

The primary consideration for the Control Rod Drop Accident (CRDA) is radiological release to the main control room and to the environment. UFSAR Table 15.4-13 provides the analysis results, assuming the sequency of events provided and an automatic RPS trip to terminate the event. It is noted that the Total Effective Dose Equivalent (TEDE) for main condenser leakage over a 30-day period is much less than the Regulatory Limit for TEDE. It is also noted that the radiological analysis did not credit the operation of the Control Room Emergency Fresh Air Supply System (CREFAS) and the Standby Gas Treatment System (SGTS). Thus, it is expected that the operator response time for performing a manual scram using the hard scram switches would have a negligible impact on the radiation release calculations. Therefore the allowance for a manual operator scram is an acceptable response to this event. For the CRDA concurrent with a postulated CCF of PPS, sufficient indications that are independent of the PPS are available for operator monitoring the operating condition of the reactor. The reactor core is adequately cooled, RCPB integrity and containment integrity are not challenged. The radiological consequences and the assumptions of the current dose analysis for this PA are within regulatory limits. Thus, BTP 7-19 3.3(c) Acceptance Criteria for this PA are satisfied.

### 3.30 EVENT: 15.5.1 INADVERTENT HPCI START

This transient is not possible with an assumed CCF of the PPS which initiates and controls HPCI. Refer to Section 5.6 for an analysis of spurious initiation of HPCI.

### 3.31 EVENT: 15.6.2 INSTRUMENT LINE BREAK

This accident involves the postulation of a small steam or liquid line pipe break inside or outside primary containment but within a controlled release structure. In order to bound the accident, it is assumed that a small instrument line, instantaneously and circumferentially, breaks at a location where it may not be able to be isolated and where immediate detection is not automatic or apparent. This event is classified as a Limiting Fault (DBA).

#### 3.31.1 Sequence of Events (UFSAR Table 15.6-1)

<u>TIME</u>	<u>EVENT</u>
-------------	--------------



0	Instrument line fails
0-10 min	Identification of break
10 min	**Activate SBGTS** and initiate orderly shutdown
5 hours	Reactor vessel depressurized and break flow terminated

### 3.31.2 Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS

1. DFWLCS maintains normal level control
2. Pressure control system maintains normal pressure control by modulation of the turbine control valves

### 3.31.3 EOP Entry Conditions

No EOP Entry Conditions.

### 3.31.4 Operator Actions with postulated PPS CCF

1. If break cannot be isolated, conduct an orderly shutdown of the reactor, and depressurize the reactor using the turbine bypass valves maintaining a cool down rate less than 100°F/hour.
2. **Initiate Reactor Enclosure isolation.** [Note: Initiation of Reactor Enclosure isolation starts Reactor Enclosure Recirculation System (RERS) and SGTS. Ref: UFSAR 6.2.3.2.3]

Estimated Time Available for Operator Actions: >10 minutes

### 3.31.5 Summary of Diverse Features from PPS

Based upon the analysis for this event, the following diverse features are required, for the postulated SCCF of the PPS:

1. Reactor water level NR indication
2. Reactor pressure indication
3. DFWLCS
4. DEHC
5. Containment isolation status display
6. **Manual initiation of Reactor Enclosure isolation**
7. SGTS
8. RERS

### 3.31.6 Conclusion

For the postulated event of Instrument Line Break, concurrent with a postulated CCF of PPS, 1) sufficient automatic control functions, 2) indications that are independent of the PPS, and 3) operator actions,



are/will be available to mitigate the event. Reactor Enclosure is isolated, RERS and SGTS are automatically initiated to limit offsite radioactivity release. The reactor core is adequately cooled and RCPB integrity and secondary containment integrity are maintained. Thus, BTP 7-19 3.3(c) Acceptance Criteria for this PA are satisfied.

### 3.32 EVENT: 15.6.4 STEAM SYSTEM PIPE BREAK OUTSIDE PRIMARY CONTAINMENT

This accident involves the postulation of a large steam line pipe break outside primary containment. It is assumed that the largest steam line instantaneously and circumferentially breaks at a location downstream of the outermost isolation valve. This event is classified as a Limiting Fault (DBA).

#### 3.32.1 Sequence of Events (UFSAR Table 15.6-8)

<u>TIME (sec)</u>	<u>EVENT</u>
0	Guillotine break of one main steam line outside primary containment.
1.0 (approx)	**High steam line flow signal initiates closure of MSIV.**
< 1.5	**Reactor begins scram.**
≤ 6.0	**MSIVs fully closed.**
60.0 (approx)	**Reactor Core Isolation Cooling (RCIC) and HPCI initiate on low water level (Level 2) (RCIC considered unavailable**, HPCI assumed single failure and therefore may not be available).
60.0 (approx)	SRVs open on high vessel pressure. The valves open and close to maintain vessel pressure at approximately 1170 psi.
1780 (approx)	Low water level (Level 1) reached. **Low pressure ECCS receives signal to start. ADS logic is initiated.**
1900 (approx)	**High drywell pressure bypass timer and ADS timer "timed out". ADS starts.** Vessel depressurizes.
2100 (approx)	**Low pressure ECCS begin injection.** Core partially uncovers.
2160 (approx)	Core effectively reflooded and clad temperature heatup terminated. No fuel rod failure.

#### 3.32.2 Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS

1. MSIVs isolate on Main Steam Line Flow - High
2. Redundant Reactivity Control System (RRCS) initiates on High Reactor RPV Pressure resulting in reactor scram and RPT actuation



3. Feedpump turbines trip with steam flow cutoff by closure of MSIVs and depressurization of main steam lines
4. SRVs cycle to relief pressure as required
5. Rapid decrease in steam line pressure results in closure of turbine control valves by the DEHC pressure regulator and subsequent turbine trip on reverse power

### 3.32.3 EOP Entry Conditions

The operator will promptly enter T-101 (Reference 14) upon recognition of any of the following entry conditions:

1. RPV water level below +12.5 inches (Level 3)
2. RPV pressure above 1096 psig
3. A reactor scram condition with APRM above 4%

The operator will promptly enter T-103, "Secondary Containment Control SCC/T, SCC/RAD, SCC/L (Flowchart)" (Reference 16) , upon recognition of any of the following entry conditions:

1. Area radiation alarms
2. Reactor Enclosure HVAC isolation on high radiation
3. Reactor Enclosure steam flooding damper actuation
4. Reactor Enclosure High-High floor drain sump alarms

### 3.32.4 Summary of Relevant Operator Actions per EOPs with postulated PPS CCF

1. Enter T-101 (Reference 14). Monitor RPV water level, pressure, power, control rod positions
  - a. Stabilize RPV pressure at a pressure below 1096 psig using ADS SRVs
  - b. Depressurize the RPV and maintain the cooldown rate below 100 °F/hr using ADS SRVs
  - c. Before RPV level reaches -186 inches (MSCRWL), Emergency Depressurization is required (using ADS SRVs)
  - d. Restore and maintain RPV water level between +12.5 inches and +54 inches using condensate pumps when RPV pressure decreases below pump shutoff head (approximately 680 psig)

Estimated Available Time for Operator Actions: > 10 minutes

1. Enter T-103 (Reference 16)
  - a. Operate available area coolers



- b. Operate Reactor Enclosure HVAC
- c. Confirm isolation of all systems discharging into the area

- 2. If suppression pool temperature increases above 95°F, enter T-102 (Reference 15) and initiate suppression pool cooling.

Estimated Time Available for Operator Actions: >10 minutes

### 3.32.5 Summary of Diverse Features from PPS

Based upon the analysis for this event, the following diverse features are required, for the postulated CCF of the PPS:

- 1. Reactor water level NR, WR, and FZ indication
- 2. Reactor Water Level Low (Level 3) alarm
- 3. Reactor pressure
- 4. Reactor power (APRM)
- 5. APRM Not Downscale indication
- 6. Control rod position indications
- 7. Area radiation alarms (for T-103 Entry)
- 8. Reactor Enclosure HVAC isolation on high radiation
- 9. Reactor Enclosure steam flooding damper actuation
- 10. Reactor Enclosure High-High floor drain sump alarms
- 11. RRCS
- 12. Suppression pool temperature
- 13. Main steam line flow
- 14. Auto initiation of MSIV closure on Main Steam Line Flow – High
- 15. Manual control of ADS SRVs
- 16. Outboard MSIV room temperatures
- 17. Outboard MSIV room differential temperature
- 18. RHR Loop-A suppression pool cooling
- 19. Manual controls of feedwater injection using the condensate pumps

### 3.32.6 Conclusion

For the postulated Steam System Pipe Break Outside Containment, concurrent with a postulated CCF of PPS, sufficient automatic control functions and information that are independent of the PPS, and operator actions, are/will be available to mitigate the event. Diverse automatic isolation of the MSIVs limit radioactivity release to the areas outside of the containment and the radioactivity release analyses are not affected. Because the MSIVs are automatically isolated, adequate core cooling is maintained, and the SRVs discharge to the suppression pool, the offsite radioactivity release is expected to remain within the limit for this PA. Furthermore, RCPB integrity is maintained, and because the break occurs outside of the primary containment maintenance of primary containment is not applicable. Furthermore, the radiological analysis described in UFSAR Section 15.6.4.5 does not credit the operability of CREFAS and SGTS, and thus diverse secondary containment isolations are not taken credit for this scenario. Thus, BTP 7-19 3.3(c) Acceptance Criteria for this PA are satisfied.



### 3.33 EVENT: 15.6.5 LOCA INSIDE CONTAINMENT

This accident involves the postulation of a spectrum of piping breaks inside containment varying in size, type, and location. The break type includes steam and/or liquid process system lines. The accident is analyzed quantitatively in LGS UFSAR Sections 6.3, 6.2, 7.3, 7.6, and 8.3. The most severe nuclear system effects and the greatest release of radioactive material to the containment result from a complete circumferential break of one of the two recirculation loops. This event is classified as a Limiting Fault (DBA).

#### 3.33.1 Sequence of Events (UFSAR Table 6.3-2)

Note: Feedwater flow was assumed to be terminated at the beginning of this event.

<u>TIME (sec)</u>	<u>EVENTS</u>
0	Design basis Loss of Coolant Accident (LOCA) is assumed to start; normal auxiliary power is assumed to be lost.
<1	**Drywell high pressure is reached. Scram initiated; HPCI is signaled to start, and containment isolates**, except for the MSIVs.
~1	**Reactor Low Water Level (Level 3) is reached. The second scram initiation signal is received.**
~4	**Reactor low-low water level (Level 2) is reached. HPCI receives the second signal to start.**
~ 5	**The reactor low-low-low water level (Level 1) is reached; MSIVs are signaled to close; the signal to start LPCI and CS is given.**
~ 25	**Reactor low pressure is reached. CS and LPCI receive the second signal to start. CS injection valve receives pressure permissive signal to open.**
≤54	**The CS pumps are at rated flow and the CS injection valves are open, which completes the CS system startup.**
≤70	**The LPCI pumps are at rated flow and the LPCI injection valves are open, which completes the LPCI system startup.**
~ 130	The core is effectively reflooded, assuming the worst single failure; heatup is terminated.
>10 min	The operator shifts to containment cooling.



### 3.33.2 Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS

1. Rapid decrease in steam line pressure results in closure of turbine control valves by the DEHC pressure regulator and subsequent main turbine trip
2. When reactor water level decreases below -38 inches (Level 2), RRCS initiates the following functions:
  - ARI initiation resulting in reactor scram
  - RPT actuation (Level 2 with 9 second delay)
3. MSIVs isolate when RPV water level decreases below -129 inches (Level 1)
4. Initiation of one loop of CS when either:
  - Drywell pressure is above 1.68 psig and RPV pressure decreases below 455 psig, or
  - RPV water level decreases below -129 inches (Level 1)

### 3.33.3 EOP Entry Conditions

The operator will promptly enter T-101 (Reference 14) upon recognition of any of the following entry conditions:

1. RPV water level below +12.5 inches (Level 3)
2. RPV pressure above 1096 psig
3. A reactor scram condition with APRM above 4%
4. Drywell pressure above 1.68 psig

The operator will promptly enter the T-102 (Reference 15) upon recognition of the following entry conditions:

1. Drywell pressure above 1.68 psig

### 3.33.4 Summary of Relevant Operator Actions per RPV Control and Primary Containment Control EOPs with postulated PPS CCF

1. Enter T-101 (Reference 14). Monitor RPV water level, pressure, power, control rod positions.
  - a. Initiate Reactor Enclosure isolation.
  - b. Restore and maintain RPV water level above -186 inches (MSCRWL).
  - c. If RPV water level cannot be restored and maintained above -186 inches (MSCRWL) restore and maintain RPV level above -211 inches with Core Spray loop flow  $\geq 6250$  gpm.
2. Enter T-102 (Reference 15).



- a. When drywell temperature cannot be maintained below 145°F:
  - i. Operate all available drywell cooling, defeating isolations if necessary.
- b. Initiate containment cooling using one loop of **RHR Suppression Pool Cooling**.
- c. Before suppression pool (chamber) pressure exceeds 7.5 psig, Suppression Pool Spray is Required. Initiate **Suppression Pool Spray** at the DPS (diverse feature identified in Position 4 analysis).

Estimated Time Available for above Operator Actions: >10 minutes

3. Upon recognition of a LOCA, enter SE-10, “LOCA” (Reference 38).

When greater than 3 hours have elapsed following the LOCA, manually initiate SLCS pumps to inject into the RPV, using manual control from RRCS if necessary\*.

\*The Regulatory Guide 1.183 accident isotopic release specification allows deposition of iodine in the suppression pool. Essentially all of the iodine is assumed to remain in solution as long as the suppression pool pH is maintained at or above a level of 7. Reference 39 calculation confirms that the addition of sodium pentaborate to the suppression pool maintains the pool pH at a minimum of 7.0 to minimize iodine releases from primary containment. SLCS pumps Sodium Pentaborate to the reactor vessel, where it is mixed with the reactor coolant which flows to the suppression pool through the LOCA pipe break. The SLCS addition must occur within 13 hours following a LOCA to ensure pH is maintained at 7.0 or above. SLCS manual initiation is implemented in the PPS. In the presence of PPS CCF, manual control from RRCS may be used to start the SLCS pumps which will also fire the squib valves.

### 3.33.5 Summary of Diverse Features from PPS

Based upon the analysis for this event, the following diverse features are required, for the postulated CCF of the PPS:

1. Reactor water level NR, **WR, and FZ** indication
2. **Reactor Water Level Low (Level 3) alarm**
3. Reactor pressure
4. Reactor power (APRM)
5. APRM Not Downscale indication
6. Control rod position indications
7. RRCS
8. Core Spray Loop-A flow
9. Core Spray Loop-A pressure
10. **Suppression pool water level**
11. Suppression pool pressure
12. Drywell temperature
13. **Drywell pressure (NR)**



14. Drywell pressure high alarm
15. Containment isolation status display
16. Manual initiation of Reactor Enclosure isolation
17. Auto initiation CS Loop-A\*
18. Auto initiation of MSIV closure on Level 1 (-129 inches)
19. Manual initiation of one RHR Loop-A for suppression pool cooling and spray (spray identified in Position 4 analysis to mitigate bypass leakage).
20. RRCS controls for SLCS pumps

\*From 6.3.2.5 of UFSAR (Reference 7):

“Certain technical specification LCO periods are justified based on NEDO-24708A which states that for postulated LOCAs, one low pressure ECCS (one LPCI loop or one CS loop) and ADS to depressurize is adequate to reflood the vessel and maintain core cooling sufficient to preclude fuel damage. NEDC-30936P-A, specifically applicable to LGS references NEDO-24708A and reaffirms this conclusion, with the advisory regarding the possible necessity of an alternate cooling path following 2 hours of post large-break LOCA LPCI injection into the core shroud.”

Note that above Items 1 through 12 are available at SPDS displays [  
] <sup>a,c</sup>

### 3.33.6 Conclusion

For the postulated event of a recirculation pipe break inside containment, concurrent with a postulated CCF of PPS, sufficient automatic control functions and information that are independent of the PPS, and operator actions, are/will be available to mitigate the event. The radiological consequences of the postulated LOCA are given in UFSAR Table 15.6-18. The automatic diverse MSIV isolation upon RPV level decreasing to Level 1, diverse manual isolation of the Reactor Enclosure and operation of the SGTS, and the use of RRCS for SLCS pump initiation for suppression pool pH control maintain the current UFSAR radiological release calculation bases. As indicated, the control room, Exclusion Area Boundary (EAB), and Low Population Zone (LPZ) calculated doses are within 10CFR100 limits. In addition, adequate core cooling is maintained by operation of one diverse CS loop, and containment integrity is maintained by operation one diverse RHR loop for suppression pool cooling, consistent with the assumptions in UFSAR Section 6.2.1.1.3.3.1.6 Long-Term Accident Responses, Case C: Loop-no containment spray. Thus, the Acceptance Criteria stated in BTP 7-19 3.3(c) for this PA are satisfied.

### 3.34 EVENT: 15.6.5 LOCA INSIDE CONTAINMENT-MAIN STEAM LINE BREAK

This accident involves the postulation of a main steam line break inside the primary containment, between the RPV nozzle to the main steam flow restrictor. This event is classified as a Limiting Fault (DBA).



### 3.34.1 Sequence of Events (UFSAR Table 6.2-16)

<u>TIME (sec)</u>	<u>EVENTS</u>
0	Break occurs.
0	**Scram assumed to occur.**
0	**Isolation signal.**
0.5	**MSIVs start to close. **
1.0	Vessel water level reaches main steam line elevation.
5.5	**MSIV fully closed.**
30	**ECCS flow starts.**
59	End of blowdown.
430	Vessel refloods.

### 3.34.2 Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS

1. **MSIV closure upon Main Steam Pressure-Low.**
2. Main turbine trips on reverse power after MSIV closure shutting off steam to the main turbine and steam to the feedpump turbines.
3. The recirculation pumps trip following the main turbine trip on reverse power and subsequent 13kV bus fast transfer.
4. Condensate pumps inject water into the RPV when reactor depressurizes to below the pump shutoff head.
5. **Initiate one loop of CS when Drywell pressure is above 1.68 psig and RPV pressure decreases below 455 psig.**

### 3.34.3 EOP Entry Conditions

The operator will promptly enter T-101 (Reference 14) upon recognition of any of the following entry conditions:

1. RPV water level below +12.5 inches (Level 3)
2. RPV pressure above 1096 psig
3. A reactor scram condition with APRM above 4%
4. Drywell pressure above 1.68 psig



The operator will promptly enter the T-102 (Reference 15) upon recognition of the following entry conditions:

1. Drywell pressure above 1.68 psig

#### 3.34.4 Summary of Relevant Operator Actions per RPV Control and Primary Containment Control EOPs with postulated PPS CCF

1. Enter T-101 (Reference 14). Monitor RPV water level, pressure, power, control rod positions.
  - a. Initiate a manual reactor scram.
  - b. **Initiate Reactor Enclosure isolation.**
  - c. Restore and maintain RPV water level between +12.5 inches and +54 inches using condensate pumps.
2. Enter T-102 (Reference 15).
  - a. When drywell temperature cannot be maintained below 145°F:
    - i. Operate all available drywell cooling, defeating isolations if necessary.
  - b. Initiate containment cooling using one loop of **RHR Suppression Pool Cooling.**
  - c. Before suppression pool (chamber) pressure exceeds 7.5 psig, Suppression Pool Spray is Required. Initiate **Suppression Pool Spray** at the DPS (diverse feature identified in Position 4 analysis).

Estimated Time Available for above Operator Actions: <5 minutes. Although this time can be chosen to be longer than 10 minutes, 5 minutes is conservatively chosen for the operator to perform a manual scram to terminate the energy discharge to the containment. This time will result in ample margins to the containment design limits, and can be validated to be achievable.

3. Upon recognition of a LOCA, enter SE-10 (Reference 38).

When greater than 3 hours have elapsed following the LOCA, manually initiate SLCS pumps to inject into the RPV, using RRCS for pump control if necessary.

#### 3.34.5 Summary of Diverse Features from PPS

Based upon the analysis for this event, the following diverse features are required, for the postulated CCF of the PPS:

1. Reactor water level NR and **WR** indication
2. **Reactor Water Level Low (Level 3) alarm**
3. **Reactor pressure (WR)**
4. Reactor power (APRM)



5. APRM Not Downscale indication
6. Control rod position indications
7. Core Spray Loop-A flow
8. Core Spray Loop-A pressure
9. Suppression pool water level
10. Suppression pool pressure
11. Drywell temperature
12. Drywell pressure (NR)
13. Drywell pressure high alarm
14. Containment isolation status display
15. Manual initiation of Reactor Enclosure isolation
16. Auto initiation of CS Loop-A\*
17. Auto MSIV isolation on Main Steam Line Pressure- Low
18. Main Steam Line Pressure
19. Manual initiation of RHR Loop-A for suppression pool cooling and spray [Spray identified in Position 4 analysis]
20. Manual controls of feedwater injection using the condensate pumps
21. RRCS controls for SLCS pumps
22. Manual scram pushbuttons

\*From 6.3.2.5 of UFSAR (Reference 7):

“Certain technical specification LCO periods are justified based on NEDO-24708A which states that for postulated LOCAs, one low pressure ECCS (one LPCI loop or one CS loop) and ADS to depressurize is adequate to reflood the vessel and maintain core cooling sufficient to preclude fuel damage. NEDC-30936P-A, specifically applicable to LGS references NEDO-24708A and reaffirms this conclusion, with the advisory regarding the possible necessity of an alternate cooling path following 2 hours of post large-break LOCA LPCI injection into the core shroud.”

### 3.34.6 Conclusion

For the postulated Main Steam Line Break event inside containment, concurrent with a postulated CCF of PPS, sufficient automatic control functions and information that are/will be independent of the PPS, and operator actions, are/will be available to mitigate the event. The radiological consequences of the postulated LOCA are given in UFSAR Table 15.6-18. The automatic diverse MSIV isolation upon RPV level decreasing to Level 1, diverse manual isolation of the Reactor Enclosure and operation of the SGTS, and the use of RRCS for SLCS pump initiation for suppression pool pH control maintain the current UFSAR radiological release calculation bases. As indicated, the control room, Exclusion Area Boundary (EAB), and Low Population Zone (LPZ) calculated doses are within 10CFR100 limits. In addition, adequate core cooling is maintained by operation of one diverse CS loop, and containment integrity is maintained by operation one diverse RHR loop for suppression pool cooling, consistent with the assumptions in UFSAR Section 6.2.1.1.3.3.1.6 Long-Term Accident Responses, Case C: Loop-no containment spray. In addition, adequate core cooling and containment integrity are maintained, the Acceptance Criteria stated in BTP 7-19 3.3(c) for this PA are satisfied.



### 3.35 EVENT: 15.6.6 FEEDWATER LINE BREAK OUTSIDE PRIMARY CONTAINMENT

The postulated break of the feedwater line, representing the largest liquid line outside primary containment, provides the envelope evaluation relative to this type of occurrence. The break is assumed to be instantaneous, circumferential, and upstream of the outermost isolation valve. This event is classified as a Limiting Fault (DBA).

#### 3.35.1 Sequence of Events (UFSAR Table 15.6-23)

<u>TIME (min)</u>	<u>EVENT</u>
0	One feedwater line breaks.
0+	Feedwater line check valves isolate the reactor from the break.
< 0.5	**At low water level (Level 3), reactor scram would initiate. At low-low water (Level 2), HPCI would initiate, RCIC would initiate, and recirculation pumps would trip. If low-low-low water level (Level 1) is reached, MSIV closure begins, and CS and LPCI receive initiation signals but will not inject due to high reactor pressure.**
2 (approx.)	The MSRVs would open and close and maintain the reactor vessel pressure at approximately 1170 psig.
60 – 120	Normal reactor cooldown procedure established.

#### 3.35.2 Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS

1. Feedpump turbines trip on high speed or low suction pressure
2. Low level alarm when reactor water level decreases below 12.5 inches (Level 3)
3. RRCS initiates the following functions:
  - ARI initiation on Level 2 resulting in reactor scram
  - RPT actuation (Level 2 with 9 second delay)
4. **Initiate MSIV closure when RPV water level decreases below Level 1 (-129 inches)**
5. **Initiate one loop of CS when RPV water level decreases below Level 1(-129 inches)**

#### 3.35.3 EOP Entry Conditions

The operator will promptly enter T-101 (Reference 14) upon recognition of any of the following entry conditions:

1. RPV water level below +12.5 inches (Level 3)



2. RPV pressure above 1096 psig
3. A reactor scram condition with APRM above 4%

The operator will promptly enter T-103 (Reference 16) upon recognition of the following entry conditions:

1. Steam leak detection alarm condition (high temperature) for Division I, II, III, or IV (indication or alarm)
2. Secondary Containment floor drain sump level high

### 3.35.4 Summary of Relevant Operator Actions per RPV Control and Secondary Containment Control EOPs with postulated PPS CCF

1. Enter T-101 (Reference 14). Monitor RPV water level, pressure, power, control rod positions.
  - a. Stabilize RPV pressure at a pressure below 1096 psig using the ADS SRVs.
  - b. Depressurize the RPV and maintain the cooldown rate below 100°F/hr using the ADS SRVs.
  - c. Before RPV level reaches -186 inches (MSCRWL), Emergency Depressurization is required (using ADS SRVs).
  - d. Restore and maintain RPV water level between +12.5 inches and +54 inches using one loop of CS when RPV pressure decreases below pump shutoff head (approximately 335 psig).
2. If suppression pool temperature increases above 95°F, enter T-102 (Reference 15) and initiate suppression pool cooling.
3. Enter T-103 (Reference 16)
  - a. Operate available area coolers.
  - b. Operate Reactor Enclosure HVAC.
  - c. Restore and maintain Secondary Containment water levels using available Reactor Enclosure sump pumps.
  - d. Confirm isolation of all systems discharging into the area.

Estimated Time Available for Operator Actions: >10 minutes

### 3.35.5 Summary of Diverse Features from PPS

Based upon the analysis for this event, the following diverse features are required, for the postulated CCF of the PPS:

1. Reactor water level NR, WR, and FZ indication



2. Reactor Water Level Low (Level 3) alarm
3. Reactor pressure
4. Reactor power (APRM)
5. APRM Not Downscale indication
6. Control rod position indications
7. RRCS
8. Containment isolation status display
9. Auto MSIV closure on Level 1 (-129 inches)
10. Auto initiation of CS Loop-A on Level 1(-129 inches)
11. Manual control of ADS SRVs
12. Outboard MSIV room temperatures
13. Outboard MSIV room differential temperature
14. RHR Loop-A suppression pool cooling

### 3.35.6 Conclusion

For the postulated Feedwater Line Break Outside Containment, concurrent with a postulated CCF of PPS, sufficient automatic control functions and information that are independent of the PPS, and operator actions, are/will be available to mitigate the event. The diverse automatic MSIV closure when RPV water level decreases below Level 1 maintains the current assumptions for radiological analysis of fission product transport to the environment. Taking no credit for radioactivity release holdup, decay, or plateout during transport through the turbine enclosure, the release of activity to the environment is presented in UFSAR Table 15.6-25. The release is assumed to take place within two hours of the occurrence of the break. The calculated exposures for the realistic analysis are presented in UFSAR Table 15.6-26 and are a small fraction of 10CFR100 limits. In addition, adequate core cooling, RPCB and containment integrity are maintained, the Acceptance Criteria stated in BTP 7-19 3.3(c) for this PA are satisfied.

### 3.36 EVENT: 15.7.1.1 MAIN CONDENSER OFFGAS TREATMENT SYSTEM FAILURE

A failure of the main condenser Offgas Treatment System is postulated to occur. This event is categorized as a Limiting Fault.

#### 3.36.1 Sequence of Events (UFSAR Table 15.7-1)

<u>TIME (sec)</u>	<u>EVENT</u>
0.0	Event begins – system fails.
0.0	Noble gases are released.
<60	Area radiation alarms alert plant personnel.
<60	Operator actions begin with: <ol style="list-style-type: none"> <li>a. Initiation of appropriate system isolations.</li> <li>b. Manual scram actuation.</li> </ol>



- c. Assurance of reactor shutdown cooling.

### **3.36.2 Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS**

1. DFWLCS maintains normal control of RPV water level, until feedpump turbines are tripped on low condenser vacuum
2. Main turbine-generator trips if condenser vacuum decreases below setpoint value
3. Pressure control system modulates turbine bypass valves until inhibited by low condenser vacuum

### **3.36.3 EOP Entry Conditions**

None, because offsite radioactivity release rate is expected to be below the limit for an Alert.

### **3.36.4 Operator Actions per RPV Control EOPs with postulated PPS CCF**

Isolation of the Offgas System will result in loss of condenser vacuum. Refer to Event 15.2.5 Loss of Condenser Vacuum for operator actions.

### **3.36.5 Summary of Diverse Features from PPS**

Refer to Event 15.2.5 Loss of Condenser Vacuum for diverse features required.

### **3.36.6 Conclusion**

For the postulated event of Main Condenser Offgas Treatment System Failure, concurrent with a postulated CCF of PPS, 1) sufficient automatic control functions, 2) indications that are independent of the PPS, and 3) operator actions, are available to mitigate the event. This event does not challenge RCPB and containment integrity. The offsite radioactivity release is provided in UFSAR Tables 15.7-5 and 15.7-8, and is a small fraction of the 10 CFR 100 release limit. Thus BTP 7-19 3.3(c) for this PA are satisfied.

## **3.37 EVENT: 15.7.1.2 MALFUNCTION OF MAIN TURBINE GLAND SEALING SYSTEM**

It is assumed that the turbine gland seal system fails, resulting in activity release in the turbine building and a slow loss of main condenser vacuum due to air in-leakage. This event is categorized as a Limiting Fault.



### **3.37.1 Sequence of Events**

It is assumed that the system fails near the condenser. This results in activity normally processed by the Offgas treatment system being discharged directly to the turbine enclosure and subsequently through the ventilation system to the environment.

### **3.37.2 Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS**

1. DFWLCS maintains normal control of RPV water level, when feedpump turbines are not tripped on low condenser vacuum
2. Main turbine-generator trips if condenser vacuum decreases below setpoint value
3. Pressure control system modulates turbine bypass valves when not inhibited by low condenser vacuum

### **3.37.3 EOP Entry Conditions**

None.

### **3.37.4 Operator Actions**

Refer to OT-116, "Loss of Condenser Vacuum" (Reference 44), and to Section 3.13 for Event 15.2.5 Loss of Condenser Vacuum for operator actions.

### **3.37.5 Summary of Diverse Features from PPS**

Refer to Section 3.13 for Event 15.2.5 Loss of Condenser Vacuum for diverse features required.

### **3.37.6 Conclusion**

For the postulated event of Malfunction of Main Turbine Gland Sealing System, concurrent with a postulated CCF of PPS, 1) sufficient automatic control functions, 2) indications that are independent of the PPS, and 3) operator actions, are available to mitigate the event. This event does not challenge RCPB and containment integrity. The offsite radioactivity release is negligible. Thus BTP 7-19 3.3(c) for this PA are satisfied.

## **3.38 EVENT: 15.7.1.3 FAILURE OF STEAM JET AIR EJECTOR LINES**

It is postulated that the line leading from the steam jet air ejector to the Offgas Treatment System fails. This event is categorized as a Limiting Fault.



### **3.38.1 Sequence of Events**

This failure results in activity normally processed by the Offgas treatment system being discharged directly to the turbine enclosure and subsequently through the ventilation system to the environment.

### **3.38.2 Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS**

1. DFWLCS maintains normal control of RPV water level, when feedpump turbines are not tripped on low condenser vacuum
2. Main turbine-generator trips if condenser vacuum decreases below setpoint value
3. Pressure control system modulates turbine bypass valves when not inhibited by low condenser vacuum

### **3.38.3 EOP Entry Conditions**

None.

### **3.38.4 Operator Actions**

Refer to Section 3.13 for Event 15.2.5 Loss of Condenser Vacuum for operator actions

### **3.38.5 Summary of Diverse Features from PPS**

Refer to OT-116 (Reference 44) and Section 3.13 for Event 15.2.5 Loss of Condenser Vacuum for diverse features required.

### **3.38.6 Conclusion**

For the postulated event of Failure of Steam Jet Air Ejector Lines, concurrent with a postulated CCF of PPS, 1) sufficient automatic control functions, 2) indications that are independent of the PPS, and 3) operator actions, are available to mitigate the event. This event does not challenge RCPB and containment integrity. The offsite radioactivity release is negligible. Thus BTP 7-19 acceptance criteria are satisfied.

## **3.39 EVENT: 15.7.2 LIQUID RADIOACTIVE WASTE SYSTEM FAILURE**

This event requires no PPS monitoring and actuations and thus, requirement for diverse instrumentation and controls are not analyzed.

## **3.40 EVENT: 15.7.3 POSTULATED RADIOACTIVE RELEASES DUE TO LIQUID RADWASTE TANK FAILURE**

This event requires no PPS monitoring and actuations and thus, requirement for diverse instrumentation and controls are not analyzed.



### 3.41 EVENT: 15.7.4 FUEL HANDLING ACCIDENT

The fuel handling accident is assumed to occur as a consequence of a failure of the fuel assembly lifting mechanism resulting in the dropping of a raised fuel assembly onto other fuel bundles. A variety of events that qualify for the class of accidents termed “fuel handling accidents” has been investigated. The accident that produces the largest number of failed spent fuel rods is the drop of a spent fuel bundle and the fuel grapple assembly of the refueling platform into the reactor core when the reactor vessel head is off. The fuel grapple assembly consists of a telescopic mast and head assembly. This event is classified as a Limiting Fault (DBA).

#### 3.41.1 Sequence of Events (UFSAR Table 15.7-15)

<u>TIME (minute)</u>	<u>EVENT</u>
0.0	Fuel assembly is being handled by refueling equipment. The fuel assembly and fuel grapple assembly drop onto the top of the core.
0.0	Some of the fuel rods in both the dropped assembly and reactor core are damaged, resulting in the release of gaseous fission products to the reactor coolant and eventually to the refueling area atmosphere.
<1	The refueling area ventilation radiation monitoring system alarms to alert plant personnel.
<5	Operator actions begin.

#### 3.41.2 Automatic Control Actions in the presence of postulated PPS CCF, diverse from PPS

No automatic control actions are credited for this event. Credit is taken for normal RF HVAC operation and the operability of its exhaust radiation monitors which are lined up as prerequisites to core alterations. Furthermore, in the radiological analysis for the FHA, no credit is taken for automatic HVAC isolation, SGTS, or CREFAS operation to maintain exposure less than regulatory limits.

#### 3.41.3 EOP Entry Conditions

No EOP entry conditions are expected for this event.

#### 3.41.4 Operator Actions

No EOP operator actions are applicable to this event. The actions that the supervisor in charge of fuel handling should take in accordance with procedure ON-120 (Reference 48), “Fuel Handling Problems”, include:

1. Initiate the evacuation of the refueling area.
2. Notify Health Physics.



3. The supervisor in charge of fuel handling will alert the control room operator to the accident.
4. Establish Refuel Floor Secondary Containment.
5. Ensure RF HVAC is isolated and SGTS is initiated.
6. Initiate action to determine the extent of potential radiation doses by measuring the radiation levels in the vicinity of or close to the refueling area.
7. Appropriate radiological control methods should be implemented at the entrance of the refueling area.
8. Before entering the refueling area, a careful study of conditions, radiation levels, etc., will be performed.

### **3.41.5 Summary of Diverse Features from PPS**

Area radiation monitors at the refuel floor area.

### **3.41.6 Conclusion**

For the postulated event of a Fueling Handling Accident, concurrent with a postulated CCF of PPS, sufficient operator actions are available to mitigate the event. In the radiological analysis for the FHA (UFSAR Section 15.7.4.5), no credit is taken for automatic HVAC isolation, SGTS, or CREFAS operation to maintain exposure less than regulatory limits. This event does not challenge RCPB and containment integrity. The offsite radioactivity release is within allowable limits. Thus BTP 7-19 3.3(c) for this PA are satisfied.

## **3.42 EVENT: 15.7.5 SPENT FUEL CASK-DROP ACCIDENT**

This event requires no PPS monitoring and actuations and thus, requirement for diverse instrumentation and controls are not analyzed.

## **3.43 EVENT: 15.7.6 MOVEMENT OF LOADS WITHOUT SECONDARY CONTAINMENT**

This event requires no PPS monitoring and actuations and thus, requirement for diverse instrumentation and controls are not analyzed.

## **3.44 EVENT: 15.7.8 ANTICIPATED TRANSIENTS WITHOUT SCRAM**

RRCS is the system for Anticipated Transient Without Scram (ATWS) mitigation and is completely independent, diverse, and separate from PPS, although some sensors are shared as permitted by 10 CFR 50.62. Specific sensor signals are hardwired into PPS and split to RRCS, prior to the PPS analog input modules. Thus, a postulated CCF in PPS will not affect the operability of RRCS.



### **3.45 SUMMARY OF REQUIRED DPS CONTROLS**

The following Table 3-1 summarizes the required DPS controls needed to cope with the CCF scenarios analyzed in this section.



Table 3-1. Summary of Required DPS Controls

a,c

Chapter 15 Event	Description of Event
15.1.2 (Section 3.2)	FWC Failure- Max Demand without Turbine Bypass
15.1.3 (Section 3.4)	Pressure Regulator Failure-Open
15.2.2 (Section 3.8)	Generator Load Rejection without Bypass
15.2.3 (Section 3.10)	Turbine Trip without Bypass
15.2.4 (Section 3.12)	MSIV Closure



Chapter 15 Event	Description of Event
15.2.5 (Section 3.13)	Loss of Condenser Vacuum
15.2.6 (Section 3.14)	Loss of All Grid Connections
15.2.7 (Section 3.15)	Loss of Feedwater
15.2.9 (Section 3.16)	Loss of Shutdown Cooling
15.6.2 (Section 3.31)	Instrument Line Break
15.6.4 (Section 3.32)	Steam Line Break Outside Containment



Chapter 15 Event	Description of Event
15.6.5 (Section 3.33)	Steam Line Break Inside Containment
15.6.5 (Section 3.34)	Recirculation Line Break Inside Containment
15.6.6 (Section 3.35)	FW Line Break Outside Containment



### 3.46 SUMMARY OF DIVERSE INDICATIONS WITH PLANT IDENTIFIERS

The following tables provide the summary list of diverse displays needed to cope with the CCF scenarios in this section along with the LGS identifier for the indication. The tables cross reference the LGS UFSAR Chapter 15 events calling out these diverse indications for coping with a PPS CCF. Bold, underlined, and italicized texts for in the Device Tag # column of the table indicates additional instruments that need to be shared from PPS for diverse indication at the DPS. The use of “\*” indicates “1” for Limerick Unit 1 or “2” for Unit 2 tag numbers.

In Table 3-2, certain sensors are indicated as “To be shared from PPS”. These sensors are shared from the PPS, by hardwiring of sensor signals to both PPS and to analog input modules at the DCS Remote Node Interface (RNI) located in PPS cabinets. The output signals from these analog input modules are transmitted to DCS via fiberoptic cables for electrical isolation and separation. They are analog sensors, so a CCF of the sensors is not considered. The sensor signals may be displayed on the DPS HMI screens, and thus their entries in the Instrument Tag # and Panel # Location columns are blanked. Table 3-3 summarizes the sensors required for each automatic function specified in Table 3-1.

**Table 3-2. Diverse Indications Summary**

a,c























**Table 3-3. Diverse Sensors for DPS Automatic Functions**

**a,c**



(Last Page of Section 3)



## SECTION 4

### BTP 7-19 POSITION 4 DISPLAYS AND CONTROLS

This is the 2<sup>nd</sup> analysis for D3 CCF described in Section 1. Position 4 of the NRC's position on D3 in SRM/SECY-93-087 and BTP 7-19 states that the applicant shall provide a set of displays and controls in the Main Control Room (MCR) for manual system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. This section defines the Position 4 diverse controls and displays for the critical safety functions.

BTP 7-19 Section 1.2, Position 4 states the following:

*“A set of displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in items 1 and 3 above.”*

SECY-93-0087 identified the following critical safety functions to be managed from the MCR in accordance with Position 4:

- reactivity control
- core heat removal
- reactor coolant inventory
- containment isolation
- containment integrity

Each of these critical safety functions are examined, and diverse controls to achieve each critical safety function and displays to monitor the performance of these functions from the main control room are defined. [

] <sup>a,c</sup>

#### 4.1 REACTIVITY CONTROL

The normal reactivity controls in the BWR are the reactor manual rod control system and the reactor recirculation system. Both systems are non-safety related systems that provide for reactivity control for plant startup, normal power operation, and plant shutdown. The Reactor Protection System (RPS) provides automatic shutdown of the reactor to rapidly insert all control rods, when one or more monitored parameters exceed their trip setpoints. The existing Neutron Monitoring System (NMS) is diverse from PPS and provides reactivity monitoring including core stability monitoring, and trip outputs to RPS, one of the functions of PPS.

##### 4.1.1 Position 4 Controls

The manual scram pushbuttons are hardwired to the RPS TU [ <sup>a,c</sup> providing the reactor shutdown capability diverse from PPS. In the unlikely event of a failure to scram event (ATWS), the diverse RRCS will automatically shut down the reactor by initiation of the SLCS



system, energization of Alternate Rod Insertion (ARI) solenoid valves at the scram air header and tripping both reactor recirculation pumps. RRCS may be manually initiated. Manual controls are provided for initiation of RRCS, ARI and SLC pumps at their respective operator HMI. Recirculation pump trip switches are provided at the main control room panel.

The minimum diverse controls are:

- The RPS manual scram pushbuttons

#### **4.1.2 Position 4 Displays**

The following displays are diverse from PPS and exist in the plant design:

- APRM
- IRM
- Oscillatory power/core stability
- Control rod positions

### **4.2 CORE HEAT REMOVAL**

In normal plant operation after a reactor shutdown, the core decay heat is removed by using the DEHC manual or automatic cool down function by manipulation of the turbine bypass valves discharging steam to the main condenser, when the reactor is at high pressure. If the reactor is isolated from the main condenser heatsink, depressurization and cool down may be performed by manual operation of the SRVs discharging steam to the suppression pool, with heat removal performed by RHR suppression pool cooling at the main control room. Cool down is performed by depressurizing the reactor to achieve a cool down rate less than 100°F/h. When reactor pressure decreases below 75 psig, the RHR Shutdown Cooling Mode can be placed into operation at the PPS. The DFWLCS operates automatically to maintain water level during this cool down process. If the feedwater system is not available, RCIC can be used for reactor coolant makeup during the cool down. When the RHR SDC interlock pressure is clear, the RHR can be used to maintain the reactor at hot shutdown condition or go to cold shutdown conditions.

In accordance with UFSAR 5.4.7.1.1.1, the reactor can be cooled down using the capacity of a single RHR heat exchanger and related RHR Service Water (RHRSW) system capability. Figure 5.4-12 of the UFSAR shows the minimum time required to reduce vessel coolant temperature to 212°F using one RHR heat exchanger in the shutdown cooling mode and allowing 2 hours for flushing.

Note that diverse features outside of the main control room for decay heat removal exist at the Remote Shutdown Panel. These features include controls for shutdown cooling with one loop of RHR and associated RHR cooling water, control of three SRVs for reactor depressurization, and control of reactor inventory using RCIC.

#### **4.2.1 Position 4 Controls**

To meet the BTP 7-19 Position 4 requirement for diverse controls for core decay heat removal from the main control room, controls for one loop of RHR will be implemented in the DPS for shutdown cooling



operation. At the main control room, the non-safety DEHC turbine bypass valves can be used to cool down the reactor and depressurize the reactor to clear the shutdown cooling interlock pressure to enable the one loop of RHR to operate in the shutdown cooling mode, and if the reactor is isolated from the main condenser, the diverse ADS SRVs can be used for reactor depressurization and one loop of RHR aligned for suppression pool cooling.

The minimum diverse controls are:

- Turbine bypass valves (DEHC)
- ADS SRVs
- One loop of RHR (suppression pool cooling, shutdown cooling)

#### **4.2.2 Position 4 Displays**

The following displays are diverse from PPS and exist in the plant design:

- Turbine bypass valve positions
- ADS SRV positions
- RHR heat exchanger inlet temperature
- RHR flow
- RHR pump discharge pressure
- Reactor water level (WR, Shutdown)
- Reactor pressure

### **4.3 REACTOR COOLANT INVENTORY**

In normal reactor power operation, DFWLCS, through modulation of the feedpump turbine speed, provides reactor coolant inventory control when steam is available to drive the feedpump turbines. If the feedpump turbines are not available the condensate pumps are available to inject water into the reactor when reactor pressure is less than the shutoff head of these pumps, approximately 680 psig. If these systems are not available, HPCI and RCIC can provide makeup to the reactor at high pressure. With ADS, the reactor can be depressurized to allow operation of the condensate pumps at reactor pressure less than approximately 680 psig, and also to allow Core Spray and RHR LPCI mode to inject water into the reactor.

UFSAR 6.3.2.5 states the following:

“Certain technical specification LCO periods are justified based on NEDO-24708A which states that for postulated LOCAs, one low pressure ECCS (one LPCI loop or one CS loop) and ADS to depressurize is adequate to reflood the vessel and maintain core cooling sufficient to preclude fuel damage. NEDC-30936P-A, specifically applicable to LGS references NEDO-24708A and reaffirms this conclusion, with the advisory regarding the possible necessity of an alternate cooling path following 2 hours of post large-break LOCA LPCI injection into the core shroud.”

The capability to manually initiate one loop of CS, and manual opening of the five ADS SRVs as diverse features at the main control room, has been identified in the Chapter 15 coping analyses.



#### 4.3.1 Position 4 Controls

The minimum diverse controls for inventory control are:

- Feedwater /Level control system (DFWLCS)
- ADS SRVs
- Condensate pumps

#### 4.3.2 Position 4 Displays

The following displays either exist in the plant design or have already been identified to be diverse in the coping analysis in Section 3:

- Reactor water level (WR, FZ)
- Reactor pressure
- Turbine bypass valve positions
- ADS SRV positions
- Feedwater/condensate pumps status

### 4.4 CONTAINMENT ISOLATION

There are numerous conditions that isolate the reactor and containment penetrations. UFSAR Table 6.2-17 provides a list of the isolation valves, automatic isolation conditions, valve tag numbers, etc. The NSSSS automatically closes specific isolation valves upon specific conditions in the reactor or containment. The purposes of isolation are to limit coolant loss and to limit radioactivity release to the secondary containment (reactor enclosure) and to the environment. Upon secondary containment isolation, the safety-related Standby Gas Treatment System limits the release to an acceptable level.

#### 4.4.1 Position 4 Controls – Primary Containment

[

] <sup>a,c</sup>



[

] <sup>a,c</sup> the following isolation valves are chosen to have diverse manual control capability as backups to CCF in PPS:

Note: The below use of \* prefix to a valve number represents 1 for Unit 1 and 2 for Unit 2. The use of \* in the suffix to a valve number represents A, B, C, or D.

1. HV-041-\*F022\*, Inboard MSIVs
2. HV-041-\*F028\*, Outboard MSIVs
3. HV-049-\*F007, Inboard RCIC Steam Line Isolation Valve
4. HV-055-\*F002, Inboard HPCI Steam Line Isolation Valve
5. HV-051-\*F008, Outboard Shutdown Cooling Supply Line Isolation Valve
6. HV-051-\*F009, Inboard Shutdown Cooling Supply Line Isolation Valve
7. HV-051-\*F015A, Outboard Shutdown Cooling Return Isolation Valve
8. HV-051-\*F015B, Outboard Shutdown Cooling Return Isolation Valve
9. HV-044-\*F001, Inboard RWCU Supply Line Isolation Valve
10. HV-051-\*F017\*, Outboard LPCI Discharge Isolation Valve

#### 4.4.2 Position 4 Controls – Secondary Containment (Reactor Enclosure)

To limit radioactivity release to the environment, the secondary containment needs to be isolated. The following diverse controls will isolate the HVAC supply and exhaust flow paths, and upon isolation the Standby Gas Treatment System (SGTS) automatically initiates to maintain a negative pressure in the secondary containment, limiting potential radioactivity release to the environment:

1. Reactor Enclosure Air Supply, HV-76-\*07
2. Reactor Enclosure Air Supply, HV-76-\*08
3. Reactor Enclosure Ventilation Exhaust, HV-76-\*57
4. Reactor Enclosure Ventilation Exhaust, HV-76-\*58
5. Reactor Enclosure Equipment Compartment Exhaust, HV-76-\*41
6. Reactor Enclosure Equipment Compartment Exhaust, HV-76-\*42

#### 4.4.3 Position 4 Displays

The following displays either exist in the plant design or have already been identified to be diverse in the coping analysis in Section 3:

1. RPV water level (WR)
2. Drywell pressure
3. RE HVAC exhaust radiation
4. Refuel floor radiation
5. Differential pressure between reactor building and outside atmosphere.



Status of all containment isolation valves is acquired and displayed on the DPS [

] <sup>a,c</sup>

## 4.5 CONTAINMENT INTEGRITY

USFAR 6.2.1.1.3.3.1.3 Assumptions for Long-Term Cooling, states that after the DBA blowdown period, flow from one RHR pump can be actuated for containment cooling, and that containment spray need not be actuated at all to keep the containment pressure below the containment design pressure. Analytically, no credit may be assumed for containment cooling earlier than 10 minutes after the accident and cooling is assumed to begin at 10 minutes. However, containment cooling will be initiated in accordance with plant emergency operating procedures based upon plant conditions.

### 4.5.1 Position 4 Controls

To meet Position 4 requirement for diverse system initiation for containment integrity, one loop of RHR for suppression pool cooling is needed, with the capability for suppression pool sprays. RHR suppression pool cooling is needed to assure that the pool temperature can be maintained below the structural design value. Suppression pool spray capability is needed to mitigate potential steam bypass leakage from the drywell to the wetwell, to limit containment pressure to below the design limit. The same RHR loop previously identified for core decay heat removal (RHR Shutdown Cooling) satisfies this requirement.

The minimum diverse controls are:

1. One loop of RHR (suppression pool cooling, suppression pool spray)

### 4.5.2 Position 4 Displays

The diverse displays needed to support containment cooling are:

1. RHR flow (suppression pool cooling mode, suppression pool spray mode)
2. Suppression pool temperature
3. Drywell temperature
4. Drywell pressure
5. Suppression pool pressure (wetwell pressure)

## 4.6 SUMMARY OF POSITION 4 DIVERSE CONTROLS

The following diverse manual controls constitute the minimum inventory of controls for the critical safety functions, and are to be implemented in the DPS, to meet the Position 4 requirements addressing CCF in the PPS:

Note: The use of **bold underline italic text** below indicates diverse controls that are required to be implemented in DPS. The use of “\*” indicates “1” for Limerick Unit 1 or “2” for Unit 2 tag numbers.

1. Reactivity Control:



PPS hardwired manual scram pushbuttons. Diverse features outside of PPS that exist in the current plant design are automatic RRCS initiation, and manual initiation of RRCS, ARI, SLCS, and RPT actuation.

2. Core Heat Removal:

- a. Turbine bypass valves (DEHC)
- b. *RHR Loop-A shutdown cooling*
- c. *RHR Loop-A suppression pool cooling\*\**
- d. *ADS SRVs\*\**

3. Reactor Coolant Inventory:

- a. DFWLCS
- b. *ADS SRVs\*\**

4. Primary Containment Isolation Valves: [

] <sup>a,c</sup>

5. Secondary Containment\*\* [

] <sup>a,c</sup>

6. Containment Integrity:

*RHR Loop -A suppression pool cooling\*\*, and suppression pool spray*

\*\*Previously included in Chapter 15 coping analysis



## 4.7 SUMMARY OF DIVERSE POSITION 4 DISPLAYS

The following displays constitute the minimum inventory for displays to support the critical safety functions and are already part of SPDS provided by PPC, or on dedicated displays (e.g., control rod positions), diverse from PPS. Unless otherwise noted, the device tag numbers can be found in Table 3-2. The use of “\*” indicates “1” for Limerick Unit 1 or “2” for Unit 2 tag numbers.

1. Reactivity Control:
  - a. APRM
  - b. IRM
  - c. Control rod positions
2. Core Heat Removal:
  - a. Turbine bypass valve positions
  - b. SRV positions
  - c. RHR heat exchanger inlet temperature (Device Tag #: **TE-051-\*N004A(B)**, to be diverse from PPS)
  - d. RHR pump discharge flow (Device Tag #: **FT-051-\*N015A (B, C, D)**, to be shared from PPS)
  - e. RHR pump discharge pressure (Device Tag #: **PT-051-\*N053A (B, C, D)**, to be shared from PPS)
  - f. RPV water level (NR, Shutdown, Upset)
  - g. **RPV water level (WR)**, identified previously in Chapter 15 coping analysis)
  - h. RPV pressure
3. Reactor Coolant Inventory:
  - a. **RPV water level (WR, FZ)**, identified previously in Chapter 15 coping analysis)
  - b. RPV pressure
4. Containment Isolation:
  - a. Status display of specific containment isolation valves
  - b. **RPV water level (WR)**, identified previously in Chapter 15 coping analysis)
  - c. **Drywell pressure** (identified previously in Chapter 15 coping analysis)
  - d. RE HVAC exhaust radiation
  - e. Refuel floor radiation
  - f. Differential pressure between reactor building and outside atmosphere
5. Containment Integrity:
  - a. RHR flow (suppression pool cooling mode, containment sprays)
  - b. Suppression pool temperature



- c. Drywell temperature
- d. Drywell pressure (NR, identified previously in Chapter 15 coping analysis)
- e. Suppression pool pressure (wetwell pressure)

## 4.8 CONCLUSION

The Position 4 criteria of BTP 7-19 are satisfied:

- a. Proposed manual actions credited to accomplish safety functions that would otherwise have been accomplished by automatic safety systems are both feasible and reliable. This will be included in an HFE analysis for the PPS.
- b. The minimum inventory of displays and controls in the MCR are identified, and this minimum inventory allows the operator to effectively monitor and control the critical safety parameters of reactivity, core heat removal, and reactor coolant inventory. The minimum inventory also allows the operator to initiate and monitor the status of containment isolation and containment integrity.
- c. The proposed manual operator actions are prescribed by Limerick approved plant procedures and subject to appropriate training. Procedure updates or a new procedure for the DPS will be required.
- d. The manual controls for critical safety functions are at the system or division level and are located within the MCR.
- e. The SPDS displays and manual controls at DPS are independent and diverse from PPS. These displays and controls are not affected by postulated CCFs that could disable the corresponding functions within PPS.

(Last Page of Section 4)



## **SECTION 5 CCF SPURIOUS ACTUATION ANALYSIS**

As described in Section 1, this is the third of three analyses to assess the adequacy of the LGS plant defense in depth and diversity to cope with a PPS spurious actuation due to a CCF.

The LGS design basis assumes manual actuations are not required for 10 minutes after a postulated accident (PA) commences (e.g., LGS UFSAR Chapter 7.5.2.4.1, Initial Accident Event). The LGS Plant Reference Simulator (PRS) was used as a tool to guide the analysis for necessary manual operator actions and estimates for time available for these actions. A separate HFE evaluation is conducted to evaluate the adequacy of the required diverse manual actions using the acceptance criteria in NUREG-0800, Chapter 18, Attachment A as a guide.

BTP 7-19 introduces the concept of PPS spurious actuation due to a CCF. A PPS spurious actuation is considered an event initiator rather than a failure to respond to a FSAR Accident Analysis event. [

] <sup>a,c</sup>





Figure 5-1. [ ]<sup>a,c</sup>

[

] <sup>a,c</sup>

For spurious initiations of HPCI, or LPCI, or CS at low RPV pressure conditions, the RPV will overfill and flood the main steam lines. The acceptability of the overfill condition was evaluated under Generic Letter 89-19 and USI A-47 (Reference 37) from the NRC. For Limerick the evaluation results were captured in the UFSAR and the operation procedure OT-110 (Reference 11) which addressed reactor vessel overfill. The analysis was submitted to the NRC as part of the required response to Generic Letter 89-19 in 1990. For Limerick, evaluation of this issue was performed, and the results were used to revise the UFSAR and to develop the actions for the operation procedure OT-110 (Reference 11).

Similar to the format for the CCF coping analysis in Section 3, the follow legend is used:

1. Initiating event description.
2. The diverse automatic controls that will be initiated as a result of the event without the PPS. **Text in this format** indicates an additional diverse automatic actuation that is needed from the DPS.
3. Diverse indications available to the operator as a result of the event plus the PPS CCF; and the Emergency Operating Procedures (EOPs) that these indications will lead the operator to follow to mitigate the event. Any additional diverse indications needed will be indicated **with text in this format**.
4. Manual operator actuations directed by the EOP. **Text in this format** indicates additional diverse manual actuations needed to cope with the CCF scenario.
5. Summary of diverse indications available in the current plant design. **Text in this format** indicates additional diverse controls needed.
6. Scenario summary.



The LGS design basis assumes manual actuations are not required for 10 minutes after a postulated accident (PA) commences (e.g., LGS UFSAR Chapter 7.5.2.4.1, Initial Accident Event).

**5.1** [ ]<sup>a,c</sup>

[ ]<sup>a,c</sup>

**5.1.1** [ ]<sup>a,c</sup>

[ ]<sup>a,c</sup>

**5.1.2** [ ]<sup>a,c</sup>

[

] <sup>a,c</sup>

**5.1.3** [ ]<sup>a,c</sup>

[

] <sup>a,c</sup>

**5.1.4** [ ]<sup>a,c</sup>

[

] <sup>a,c</sup>



5.1.5 [ ]<sup>a,c</sup>

[

] <sup>a,c</sup>

### 5.1.6 Conclusion

[

] <sup>a,c</sup>

5.2 [ ]<sup>a,c</sup>

] <sup>a,c</sup>

5.2.1 [ ]<sup>a,c</sup>

[

] <sup>a,c</sup>

5.2.2 [ ]<sup>a,c</sup>

[

] <sup>a,c</sup>

5.2.3 [ ]<sup>a,c</sup>

[ ]<sup>a,c</sup>



5.2.4 [ ]<sup>a,c</sup>

[

] <sup>a,c</sup>

5.2.5 [ ]<sup>a,c</sup>

[

] <sup>a,c</sup>

5.2.6 Conclusion

[

] <sup>a,c</sup>

5.3 [ ]<sup>a,c</sup>

[

] <sup>a,c</sup>

5.3.1 [ ]<sup>a,c</sup>

[

] <sup>a,c</sup>

5.3.2 [ ]<sup>a,c</sup>

[

] <sup>a,c</sup>



[

] <sup>a,c</sup>

**5.3.3** [ ] <sup>a,c</sup>

[

] <sup>a,c</sup>

**5.3.4** [ ] <sup>a,c</sup>

[

] <sup>a,c</sup>



5.3.5 [ ]<sup>a,c</sup>

[

] <sup>a,c</sup>

### 5.3.6 Conclusion

[

] <sup>a,c</sup>

5.4 [ ]<sup>a,c</sup>

[

] <sup>a,c</sup>

5.4.1 [ ]<sup>a,c</sup>

[

] <sup>a,c</sup>

5.4.2 [ ]<sup>a,c</sup>

[

] <sup>a,c</sup>



5.4.3 [ ]<sup>a,c</sup>

[

] <sup>a,c</sup>

5.4.4 [ ]<sup>a,c</sup>

[

] <sup>a,c</sup>

5.4.5 [ ]<sup>a,c</sup>

[

] <sup>a,c</sup>

5.4.6 Conclusion

[

] <sup>a,c</sup>



[ ]<sup>a,c</sup>

5.5 [ ]<sup>a,c</sup>

] <sup>a,c</sup>

5.5.1 [ ]<sup>a,c</sup>

[ ]<sup>a,c</sup>

5.5.2 [ ]<sup>a,c</sup>

[

] <sup>a,c</sup>

5.5.3 [ ]<sup>a,c</sup>

[

] <sup>a,c</sup>



5.5.4 [ ]<sup>a,c</sup>

[

]<sup>a,c</sup>

5.5.5 [ ]<sup>a,c</sup>

]<sup>a,c</sup>

5.5.6 Conclusion

[

]<sup>a,c</sup>



[

] <sup>a,c</sup>

5.6

[

] <sup>a,c</sup>

[

] <sup>a,c</sup>

5.6.1

[

] <sup>a,c</sup>

[

] <sup>a,c</sup>

5.6.2

[

] <sup>a,c</sup>

[

] <sup>a,c</sup>



5.6.3 [ ]<sup>a,c</sup>

[ ]<sup>a,c</sup>

[

] <sup>a,c</sup>

5.6.4 [ ]<sup>a,c</sup>

[

5.6.5 [ ]<sup>a,c</sup>

] <sup>a,c</sup>



[

] <sup>a,c</sup>

### 5.6.6 Conclusion

[

] <sup>a,c</sup>

5.7 [

] <sup>a,c</sup>

[

] <sup>a,c</sup>

5.7.1 [ ] <sup>a,c</sup>

[

] <sup>a,c</sup>

5.7.2 [ ] <sup>a,c</sup>

[

] <sup>a,c</sup>



[

] <sup>a,c</sup>

**5.7.3** [ ] <sup>a,c</sup>

[

] <sup>a,c</sup>

**5.7.4** [ ] <sup>a,c</sup>  
[

] <sup>a,c</sup>

**5.7.5** [ ] <sup>a,c</sup>

[

] <sup>a,c</sup>



[

] <sup>a,c</sup>

### 5.7.6 Conclusion

[

] <sup>a,c</sup>

5.8 [ ] <sup>a,c</sup>

[

] <sup>a,c</sup>

5.8.1 [ ] <sup>a,c</sup>

[

] <sup>a,c</sup>

5.8.2 [ ] <sup>a,c</sup>

[

] <sup>a,c</sup>



[

] <sup>a,c</sup>

**5.8.3** [ ] <sup>a,c</sup>

[ ] <sup>a,c</sup>

**5.8.4** [ ] <sup>a,c</sup>

[

] <sup>a,c</sup>

**5.8.5** [ ] <sup>a,c</sup>

[

] <sup>a,c</sup>

**5.8.6 Conclusion**

[

] <sup>a,c</sup>



<b>5.9</b>	[	]	<b>a,c</b>
	[		<b>a,c</b>
<b>5.9.1</b>	[	]	<b>a,c</b>
	[	]	<b>a,c</b>
<b>5.9.2</b>	[	]	<b>a,c</b>
	[		
		]	<b>a,c</b>
<b>5.9.3</b>	[	]	<b>a,c</b>
	[		
		]	<b>a,c</b>
<b>5.9.4</b>	[	]	<b>a,c</b>
	[		
		]	<b>a,c</b>
<b>5.9.5</b>	[	]	<b>a,c</b>
	[	]	<b>a,c</b>



[

]a,c

## 5.9.6 Conclusion

[

]a,c

5.10 [ ]a,c

[

]a,c

5.10.1 [ ]a,c

[

]a,c

5.10.2 [ ]a,c

[

]a,c

5.10.3 [ ]a,c

[

]a,c



[

]a,c

**5.10.4** [

]a,c

[

]a,c

**5.10.5** [

]a,c

[

]a,c

**5.10.6 Conclusion**

[

]a,c

**5.11** [

]a,c

[

]a,c



[  
] <sup>a,c</sup>

**5.12** [ ] <sup>a,c</sup>

[ ] <sup>a,c</sup>

(Last Page of Section 5)



## SECTION 6

### DIVERSITY ATTRIBUTES BETWEEN PPS, DCS, AND OTHER CREDITED SYSTEMS

This section describes the diversity attributes between the PPS and the DCS which are credited for diverse backup to required functions to cope with the CCF scenarios. DCS include the RRCS, DPS, and the Diverse Non-Safety System Interface indicated in Figure 6-1. The attribute categories are from NUREG-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems (Reference 19). The diversity attributes are:

- Human Diversity
- Design Diversity
- Software Diversity
- Functional Diversity
- Signal Diversity
- Equipment Diversity

Sections 6.1 through 6.6 provide a detailed assessment of the diversity attributes of the DCS (DPS/RRCS). Section 6.7 provides a summary table of the diversity attributes of the existing LGS systems that are credited for diverse display and control.

#### 6.1 HUMAN DIVERSITY

##### PPS

The Common Q Platform AC160 controller was designed and manufactured by Asea Brown Boveri (ABB) and the Common Q Platform Flat Panel Display System is a Westinghouse bespoke design using commercially dedicated equipment manufactured by a third party. The personnel involved in the design and implementation of the AC160 controller were ABB personnel. Recently Westinghouse obtained the rights to the design and maintenance of the AC160 controller. Any modifications to the AC160 controller will be performed within the same Westinghouse safety systems organization within Westinghouse responsible for the PPS. [

] <sup>a,c</sup>

The Westinghouse team developing the PPS application on the Common Q Platform are in the Westinghouse safety system design organization, which utilizes different personnel for the design and implementation of the PPS than those designing and implementing the DCS.

##### DCS

The DCS is implemented using the non-safety, diverse and separate Ovation platform, designed and manufactured by Emerson. The personnel involved in the design, implementation and test of the Ovation platform are Emerson personnel. [

] <sup>a,c</sup>



[

] <sup>a,c</sup>

The Westinghouse team developing the DCS applications on the Ovation platform are in the Westinghouse non-safety control system design organization, with utilizes different personnel for the design and implementation of the DCS than those designing and implementing the PPS.

## **6.2 DESIGN DIVERSITY**

The comparison in architecture between the PPS and the DCS is depicted in Figure 6-1. [

] <sup>a,c</sup> Thus, the design of the DCS is diverse from the PPS design.



Figure 6-1. PPS and DCS Architectures



## 6.3 SOFTWARE DIVERSITY

[

]<sup>a,c</sup>

## 6.4 FUNCTIONAL DIVERSITY

The functional design of the PPS is based on the controls of existing LGS RPS, NSSSS, and ECCS. The control functionality of the DPS is based on the results of this analysis. The DPS is a new control system design developed to implement diverse automatic and manual protection functions identified in this analysis in case the PPS suffers a software CCF. The functional design of the RRCS is based on the existing LGS RRCS and is implemented in the DCS.

## 6.5 SIGNAL DIVERSITY

The PPS uses signals it needs to perform the same functions as the existing LGS RPS, NSSSS, and ECCS. These sensors are shared from the PPS, using 1E qualified isolators for electrical separation. The PPS and sensors use diverse technology, so a CCF of the sensors and PPS is not considered. The RRCS uses the required signals necessary to perform the same functions as the existing RRCS. The DPS and RRCS use the same sensors as the PPS to perform the backup automatic protection functions as allowed by NUREG-0800, Chapter 7, BTP 7-19 and 10 CFR 50.62. The DPS/RRCS and PPS are not susceptible to the same CCF. The DPS/RRCS and PPS read the sensor signal using diverse input hardware (see section 6.6). Failure of a DPS/RRCS input module will not impact the ability of the PPS read the field sensor. The power source for the signal is also not susceptible to a CCF as described in section 2.2.4.

## 6.6 EQUIPMENT DIVERSITY

As explained in the previous sections, the PPS and DCS use different platforms manufactured by different companies. [

]<sup>a,c</sup>

The CIM is used by both the PPS and DCS to interface to the same safety-related components. As discussed in Section 2.2, the CIM is not considered vulnerable to a CCF.

## 6.7 DIVERSITY ATTRIBUTES OF EXISTING CONTROL AND MONITORING SYSTEMS

The existing control and monitoring systems, and their diversity attributes that are taken credit for diverse backup to required functions to cope with the CCF scenarios, are described in Table 6-1.



Table 6-1 Diversity Attributes of Control and Monitoring Systems

<u>System</u>	<u>Human</u> <u>Diversity</u>	<u>Design</u> <u>Diversity</u>	<u>Software</u> <u>Diversity</u>	<u>Functional</u> <u>Diversity</u>	<u>Signal</u> <u>Diversity</u>	<u>Equipment</u> <u>Diversity</u>
RBM (RMCS) APRM (NMS) RWM (RMCS)	General Electric Company	Independent hardware and MCR displays (ODAs)	Custom GEH code run on an executive loop	Monitors neutron flux in core	LPRM's are direct inputs to APRMs / RBM	NUMAC, Harris 80C36 microprocessor
SRM / IRM (NMS)	General Electric Company	Independent hardware and MCR displays (Analog Meters)	N/A	Monitors neutron flux in core	SRM / IRM detectors directly to associate analog drawer	Analog
DFWLCS	ABB (Westinghouse)	Independent hardware and MCR operator workstation / analog meters	<ul style="list-style-type: none"> <li>• Unix MCR workstation</li> <li>• Control builder for function blocks</li> </ul>	Controls reactor level via speed demand to non-safety related reactor feedwater pumps	Independent, non-safety related, reactor level, feedwater flow and steam line flow sensors	AC450
Reactor Feedpump Turbine Trip Circuits, Low Suction Pressures	Bechtel	Independent analog hardware (Independent of both PPS and DFWLCS)	N/A	Provides trip signal to A/B/C reactor feedwater pump turbine speed control system	Independent, non-safety related, feedpump suction pressure switches and time delay relays (5s for C, 10s for B, and 15s for A turbine trips)	Analog



<u>System</u>	<u>Human Diversity</u>	<u>Design Diversity</u>	<u>Software Diversity</u>	<u>Functional Diversity</u>	<u>Signal Diversity</u>	<u>Equipment Diversity</u>
DEHC	Westinghouse	Independent hardware and MCR operator workstation	<ul style="list-style-type: none"> <li>Ovation MCR workstation</li> <li>Ovation Control Builder for function blocks</li> </ul>	Controls reactor pressure via turbine control valves and bypass valves	Independent, non-safety related, reactor and MSL pressure sensors	Ovation 3.3.1
Plant Process Computer (PPC)	Sciencetech	Independent hardware and MCR operator workstations (multiple)	<ul style="list-style-type: none"> <li>R*Time (MCR Displays)</li> <li>Custom Sciencetech code (system servers)</li> </ul>	Monitors plant parameters via dedicated I/O	<ul style="list-style-type: none"> <li>Independent sensors</li> <li>Monitors shared sensors signal via independent I/O</li> </ul>	<ul style="list-style-type: none"> <li>RTP I/O</li> <li>HP servers</li> <li>Cisco network switches</li> </ul>
Reactor Feedwater Pump Turbine (RFPT) speed control (DFWLCS)	Woodward	Independent hardware and dedicated MCR hand switches	Control Assistant	Controls reactor level via speed demand to non-safety related reactor feedwater pumps	<ul style="list-style-type: none"> <li>Automatic input from DFWLCS</li> <li>Manual input from MCR hand switches</li> <li>Independent speed sensors</li> </ul>	MicroNet (Motorola MPC5200)
Condensate System and Feedwater System Injection Valves	Bechtel	Independent hardware and dedicated MCR hand switches	N/A	Inject water into the reactor using condensate pumps and injection valves	Manual input from MCR operators	Analog



<u>System</u>	<u>Human Diversity</u>	<u>Design Diversity</u>	<u>Software Diversity</u>	<u>Functional Diversity</u>	<u>Signal Diversity</u>	<u>Equipment Diversity</u>
Recirculation Flow Control (RFCS)	Siemens	Independent hardware and dedicated MCR pushbuttons	PLC: Simatic Step 7 for programing	Controls recirculation pump speed (neutron flux) via dedicated inputs from MCR pushbuttons	Manual input from MCR operators	Simatic S7400 Adjustable Speed Drive
Reactor Manual Control (RMCS)	GE Nuclear	Independent hardware and dedicated MCR control panel	N/A	Controls reactor power via control of rod positions via dedicated inputs from MCR control panel	Manual input from MCR operators	TTL
Nuclear Boiler Instrumentation (NBI)	GE Nuclear	Independent hardware and dedicated MCR display	N/A	Provides independent displays of RPV water level	Independent sensors	Analog
Standby Gas Treatment System (SGTS)	Bechtel	Independent hardware with local controls / indications	Firmware	Provides carbon filtration exhaust path for secondary containment	Independent fans and dampers	Moore Industries Model 535 controllers
Reactor Enclosure Recirculation System (RERS)	Bechtel	Independent hardware with local controls / indications	Firmware	Provides recirculation path for secondary containment	Independent fans and dampers	Moore Industries Model 535 controllers



<u>System</u>	<u>Human Diversity</u>	<u>Design Diversity</u>	<u>Software Diversity</u>	<u>Functional Diversity</u>	<u>Signal Diversity</u>	<u>Equipment Diversity</u>
Area Radiation Monitors (Refuel Floor)	GE Nuclear	Local independent hardware and dedicated display	N/A	Monitor refueling area radiation and annunciation.	Independent radiation sensors	Analog
Reactor Mode Switch (RPS, refuel bridge and control rod block)	GE Nuclear	Independent hardware and MCR hand switch	N/A	Provides interlock signals to RMCS	Dedicated contacts for Refuel position	Analog

(Last Page of Section 6)



\*\*This page was added to the quality record by the PRIME system upon its validation and shall not be considered in the page numbering of this document.\*\*

## Approval Information

Author Approval Tang Calvin K Aug-04-2022 10:17:01

Reviewer Approval Setchenski Boyan A Aug-04-2022 14:23:44

Reviewer Approval Seaman Stephen Aug-04-2022 16:50:48

Verifier Approval Odess Gillett Warren Aug-04-2022 17:04:49

Verifier Approval Solmos Matthew Aug-04-2022 17:05:28

Manager Approval Pantis William G Aug-04-2022 22:59:59

Files approved on Aug-04-2022

\*\*\* This record was final approved on 8/4/2022, 10:59:59 PM. (This statement was added by the PRIME system upon its validation)



**ATTACHMENT 3 TRANSMITTED HERewith CONTAINS PROPRIETARY INFORMATION –  
WITHHOLD UNDER 10 CFR 2.390**

**Attachment 3**

**Limerick Generating Station, Units 1 and 2  
Docket Nos. 50-352 and 50-353**

**Limerick Generating Station Defense in Depth and Diversity Common Cause Failure  
Coping Analysis, WNA-AR-01074-GLIM-P, Revision 2**



**ATTACHMENT 4**

**Limerick Generating Station, Units 1 and 2  
NRC Docket Nos. 50-352 and 50-353**

**Affidavit CAW-22-028**



Commonwealth of Pennsylvania:

County of Butler:

- (1) I, Zachary Harper, Manager, Licensing Engineering, have been specifically delegated and authorized to apply for withholding and execute this Affidavit on behalf of Westinghouse Electric Company LLC (Westinghouse).
- (2) I am requesting the proprietary portions of WCAP-18598-P, Revision 0 be withheld from public disclosure under 10 CFR 2.390.
- (3) I have personal knowledge of the criteria and procedures utilized by Westinghouse in designating information as a trade secret, privileged, or as confidential commercial or financial information.
- (4) Pursuant to 10 CFR 2.390, the following is furnished for consideration by the Commission in determining whether the information sought to be withheld from public disclosure should be withheld.
  - (i) The information sought to be withheld from public disclosure is owned and has been held in confidence by Westinghouse and is not customarily disclosed to the public.
  - (ii) The information sought to be withheld is being transmitted to the Commission in confidence and, to Westinghouse's knowledge, is not available in public sources.
  - (iii) Westinghouse notes that a showing of substantial harm is no longer an applicable criterion for analyzing whether a document should be withheld from public disclosure. Nevertheless, public disclosure of this proprietary information is likely to cause substantial harm to the competitive position of Westinghouse because it would enhance the ability of competitors to provide similar technical evaluation justifications and licensing defense services for commercial power reactors without commensurate expenses. Also, public disclosure of the information would enable others to use the information to meet NRC requirements for licensing documentation without purchasing the right to use the information.




- (5) Westinghouse has policies in place to identify proprietary information. Under that system, information is held in confidence if it falls in one or more of several types, the release of which might result in the loss of an existing or potential competitive advantage, as follows:
- (a) The information reveals the distinguishing aspects of a process (or component, structure, tool, method, etc.) where prevention of its use by any of Westinghouse's competitors without license from Westinghouse constitutes a competitive economic advantage over other companies.
  - (b) It consists of supporting data, including test data, relative to a process (or component, structure, tool, method, etc.), the application of which data secures a competitive economic advantage (e.g., by optimization or improved marketability).
  - (c) Its use by a competitor would reduce his expenditure of resources or improve his competitive position in the design, manufacture, shipment, installation, assurance of quality, or licensing a similar product.
  - (d) It reveals cost or price information, production capacities, budget levels, or commercial strategies of Westinghouse, its customers or suppliers.
  - (e) It reveals aspects of past, present, or future Westinghouse or customer funded development plans and programs of potential commercial value to Westinghouse.
  - (f) It contains patentable ideas, for which patent protection may be desirable.
- (6) The attached documents are bracketed and marked to indicate the bases for withholding. The justification for withholding is indicated in both versions by means of lower-case letters (a) through (f) located as a superscript immediately following the brackets enclosing each item of information being identified as proprietary or in the margin opposite such information. These lower-case letters refer to the types of information Westinghouse customarily holds in confidence identified in Sections (5)(a) through (f) of this Affidavit.



I declare that the averments of fact set forth in this Affidavit are true and correct to the best of my knowledge, information, and belief. I declare under penalty of perjury that the foregoing is true and correct.

Executed on: 7/11/2022

A handwritten signature in black ink, appearing to read "Zachary Harper", is written over a horizontal line.

Signed electronically by

Zachary Harper



\*\*This page was added to the quality record by the PRIME system upon its validation and shall not be considered in the page numbering of this document.\*\*

## Approval Information

Manager Approval Harper Zachary S Jul-11-2022 15:44:16

Files approved on Jul-11-2022

\*\*\* This record was final approved on 7/11/2022, 3:44:16 PM. (This statement was added by the PRIME system upon its validation)



**Attachment 5**

**Limerick Generating Station, Units 1 and 2  
Docket Nos. 50-352 and 50-353**

**Licensing Technical Report for the Limerick Generating Station Units 1&2  
Digital Modernization Project, WCAP-18598-NP, Revision 0**



# **Licensing Technical Report for the Limerick Generating Station Units 1&2 Digital Modernization Project**





**WCAP-18598-NP**  
**Revision 0**

**Licensing Technical Report for the Limerick Generating  
Station Units 1&2 Digital Modernization Project**

**Warren R. Odess-Gillett\***  
Licensing Engineering

**July 2022**

Reviewers: Stephen Seaman\*  
Safety I&C  
  
Matthew Solmos\*  
Component Engineering  
  
Matthew A. Shakun\*  
Licensing Engineering  
  
Dominic M. Mocello\*  
I&C Safety, Plant Protection System

Approved: Zachary S. Harper\*, Manager  
Licensing Engineering

\*Electronically approved records are authenticated in the electronic document management system.

---

Westinghouse Electric Company LLC  
1000 Westinghouse Drive  
Cranberry Township, PA 16066, USA

© 2022 Westinghouse Electric Company LLC  
All Rights Reserved



**REVISION HISTORY**

<b>Revision</b>	<b>Author</b>	<b>Description</b>	<b>Completed</b>
A	Warren Odess-Gillett	Initial issue.	6/6/2022
0	Warren Odess-Gillett	Incorporated comments from Constellation.	See PRIME

**OPEN ITEMS**

<b>Item</b>	<b>Description</b>	<b>Status</b>
	None.	



## TABLE OF CONTENTS

REVISION HISTORY .....	II
OPEN ITEMS.....	II
LIST OF TABLES .....	vii
LIST OF FIGURES .....	viii
ACRONYMS AND TRADEMARKS .....	x
1 INTRODUCTION .....	1-1
2 PLANT SYSTEM DESCRIPTION (D.1) .....	2-1
2.1 REACTOR PROTECTION SYSTEM .....	2-1
2.2 PRIMARY CONTAINMENT AND REACTOR VESSEL ISOLATION CONTROL SYSTEM.....	2-3
2.3 EMERGENCY CORE COOLING SYSTEM .....	2-14
2.4 REDUNDANT REACTIVITY CONTROL SYSTEM.....	2-15
2.5 REACTOR CORE ISOLATION COOLING SYSTEM.....	2-17
2.6 STANDBY LIQUID CONTROL SYSTEM.....	2-17
2.7 RG 1.97 INDICATIONS.....	2-18
3 SYSTEM ARCHITECTURE (D.2) .....	3-1
3.1 EXISTING SYSTEM ARCHITECTURE (D.2.1).....	3-3
3.1.1 RPS.....	3-5
3.1.2 PCRVICS.....	3-12
3.1.3 ECCS .....	3-22
3.1.4 Reactor Core Isolation Cooling System .....	3-39
3.1.5 Standby Liquid Control System .....	3-43
3.1.6 RRCS.....	3-45
3.2 PPS - NEW SYSTEM ARCHITECTURE (D.2.2) .....	3-46
3.2.1 Bistable Processing Logic .....	3-52
3.2.2 Local Coincidence Logic.....	3-52
3.2.3 Reactor Scram Matrix.....	3-54
3.2.4 Integrated Logic Processor .....	3-57
3.2.5 Component Interface Module.....	3-62
3.2.6 Interface and Test Processor .....	3-69
3.2.7 Maintenance and Test Panel .....	3-70
3.2.8 Safety Displays.....	3-72
3.2.9 Power Supply .....	3-73
3.2.10 HVAC Requirements .....	3-75
3.2.11 PPS Design Function.....	3-75
3.2.12 Service/Test Functions.....	3-76
3.2.13 Separation and Independence .....	3-77
3.2.14 Cross Divisional Interfaces.....	3-77
3.2.15 Connections to Human-System Interfaces .....	3-77
3.2.16 Connections between Safety-Related Systems.....	3-78



3.2.17	Connections between Safety-Related and Non-Safety-Related Systems .....	3-78
3.2.18	Temporary connections .....	3-78
3.2.19	Interfacing with Supporting Systems .....	3-78
3.2.20	Physical Location of System Equipment.....	3-78
3.2.21	Communications.....	3-78
3.2.22	Failure Modes and Effects Analysis .....	3-96
3.2.23	Common Cause Failure (CCF).....	3-98
3.2.24	Compliance to Applicable IEEE Std 603-1991 and IEEE Std 7-4.3.2-2003 Clauses .....	3-98
3.3	PPS - NEW SYSTEM FUNCTIONS (D.2.3 AND D.2.3.1).....	3-104
3.3.1	IEEE Std 603-1991 Clause 4 Compliance.....	3-116
3.3.2	IEEE Std 603-1991 Applicable Clauses for New System Functions .....	3-119
3.3.3	System Requirements Documentation (D.2.3.3 and D.2.3.3.1) .....	3-126
3.4	PPS - FUNCTION ALLOCATION (D.2.4 AND D.2.4.1) .....	3-131
3.4.1	PPS Response Times .....	3-131
3.5	PPS -SYSTEM INTERFACES (D.2.5) .....	3-138
3.5.1	Transmitter Consolidation .....	3-138
3.5.2	Cross Division Communication .....	3-145
3.5.3	Shared Sensor Interface.....	3-146
3.5.4	Sequence of Events.....	3-147
3.5.5	MTP DCS Interface (AOI) .....	3-149
3.5.6	PPS Interface for Reactor Scram.....	3-149
3.5.7	CIM Y-Port for DCS Control of Safety Related Components.....	3-152
3.5.8	CIM Z-Port DPS/RRCS Interface for Diverse Component Actuation .....	3-153
3.5.9	CIM Interface to Actuating Components.....	3-154
3.5.10	RRCS Direct Control of Safety-Related Components .....	3-158
3.5.11	MTP IRIG-B Communication Interface.....	3-158
3.5.12	Support and Auxiliary System Interfaces.....	3-159
3.5.13	Safety to Non-Safety Isolation Requirements .....	3-160
3.5.14	IEEE Std 603 and IEEE Std 7-4.3.2 Relevant Clauses.....	3-160
3.6	PPS - FUNDAMENTAL DESIGN PRINCIPLES IN THE NEW ARCHITECTURE (D.2.6).....	3-165
3.6.1	Redundancy (D.2.6.2.1).....	3-165
3.6.2	Independence (D.2.6.2.2) .....	3-168
3.6.3	Deterministic Behavior (D.2.6.2.3) .....	3-171
3.6.4	Defense-in-Depth and Diversity (D.2.6.2.4) .....	3-175
3.6.5	Simplicity of Design (D.2.6.2.5) .....	3-175
4	PPS - HARDWARE EQUIPMENT QUALIFICATION (D.3).....	4-1
5	PPS - I&C SYSTEM DEVELOPMENT PROCESSES (D.4).....	5-1
5.1	COMMON Q SPM PLANT SPECIFIC ACTION ITEMS.....	5-2
5.1.1	PSAI 1 .....	5-2
5.1.2	PSAI 2 .....	5-3
5.1.3	PSAI 3 .....	5-4
5.1.4	PSAI 4 .....	5-5
5.1.5	PSAI 5 .....	5-5



	5.1.6	PSAI 6 .....	5-7
	5.1.7	PSAI 7 .....	5-7
5.2		SYSTEM AND SOFTWARE DEVELOPMENT ACTIVITIES (D.4.2.1).....	5-8
	5.2.1	Plant and Instrumentation and Control System Safety Analysis (D.4.2.1.1)...	5-8
	5.2.2	Instrumentation and Control System Requirements (D.4.2.1.2) .....	5-8
	5.2.3	Instrumentation and Control System Architecture (D.4.2.1.3).....	5-9
	5.2.4	Instrumentation and Control System Design (D.4.2.1.4) .....	5-9
	5.2.5	Software Requirements (D.4.2.1.5).....	5-9
	5.2.6	Software Design (D.4.2.1.6).....	5-10
	5.2.7	Software Implementation (D.4.2.1.7).....	5-11
	5.2.8	Software Integration (D.4.2.1.8).....	5-11
	5.2.9	Instrumentation and Control System Testing (D.4.2.1.9).....	5-12
	5.2.10	Project Management Processes (D.4.2.2).....	5-12
	5.2.11	Software Quality Assurance Processes (D.4.2.3) .....	5-13
	5.2.12	Software Verification and Validation Processes (D.4.2.4).....	5-13
	5.2.13	Configuration Management Processes (D.4.2.5).....	5-13
6		PPS - APPLYING A REFERENCED TOPICAL REPORT SAFETY EVALUATION (D.5) .....	6-1
	6.1	COMMON Q PLATFORM CHANGES (D.5.1.1).....	6-1
	6.1.1	Common Q Platform Topical Report Revision .....	6-1
	6.2	RESOLUTION OF TOPICAL REPORT PLANT-SPECIFIC ACTION ITEMS (D.5.1.2)	
		.....	6-1
	6.2.1	Generic Open Items.....	6-2
	6.2.2	Plant-Specific Action Items .....	6-3
7		PPS - COMPLIANCE/CONFORMANCE MATRIX FOR IEEE STANDARDS 603-1991 AND	
		7-4.3.2-2003 (D.6) .....	7-1
8		PPS - SECURE DEVELOPMENT AND OPERATIONAL ENVIRONMENT (D.8) .....	8-1
	8.1	SECURE DEVELOPMENT ENVIRONMENT .....	8-1
	8.2	SECURE OPERATIONAL ENVIRONMENT.....	8-1
	8.2.1	Secure Operational Environment Vulnerability Assessment .....	8-2
9		DISTRIBUTED CONTROL SYSTEM.....	9-1
	9.1	RRCS NEW SAFETY CLASSIFICATION .....	9-1
	9.2	DCS ARCHITECTURE .....	9-1
	9.3	RRCS/DPS SEPARATION AND DIVERSITY .....	9-4
	9.3.1	Separation.....	9-4
	9.3.2	Diversity .....	9-4
	9.4	DCS SOFTWARE QUALITY ASSURANCE.....	9-5
	9.5	DCS RELIABILITY .....	9-7
	9.6	RRCS FUNCTIONS.....	9-7
	9.7	DPS FUNCTIONS.....	9-8
	9.8	AUTOMATED OPERATOR AIDS .....	9-9
	9.9	HUMAN SYSTEM INTERFACE .....	9-11
10		REFERENCES .....	10-1



APPENDIX A ELIMINATION OF SPECIFIC PPS TECHNICAL SPECIFICATION SURVEILLANCE  
REQUIREMENTS..... A-1

APPENDIX B ENDNOTES ..... B-1

\*\*\* This record was final approved on 7/13/2022, 1:56:11 PM. (This statement was added by the PRIME system upon its validation)



**LIST OF TABLES**

Table 3.2.5-1 DI&C-ISG-04, Section 2 Compliance .....	3-63
Table 3.2.21-1 DI&C-ISG-04 Compliance .....	3-81
Table 3.3-2 ISG-06 System Requirements Document Content.....	3-127
Table 5.1.2-1 BTP 7-14 Documents.....	5-3
Table 7-1 Compliance/Conformance Matrix for IEEE Std 603 and IEEE Std 7-4.3.2 .....	7-1
Table 8.2.1.5-1 Summary of Vulnerabilities, Controls, and Overall Effectiveness .....	8-6



## LIST OF FIGURES

Figure 2.1-1 RPS Scram Functions.....	2-3
Figure 2.2-1 Reactor Vessel Water Level Range Definition .....	2-13
Figure 3-1 LGS Digital Modernization I&C Architecture .....	3-2
Figure 3.1-1 Typical System Trip Unit and Actuating Relay .....	3-4
Figure 3.1.1-1 RPS Block Diagram .....	3-7
Figure 3.1.1-2 RPS Trip Logic A Scram Outputs .....	3-8
Figure 3.1.1-3 Scram Contactors and Scram Contactor Logics.....	3-9
Figure 3.1.2-1 PCRVICS (NSSSS) Block Diagram.....	3-14
Figure 3.1.3-1 ECCS activations (CS=Core Spray).....	3-25
Figure 3.1.3-2 ECCS Divisional Arrangement (CS=Core Spray).....	3-26
Figure 3.1.3.2-1 System Level Automatic Initiation Logic – ADS, Core Spray (CS in figure), RHR ....	3-32
Figure 3.2-1 PPS 3-Level Architecture .....	3-48
Figure 3.2-2 PPS Architecture .....	3-51
Figure 3.2.2-1 LCL CI631 Configuration .....	3-53
Figure 3.2.3-1 Reactor Scram Matrix .....	3-56
Figure 3.2.9-1 LGS Plant Power Configuration .....	3-73
Figure 3.2.9-2 PPS Cabinet Power Arrangement.....	3-74
Figure 3.2.9-3 MCR Safety Display Power Configuration.....	3-75
Figure 3.2.22-1 PPS BPL Channel (Typical) .....	3-97
Figure 3.4-1 RPS Trip Functions $\leq 50$ ms Response Time .....	3-133
Figure 3.4-2 RPS Trip Functions Reactor Vessel Pressure and Reactor Vessel Water Level.....	3-135
Figure 3.4-3 RPS Trip Functions with $> 124$ ms Response Time .....	3-137
Figure 3.5.1.1-1 LCL Segmentation for Reactor Trip (One Division).....	3-142
Figure 3.5.1.1-2 LCL Segmentation for ECCS and NSSSS Actuation (One Division).....	3-143
Figure 3.5.1.1-3 ILP Configuration (One Division).....	3-144
Figure 3.5.3-1 Typical configuration for Shared Sensor Data .....	3-147
Figure 3.5.4-1 PPS Interface for SOE data .....	3-148
Figure 3.5.5-1 AOI Interface.....	3-149
Figure 3.5.6-1 HARP Interfaces for Reactor Scram .....	3-151



Figure 3.5.7-1 CIM Y-Port Configuration.....	3-153
Figure 3.5.8-1 Z-Port Interface .....	3-154
Figure 3.5.9.1-1 Typical HARP Interface to AC Powered MOV.....	3-156
Figure 3.5.9.1-2 Typical HARP Interface to DC Powered MOV .....	3-157
Figure 3.5.10-1 RRCS Safety-Related Component Interface .....	3-158
Figure 3.5.11-1 MTP IRIG-B Interface.....	3-159
Figure 9.2-1 DCS Architecture .....	9-3
Figure 9.4-1 Software Design Process for DCS .....	9-6
Figure A.4-1 RPS TU feedback Signals.....	A-6
Figure A.6.2-1 RPS Scram Matrix WWDT Configuration.....	A-20
Figure A.6.3.1-1 PPS RPS Signal Path .....	A-24
Figure A.6.3.1-2 ECCS/NSSSS Signal Path .....	A-25



## ACRONYMS AND TRADEMARKS

The following abbreviations and acronyms are defined to allow an understanding of their use within this document.

Acronym	Definition
2oo4	2 out of 4 coincidence. The same format is used for other coincidences: 2oo3, 2oo2, 1oo2, etc.
AI	Analog Input
AC	Alternating Current
AC160	Advant Controller 160
A/D	Analog to Digital [conversion]
AER	Auxiliary Equipment Room
ADS	Automatic Depressurization System
AF100	Advant Fieldbus 100 (data bus within a PPS channel/division)
ALS	Advanced Logic System
AO	Analog Output
AOI	Advant to Ovation Interface. It is the MTP fiber optically isolated unidirectional data link to the non-safety DCS.
AOO(s)	Anticipated Operating Occurrence(s)
AOV	Air Operating Valve
ARI	Alternate Rod Insertion
APRM	Average Power Range Neutron Monitor
AR	Alternate Review [process] (new process described in DI&C-ISG-06, Revision 2)
ATWS	Anticipated Transient Without Scram



Acronym	Definition
BIST	Built In Self Tests
BPL	Bistable Processing Logic
BLC	Bistable Logic Cabinet
BTP	Branch Technical Position
CCF	Common Cause Failure
CIM	Component Interface Module
CLC	Coincidence Logic Cabinet
CMRR	Configuration Management Release Report
COLR	Core Operating Limits Report
CONTRM	AC160 control module (i.e., periodic executable application in the PM646A)
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CRD	Control Rod Drive
CS	Communication Section (see PS)
CST	Condensate Storage Tank
DCS	Distributed Control System
DEHC	Digital Electro-Hydraulic Control System
DFWLCS	Digital Feedwater Level Control System
DI(s)	Digital Input(s)
DMP	Digital Modernization Project
DO	Digital Output



Acronym	Definition
EC	Engineering Change
ECCS	Emergency Core Cooling System
EOC	End Of Cycle
EOP	Emergency Operating Procedure
EQSR	Equipment Qualification Summary Report
ESFAS	Engineered Safety Features Actuation System
FAT	Factory Acceptance Test
FPD	Flat Panel Display
FPDS	[Common Q] Flat Panel Display System
FE	Function Enable [key switch]
FMEA	Failure Modes and Effects Analysis
FPGA	Field Programmable Gate Array
FWRB	Feedwater Runback
GDC	General Design Criteria
GOI(s)	Generic Open Item(s)
GUI	Graphical User Interface
H <sub>2</sub> /O <sub>2</sub>	Hydrogen/Oxygen
HARP	High Amperage Relay Panel
HCU	Hydraulic Control Unit
HFE	Human Factors Engineering
HPCI	High Pressure Coolant Injection



Acronym	Definition
HSI	Human System Interface
HSL(s)	High Speed Link(s)
HVAC	Heating, Ventilation, and Air Conditioning
I/O	Input/Output
ICC	Inadequate Core Cooling
IEEE	Institute of Electrical and Electronics Engineers
ICP	AP1000 PMS Integrated Communications Processor
ILC	Integrated Logic Cabinet
ILP	Integrated Logic Processor
INL	Idaho National Laboratory
ISG	[NRC] Interim Staff Guidance
ITC	Interface and Test Cabinet
ITP	Interface and Test Processor
IRM	Intermediate Range [Neutron] Monitoring
KV	Kilovolt
LAR	License Amendment Request
LCC	Local Coincidence Logic Cabinet
LCL	Local Coincidence Logic
LCO	Limiting Condition for Operation
LGS	Limerick Generating Station
LOCA	Loss of Coolant Accident



Acronym	Definition
LOOP	Loss Of Offsite Power
LPCI	Low Pressure Coolant Injection
LTR	Licensing Technical Report
MAT	Modification Acceptance Testing
MCB	Main Control Board
MCC	Motor Control Center
MCR	Main Control Room
MOV	Motor Operated Valve
MPB	Manual Partial Bypass
MPT	Manual Partial Trip
MSFIS	Main Steam and Feedwater Isolation System
MSIV	Main Steam Line Isolation Valve
MTBF	Mean Time Between Failure
MTC	Maintenance and Test Cabinet
MTP	Maintenance and Test Panel
N <sub>2</sub>	Nitrogen
NI	Nuclear instrumentation
NMS	Neutron Monitoring System
NRC	Nuclear Regulatory Commission
NRR	NRC Office of Nuclear Reactor Regulation
NSSS	Nuclear Steam Supply System



Acronym	Definition
NSSSS	Nuclear Steam Supply Shutoff System
OEM	Original Equipment Manufacturer
PA	Postulated Accident
PCIG	Primary Containment Instrument Gas
PCRVICES	Primary Containment and Reactor Vessel Isolation Control System
PGCC	Power Generation Control Complex
P&ID	Piping and Instrumentation Diagram
PLC	Programmable Logic Controller
PMS	AP1000 Protection and Safety Monitoring System (Note: this should not be confused with the LGS Plant Monitoring System which is not used in this document)
PMT	Post Maintenance Test
PPS	Plant Protection System
PS	Processing Section (within the PM646A)
PSAI	Plant Specific Action Item
RBD	Reliability Block Diagram
RCIC	Reactor Core Isolation Cooling
RCPB	Reactor Coolant Pressure Boundary
RE	Responsible Engineer
RECW	Reactor Enclosure Cooling Water
REECE	Reactor Enclosure Equipment Compartment Exhaust
REIS	Reactor Enclosure Isolation System
RG	US NRC Regulatory Guide



<b>Acronym</b>	<b>Definition</b>
RHR	Residual Heat Removal
RMCS	Reactor Manual Control System
RNI	Ovation Remote Node Interface
RPS	Reactor Protection System
RPT	Recirculation Pump Trip
RPV	Reactor Pressure Vessel
RRCS	Redundant Reactivity Control System
RSE	Reusable Software Element
RSED	Reusable Software Element Document
RTD	Resistor Temperature Detector
RTM	Requirements Traceability Matrix
RTP	Rated Thermal Power
RTS	Return To Service
RTT	Response Time Test
RWCU	Reactor Water Cleanup
SAG	Severe Accident Guidelines
SAT	Site Acceptance Testing
SBO	Station Blackout
SDD	Software Design Description
SD	Safety Display
SDV	Scram Discharge Volume



Acronym	Definition
SER	Safety Evaluation Report
SGTS	Standby Gas Treatment System
SHA	Software Hazards Analysis
SLCS	Standby Liquid Control System
SLE	Software Load Enable [key switch]
SM	System Manager
SOE	Sequence of Events
SOV	Solenoid Operating Valve
SPM	Software Program Manual
SQAP	Software (System) Quality Assurance Program
SR	Surveillance Requirement(s)
SRM	Source Range Monitor
SRNC	Safety Remote Node Controller
SRS	Software Requirements Specification
SRV	Safety Relief Valve
SSC	Structure, System or Component
SSPV	Scram Solenoid Pilot Valve
SWIL	Software in Loop
TCV	Main Turbine Control Valve
TIP	Traversing Incore Probe(s)
TRS	Transient Recording Analysis



Acronym	Definition
TS	Technical Specification(s)
Tsat	Saturation temperature
TSV	Main Turbine Stop Valve
TU	Termination Unit
UDP/IP	User Datagram Protocol/Internet Protocol
UFSAR	Updated Final Safety Analysis Report
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
V&V	Verification and Validation
Vac	Volts alternating current
Vdc	Volts direct current
WDT	Watchdog timer
WWDT	Window watchdog timer



# 1 INTRODUCTION

The logic portions of the Reactor Protection System (RPS), Emergency Core Cooling Systems (ECCS), Primary Containment and Reactor Vessel Isolation and Control System (PCRVICS), Reactor Core Isolation Cooling (RCIC) System, and the manual control of the Standby Liquid Control System (SLCS) at Limerick Generating Station Units 1&2 (LGS) are being replaced with a new system based on the Common Qualified (Common Q<sup>TM</sup>) Platform. The new integrated digital system is called the Plant Protection System (PPS). In addition, because RRCS is being replaced by a non-safety system, the automatic control of the Standby Liquid Control (SLC) System logic is incorporated into the new non-safety related RRCS. Both RCIC and manual initiation of SLC are considered Safe Shutdown Systems in UFSAR Chapter 7.4.

This report supports the LGS License Amendment Request (LAR) to be reviewed and approved by the United States Nuclear Regulatory Commission staff (NRC). This licensing technical report (LTR) follows aspects of the structure in revision 2 of DI&C-ISG-06, “Digital Instrumentation and Controls Licensing Process Interim Staff Guidance” (Reference 1). The aspects followed are those that pertain to the alternate review (AR) process as described in Section C.2 of DI&C-ISG-06 (Reference 1).

LGS can use the information in this LTR to complete sections of the LAR that pertain to DI&C-ISG-06 Sections D.1 through D.8. Each section heading includes the corresponding DI&C-ISG-06 Section in parentheses (e.g., “Plant System Description (D.1)”).

The scope of the PPS modification includes replacing the RRCS that performs the functions to meet the Anticipated Transient Without Scram (ATWS) rule 10 CFR 50.62. RRCS is currently classified as safety-related. The LTR describes the RRCS, its replacement with the Ovation programmable logic controller (PLC) platform, and the change in RRCS classification to non-safety-related to be consistent with the system classification requirements of 10 CFR 50.62. Any additional diverse actuation functions that are needed as a result of the D3 Common Cause Failure (CCF) Coping analysis is implemented in the new Ovation-based RRCS. When the LTR is referring to the PPS modification, it includes these changes to RRCS.

Table 1-1 maps the DI&C-ISG-06 Enclosure B for the AR process to the contents of this LTR.

**Table 1-1 Mapping of DI&C-ISG-06 Enclosure B to LTR Contents**

DI&C-ISG-06 Enclosure B (AR)	LTR Section
1.1 (Summary of) Application Software Planning and Processes	Section 5
1.2 (Summary of) Vendor Oversight Plan	Not included. The VOP Summary is provided as a separate attachment to the License Amendment Request..
1.3 Approved Topical Report Safety Evaluation	Section 6



DI&C-ISG-06 Enclosure B (AR)	LTR Section
1.4 System Description	Section 2
1.5 System Architecture	Section 3
1.6 (Summary of) Hardware Equipment Qualification	Section 4
1.7 (Unified Compliance/Conformance Matrix for) IEEE Std 603-1991 and 7-4.3.2-2003	Section 7
1.8 (Changes to) Technical Specifications	Not included. Technical Specification Changes is part of the LAR. LTR Appendix A provides the safety case for eliminating certain PPS surveillance requirements in accordance with WCAP-18461-P-A (Reference 54).
1.9 Setpoint Methodology and Calculations	N/A – setpoint methodology and calculations are not changing.
1.10 Secure Development and Operational Environment	Section 8



## 2 PLANT SYSTEM DESCRIPTION (D.1)

The LGS analog-based reactor protection system, specific engineered safety features, and isolation systems, are being replaced with a new Plant Protection System (PPS) using the Common Qualified (Common Q™) Platform. The following existing individual systems will be replaced by a single Plant Protection System (PPS):

- Reactor trip system (RPS)
- Emergency Core Cooling System (ECCS)
- Primary Containment and Reactor Vessel Isolation and Control System (PCRVICES)
- Reactor Core Isolation Cooling System (RCIC)
- Standby Liquid Control System
- US Regulatory Guide (RG) 1.97 safety-related indications.

The existing equipment and system architecture are described in Section 3.1, “Existing Architecture”.

In addition, the RRCS will be replaced by the Westinghouse Ovation PLC platform that will replicate the current ATWS functions it performs. In addition, if any new diverse actuation functions are required as a result of the D3 CCF coping analysis, these additional actuation functions would be performed by the upgraded RRCS.

### 2.1 REACTOR PROTECTION SYSTEM

The RPS is classified as Safety Class 2, seismic Category I, Quality Group B, and electric Class 1E.

- The RPS initiates a rapid, automatic shutdown (scram) of the reactor. This action is taken in time to prevent excessive fuel cladding temperatures and any nuclear system process barrier damage following abnormal operational transients. The RPS overrides all operator actions and process controls.<sup>1</sup>

The RPS provides its function by monitoring certain plant parameters and, if one or more parameters exceed a specified limit, the RPS system functions to automatically insert control rods to terminate power production in the core. Control rod movement is performed by the Control Rod Drive (CRD) system. When power is removed from the Scram Solenoid Pilot Valves (SSPVs) the de-energized valves exhaust air causing the control rods to insert. The automatic scram function of RPS is accomplished by monitoring the following plant parameters<sup>2</sup>:

- Scram Discharge Volume (SDV) Water Level
- Main Steam Line Isolation Valve (MSIV) position
- Main Turbine Stop Valve (TSV) Position
- Main Turbine Control Valve (TCV) Fast Closure
- Reactor Vessel Water Level
- Average Power Range Monitor
- Intermediate Range Monitors
- Drywell Pressure
- Reactor Vessel Pressure



In addition to generating automatic reactor scram signals in response to the conditions described above, the RPS provides the capability to manually scram the reactor through the use of Manual Scram Pushbutton switches or by placing the Reactor Mode Switch in the “Shutdown” position.

The RPS consists of two trip systems (A and B) each containing two channels of sensors and logic, for a total of four logic channels. The monitored parameters each have at least one input to each of the logic channels. The overall RPS logic requires that at least one channel in each trip system must be tripped in order to cause a scram.

The RPS is a normally energized system. De-energizing any channel or the relay trip system in an electrical division places the trip system in that electrical division in a tripped condition (i.e., half-scram). This makes the RPS fail safe on loss of electrical power. For this reason, each electrical division is powered by two independent power sources so that failure of one power source does not cause a half-scram.

In addition to the various sensors, relays, and switches, the RPS includes the RPS inverter power sources which provide the RPS with the ability to remain energized (prevent spurious trips) during short power loss transients, and the RPS bus protective devices which ensure that when power is available it is within the requirements of the bus loads.

The Design Basis functions are changing only with respect to coincidence trip logic. The current coincidence logic is described in Section 3.1.1 and the new coincidence logic is described in Section 3.2. All the design basis events in Chapter 15 and the reliance on the RPS trips are unchanged. The methodologies and algorithms used in RPS trip processor calculations remain unchanged.<sup>3</sup>

Figure 2.1-1 depicts the scram functions of the RPS.<sup>4</sup>



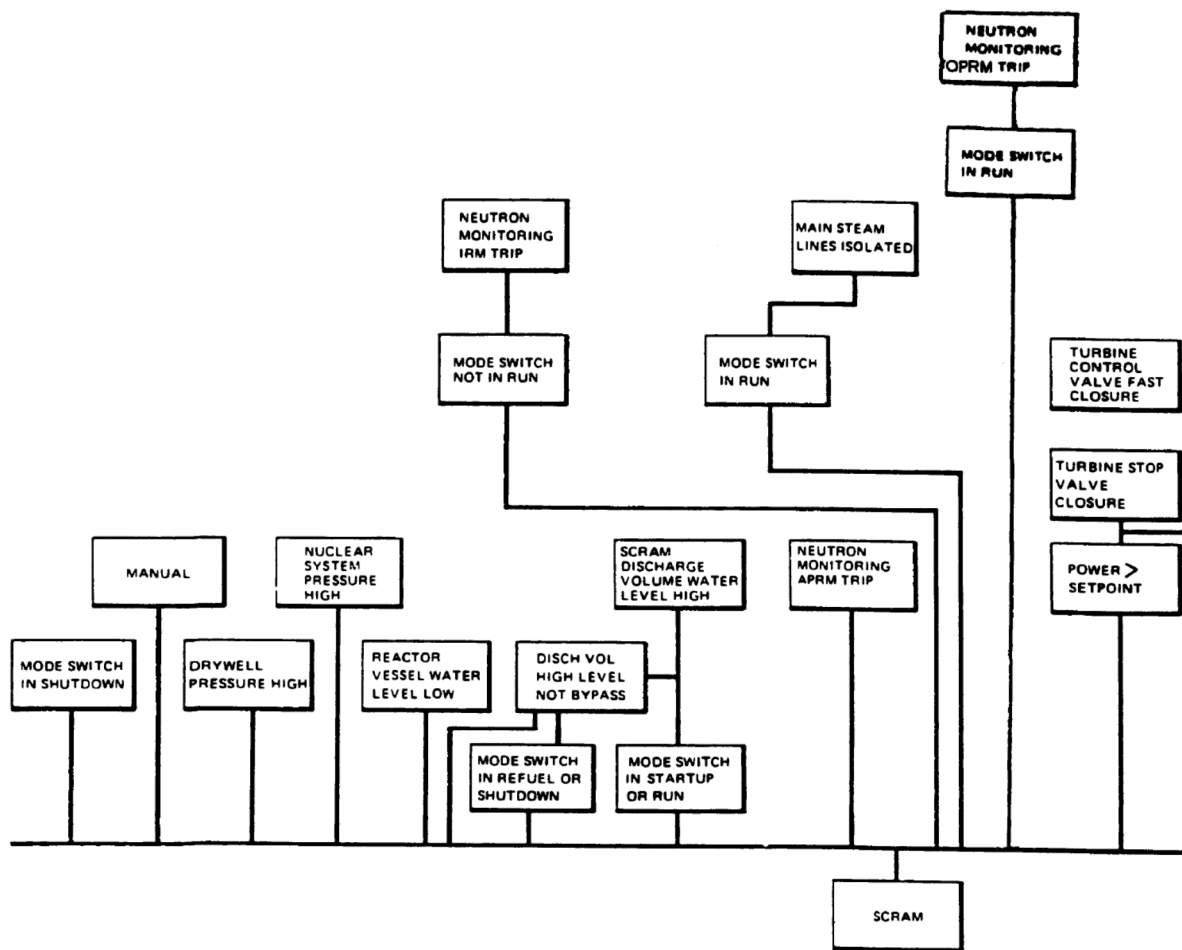


Figure 2.1-1 RPS Scram Functions

## 2.2 PRIMARY CONTAINMENT AND REACTOR VESSEL ISOLATION CONTROL SYSTEM

The purpose of the PCRVICES is to isolate the reactor pressure vessel, primary and secondary containments during accident conditions in order to limit the loss of reactor coolant and to prevent the release of radioactive materials to the environment in excess of 10 CFR 100 limits. The functional classification of the PCRVICES is that of a safety related system. Its regulatory classification is that of an engineered safety feature (ESF) system.<sup>5</sup>

The PCRVICES initiates closure of various automatic isolation valves if monitored system variables exceed pre-established limits. This action limits the loss of coolant from the Reactor Coolant Pressure Boundary (RCPB) and the release of radioactive materials from the RCPB, the primary containment, and



the reactor enclosure. The functional requirements associated with the PCRVICES and its interfacing systems necessitate the following:

1. Pipes or vents that penetrate primary containment and communicate directly with the reactor vessel have two isolation valves: one inside primary containment (i.e., inboard) and one outside primary containment (i.e., outboard).
2. Pipes or vents that connect directly to the containment atmosphere and penetrate primary containment have two valves outside containment (i.e., inboard closest to containment and outboard further away from containment).

The PCRVICES consists of seven functions implemented using eight logical isolation groups. These functions and groups are largely divided by the interfacing systems which are isolated by actuation of the PCRVICES (e.g., Group IA provides main steam isolation, Group IIA provides isolation of the RHR system, etc.). Table 2.2-1 provides PCRVICES Groups.<sup>6</sup>

**Table 2.2-1 PCRVICES Groups**

Group	Isolated Equipment	Conditions for Isolation	Logic	Bypass
IA	MSIVs		1oo2 Take Twice	
	Main Steam Line Drains	a. Reactor Level 1 – Low, Low, Low	2oo2	No
		b. Main Steam Line – Low Pressure	2oo2	Only applies when the Reactor Mode Switch is not in Run
		c. Main Steam Line – High Flow	2oo2	No
		d. Condenser Vacuum – Low	2oo2	Only applies when the Reactor Mode Switch is not in Run
		e. Outboard MSIV Room Temperature High	2oo2	No



Group	Isolated Equipment	Conditions for Isolation	Logic	Bypass
		f. Turbine Enclosure – Main Steam Tunnel – High Temperature	2oo2	No
		g. Manual Initiation	1oo1	No
IB	Main Steam and Reactor Sample	a. Reactor Level 2 – Low, Low b. Manual Initiation	a. 2oo2 b. 1oo1	No
IIA	RHR Shutdown Cooling	a. Reactor Level 3 – Low b. Reactor Pressure – High (RHR Valve Permissive) c. Manual Initiation	a. 2oo2 b. 1oo2 c. 1oo1	No
IIB	RHR Htx Sample and Drn to R/W	a. Reactor Level 3 – Low b. Drywell Pressure – High	a. 2oo2 b. 2oo2	No No
III	Reactor Water Cleanup	c. RWCU – Differential Flow High d. RWCU – Area Temperature e. RWCU – Area Delta Temperature High f. SLCS Initiation (Initiated by RRCS, see Section 9.6) g. Reactor Level 2 – Low, Low	b. 1oo1 c. 1oo1 d. 1oo1 e. 1oo2 (Inboard Valve, 1oo1 Outboard Valve) f. 2oo2	High is bypassed 45 seconds once setpoint is exceeded. No No No No



Group	Isolated Equipment	Conditions for Isolation	Logic	Bypass
		h. Manual Initiation	g. 1001	No
IVA	High Pressure Coolant Injection Process	a. HPCI – Reactor Steam Flow - High  b. HPCI – Steam Supply Pressure - Low c. HPCI – Turbine Exhaust Diaphragm Pressure – High d. HPCI – Room Temperature – High e. HPCI – Pump Room Delta Temperature – High f. Manual Initiation (Division 2 only. Requires HPCI initiation condition to be present)	a. 1001  b. 2002  c. 2002  d. 1001  e. 1001  f. 1001	Bypassed 3 seconds once setpoint is exceeded.  No  No  No  No  No



Group	Isolated Equipment	Conditions for Isolation	Logic	Bypass
IVB	HPCI Vacuum Breaker	a. Drywell Pressure – High  AND  b. HPCI – Steam Supply Pressure – Low	a. 2oo2   b. 2oo2	No
VA	Reactor Core Isolation Cooling Process	a. RCIC – Steam Flow - High  b. RCIC – Steam Supply Pressure – Low c. RCIC – Exhaust Diaphragm Pressure – High d. RCIC – Room Temperature – High e. RCIC – Pump Delta Temperature – High f. Manual Initiation (Division 1 only. Requires RCIC initiation signal not reset)	a. 1oo2  a. 2oo2 b. 2oo2 c. 1oo1 d. 1oo1 e. 1oo1	Bypassed 3 seconds after setpoint is exceeded  No No No
VB	RCIC Vacuum Breaker	a. Drywell Pressure – High  AND  b. RCIC – Steam Supply Pressure – Low	a. 2oo2   b. 2oo2	No
VIA	Primary Containment Purge Supply and Exhaust	a. Reactor Level 2 – Low, Low b. Drywell Pressure – High c. North Stack Effluent Radiation – High	a. 2oo2 b. 2oo2 c. 1oo1	Yes Yes No



Group	Isolated Equipment	Conditions for Isolation	Logic	Bypass
		d. Reactor Enclosure Ventilation Exhaust Duct Radiation – High e. Refueling Area Ventilation Duct Radiation - High f. Outside Atmosphere to Refueling Area Differential Pressure – Low g. Outside Atmosphere to Reactor Enclosure Differential Pressure – Low h. Refuel Floor/SGTS Connecting Valves - Failed Open i. Reactor Enclosure/SGTS Connecting Valves – Failed Open j. Manual Initiation	d. 2oo2 e. 2oo2 f. 1oo1 g. 1oo1 h. 1oo1 i. 1oo1 j. 1oo3	Yes Yes Yes Yes Yes Yes Yes
VIB	Primary Containment Exhaust to Reactor Enclosure Equipment Compartment Exhaust (REECE) and Nitrogen (N <sub>2</sub> ) Block Valves	a. Reactor Level 2 – Low, Low b. Drywell Pressure – High c. Reactor Enclosure Ventilation Exhaust Radiation - High d. Refueling Area Ventilation Exhaust Duct Radiation – High	a. 2oo2 b. 2oo2 c. 2oo2 d. 2oo2	Yes



Group	Isolated Equipment	Conditions for Isolation	Logic	Bypass
		e. Outside Atmosphere to Refueling Area Differential Pressure – Low f. Outside Atmosphere to Reactor Enclosure Differential Pressure – Low g. Refuel Floor/SGTS Connecting Valves – Failed Open h. Reactor Enclosure/SGTS Connecting Valves – Failed Open i. Manual Initiation	e. 1001 f. 1001 g. 1001 h. 1001 i. 1003	
VIC	Primary Containment Hydrogen/Oxygen (H <sub>2</sub> /O <sub>2</sub> ) Sampling and Recombiner Lines	a. Reactor Level 2 – Low, Low b. Drywell Pressure – High c. Refueling Area Ventilation Exhaust Duct Radiation – High d. Reactor Enclosure Ventilation Duct Radiation – High e. Manual Initiation	a. 1001 b. 1001 c. 1001 d. 1001 e. 1001	Yes (All valves except for Drywell Rad Sample Supply and Return Lines valves)
VIIA	Primary Containment Instrument Gas (PCIG)	a. Reactor Level 1 – Low, Low, Low	a. 2002	Yes (Except for Primary Containment Relief Valve Supply Line)



Group	Isolated Equipment	Conditions for Isolation	Logic	Bypass
		b. Drywell High Pressure  c. Reactor Enclosure Ventilation Exhaust Duct Radiation – High d. Manual Initiation	b. 2002  c. 2002  d. 1002	Yes (Except for Primary Containment Relief Valve Supply Line)  Yes  Yes
VIIB	PCIG Traversing Incore Probes (TIP) Purge Supply	a. Reactor Level 2 – Low, Low b. Drywell Pressure – High  c. Reactor Enclosure Ventilation Exhaust Duct Radiation – High d. Manual Initiation	a. 2002 b. 2002  c. 2002  d. 1002	No
VIIC	PCIG to ADS	a. PCIG to Drywell Differential Pressure – Low	a. 1001	No
VIIIA	Drywell Chilled Water and Reactor Enclosure Cooling Water (RECW)	a. Reactor Level 1 – Low, Low, Low b. Drywell Pressure – High  c. Manual Initiation	a. 2002 b. 2002  c. 1001	Yes
VIIIB	Drywell Sump, Suppression Pool Cleanup, TIPs	a. Reactor Level 2 – Low, Low b. Drywell Pressure – High c. Manual Initiation	a. 2002 b. 2002 c. 1001	No



Group	Isolated Equipment	Conditions for Isolation	Logic	Bypass
	Bypass Barrier Block and Vents	a. Reactor Level 2 – Low, Low  b. Drywell Pressure – High c. Refueling Area Ventilation Exhaust Duct Radiation – High d. Reactor Enclosure Ventilation Exhaust Duct Radiation – High e. Manual Initiation	a. 1001  b. 1001 c. 1001  d. 1001  e. 1001	No (Except for N <sub>2</sub> Supply Vent Valves)
	PCIG Block and Vents	a. Reactor Vessel Water Level – at or below Level 1 (see Figure 2.2-1) b. Drywell Pressure – High c. Reactor Enclosure Ventilation Exhaust Duct – High Radiation d. Manual Initiation	a. 1001  b. 1001 c. 1001  d. 1001	Yes
	Refuel Floor Heating, Ventilation, and Air Conditioning (HVAC)	a. Refueling Area Ventilation Exhaust Duct Radiation - High b. Outside Atmosphere to Refueling Area Differential Pressure – Low c. Refuel Floor/SGTS Connecting Valves – Failed Open d. Manual Initiation	a. 2002  b. 1001  c. 1001  d. 1006	Yes



Group	Isolated Equipment	Conditions for Isolation	Logic	Bypass
	Reactor Enclosure HVAC	a. Reactor Level 2 – Low, Low b. Drywell Pressure – High c. Reactor Enclosure Ventilation Exhaust Duct Radiation – High d. Outside Atmosphere to Reactor Enclosure Differential Pressure – Low e. Reactor Enclosure/SGTS Connecting Valves – Failed Open f. Manual Initiation	a. 2oo2 b. 2oo2 c. 2oo2 d. 1oo1 e. 1oo1 f. 1oo6	Yes

Note: The logic in this table refers to the logic required for isolation in each division, where divisions typically refer to either inboard and outboard divisions. Each channel of steam leak detection monitoring contains inputs from multiple areas.

The replacement PCRVICS safety functions are unchanged.



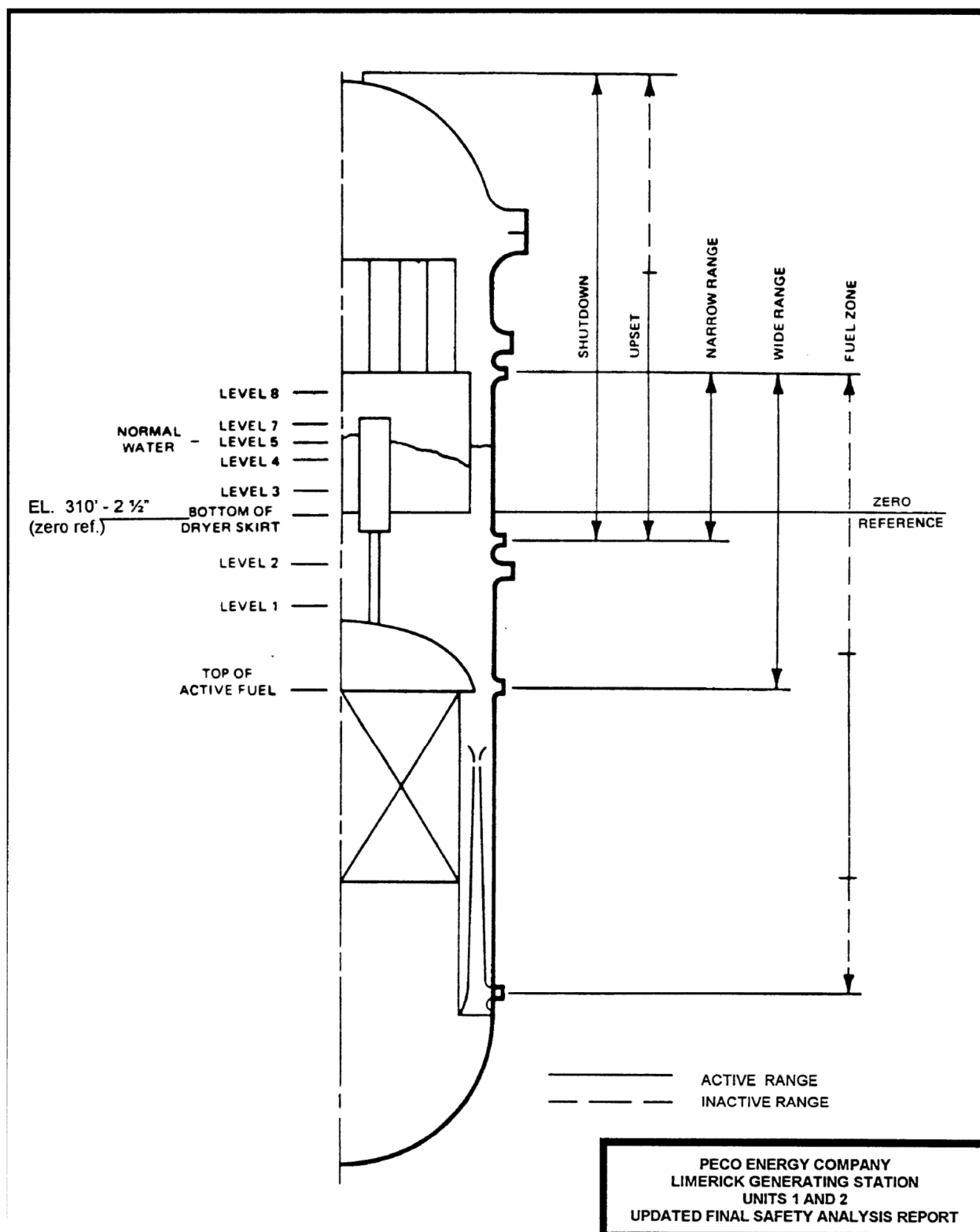


Figure 2.2-1 Reactor Vessel Water Level Range Definition



## 2.3 EMERGENCY CORE COOLING SYSTEM

The ECCS control and instrumentation is designed to meet the following functional safety design bases:

- a. Automatically initiate and control the ECCS to prevent fuel cladding temperatures from reaching 2200 °F.
- b. Respond to a need for emergency core cooling, regardless of the physical location of the malfunction or break that causes the need.
- c. The following safety design bases are specified to limit dependence on operator judgement in times of stress:
  1. The ECCS responds automatically so that no action is required of plant operators within 10 minutes after a LOCA.
  2. The performance of the ECCS is indicated by control room instrumentation.
  3. Facilities for manual control of the ECCS are provided in the control room.<sup>7</sup>

The ECCS instrumentation and controls are classified as Safety Class 2, seismic Category I, Quality Group B, and electric Class 1E.<sup>8</sup>

The ECCS is comprised of independent core cooling systems that ensure the requirements of 10 CFR 50.46, "Acceptance criteria for emergency core cooling systems for light-water nuclear power reactors," are satisfied if a breach in the RCPB results in a loss of reactor coolant. The following systems are included in the ECCS, except where noted:

- High Pressure Coolant Injection (HPCI): The HPCI system provides and maintains an adequate coolant inventory inside the reactor vessel to limit fuel clad temperatures resulting from postulated small breaks in the RCPB. HPCI uses a large steam-driven pump to inject water into one of the main feedwater (FW) lines and one of the Core Spray (CS) headers to the Reactor Pressure Vessel (RPV).
- Automatic Depressurization System (ADS): The ADS acts to rapidly reduce reactor vessel pressure in a Loss of Coolant Accident (LOCA) situation in which the HPCI system fails to maintain reactor vessel water level. Under certain circumstances, HPCI may be unable to provide sufficient inventory to recover from a LOCA. However, if reactor pressure remains high concurrent with the LOCA, then the high capacity, low pressure ECCS pumps cannot inject until pressure has been lowered below their shutoff head pressure. This depressurization function is executed by the simultaneous opening of five Safety/Relief Valves (SRVs) by the ADS, based on conditions that indicate HPCI cannot maintain level sufficiently high while the RPV is still pressurized.
- Core Spray: The Core Spray system cools the fuel by spraying water on the core in the event of a LOCA associated with a wide range of pipe break sizes. This function is executed through the use of two mechanical divisions of two pumps each along with the requisite piping and valves. Electrically, the Core Spray system is divided into four divisions where each pump is powered from one emergency 4 KV bus, which can also be powered by an EDG. Each division of Core Spray system also includes a separate instrumentation and controls (I&C) architecture.
- Residual Heat Removal (RHR): The RHR system provides a number of different operating modes. The Low Pressure Coolant Injection (LPCI) mode is credited as part of the ECCS. LPCI acts to mitigate the consequences of a large break LOCA by injecting to the RPV at low reactor



pressures. The RHR system also has non-ECCS modes that support containment cooling (suppression pool cooling, containment spray), shutdown cooling for decay heat removal, and other support functions (e.g., fuel pool cooling assist, alternate decay heat removal, and suppression pool level control through a radioactive waste system interface). The RHR system executes this function through the use of four divisions, each containing a pump along with the requisite piping, valves, and control systems. Two heat exchangers are also provided to support cooling capabilities.

The diesel generators are designed to start and attain the required voltage and frequency within 10 seconds. The generator, static exciter, and voltage regulator are designed to permit the unit to accept the load and to accelerate the motors in the sequence and time requirements. LGS does not use an emergency load sequencer associated with the offsite and onsite power sources. Sequencing of loads on the Class 1E buses is achieved by individual time-delay relays for each load.<sup>9</sup> The PPS interfaces with and sends the initiating signal to the existing plant equipment that performs the Emergency Diesel Generator Load Sequencing.

## **2.4 REDUNDANT REACTIVITY CONTROL SYSTEM**

The RRCS is currently classified as Safety Class 2, seismic Category I, Quality Group B, and electric Class 1E. However, the License Amendment Request is changing the classification to non-safety related. Section 9.1 provides the safety case for this classification change.

The RRCS is designed to provide a redundant and diverse method of shutting down the reactor, in the unlikely event that the RPS does not scram the reactor as a result of an anticipated operating transient. The RRCS logic is initiated when either the high reactor pressure or low reactor water level setpoints are reached. A signal is then sent to energize the ARI valves that block and vent the CRD scram air header to insert the control rods into the reactor. A signal is also transmitted to the recirculation pump trip (RPT) breakers to trip the reactor recirculation pumps to reduce the reactor power. If reactor power has not decreased to a predetermined level, within a specified period of time, the RRCS logic will initiate a feedwater runback and the injection of a neutron poison solution into the reactor, via the SLCS, and shut down the reactor. See Section 9.6 for the safety case to eliminate the RRCS feedwater runback function.

The RRCS logic monitors reactor dome pressure and water level. The logic will cause the immediate energization of the ARI valves when either the reactor high pressure trip setpoint or low water level 2 setpoint is reached, or the manual push buttons are armed and depressed. Energization of the RRCS ARI valves depressurizes the scram air header independent of the logic and valves actuated by the RPS system. Additional immediate RRCS response to the initiation signals include recirculation system pump motor breaker trip immediately if reactor high pressure is received or 9 seconds after a low water level 2 signal is received. The high pressure initiation signal will initiate a feedwater runback after 25 seconds whether the feed pumps are in automatic or manual if the APRM not downscale trip signal is present. If power is not downscale after a 118 second time delay from the beginning of the ATWS event, the RWCU system will be isolated and the SLCS will be automatically initiated. Ten minutes after the SLCS initiation, the RRCS can be reset, provided that RRCS actuation parameters have reset and the RRCS manual reset push buttons are depressed.<sup>10</sup>



### *RRCS Alternate Rod Insertion*

The RRCS signal to insert the control rods is generated in either of two separate divisions (two-out-of-two logic in a given division) and results in the energization of eight valves. Two of these vent the scram air supply line downstream of the backup scram valves. These RRCS valves also act to block the supply of air to the scram header. Check valves provide an air flow path around the valves that vent the scram air supply in the event one or more of the valves fails. Four additional RRCS valves vent the A and B scram header to the atmosphere. As the header depressurizes, the scram valves at each hydraulic control unit (HCU) will spring open, scrambling the rods. Two RRCS valves vent the scram air header to the SDV drain and vent valves, closing these valves and isolating the SDV. All eight RRCS alternate rod insertion (ARI) valves are normally de-energized. Positive position of the ARI solenoid valves is indicated by voltage and plant air indications.

The ARI signal can be reset after a 30 second time delay, provided that the high reactor pressure, low water level 2, and manual initiation signals no longer exist.<sup>11</sup>

### *RRCS Recirculation System Trips*

The ATWS RPT contributes to the mitigation of the consequences of an ATWS event by tripping the recirculation pumps early in the event, reducing core flow and thereby reducing the core power generation.

Low water level 2 or high reactor pressure RRCS signals cause a trip of the recirculation pump drive motor breakers. There are two separate divisions of instrumentation with divisional power sources, each one with two pressure sensors and two level sensors. A reactor vessel high dome pressure signal from either division will immediately trip both recirculation pump motors. A reactor vessel low water level signal from either division will trip both recirculation pump motors after a 9 second delay. This reduction in core flow protects the vessel and fuel during the ATWS event by limiting core power during the time required for the scram air header to depressurize sufficiently to open the scram valves.

Both sensors in either division (i.e., two level sensors in one division or two pressure sensors in one division) are required to generate a trip signal. The ATWS RPT pump breakers are the same ones used in the end of cycle (EOC) RPT. There are two breakers in series in each pump motor feed; the control logic of each breaker is assigned to a separate safety division.

Manual initiation of RRCS without reactor high pressure or reactor low level 2 does not trip the recirculation pump drive motor breaker; however, after manual initiation of RRCS, the breaker trip will occur if either reactor high pressure or low level 2 occur.

The ATWS RPT trip circuitry is separate from and independent of the EOC RPT trip circuitry. Separate trip coils are used in each breaker (one for ATWS RPT and one for EOC RPT). The trip coils are fed from RPS power supplies.

The trip circuits, including the sensors and the pump breakers, are Class 1E. The entire trip circuits may be tested during plant operation, except for opening of the pump breakers. ATWS RPT circuitry is separated from non-Class 1E circuitry in accordance with the LGS separation criteria.



Indicators and annunciators in the control room provide the status of the trip coils and the mechanical position of the pump circuit breakers. Actuation of the ATWS-RPT is recorded in the control room.<sup>12</sup>

### *RRCS Feedwater Runback*

The feedwater runback function mitigates the consequences of an ATWS event by stopping feedwater flow into the vessel, which reduces the core subcooling, thereby reducing the core power generation.

Reactor high pressure combined with a 25 second time delay and APRM power not downscale will initiate a feedwater runback. Feedwater flow will be reduced to 0% within 15 seconds. The logic to initiate feedwater runback is energized to trip and can be manually overridden 30 seconds after runback initiation. The runback reduces the input of cooler water flowing to the vessel. As average core coolant temperature increases, voids increase, reactivity decreases, and power is reduced.

The RRCS feedwater runback will occur whether the feed pumps are in automatic or in manual mode of control. The normal loss of signal interlock that prohibits changes in feedwater pump output during loss of signal conditions is disabled during ATWS.<sup>13</sup> See Section 9.6 for the safety case to eliminate the RRCS feedwater runback function.

### *Standby Liquid Control System Initiation*

Low water level 2, reactor high pressure, or manual initiation of the RRCS immediately starts a timer. A signal will be sent to initiate the SLCS if, at the expiration of a 118 second time delay, the core power is not downscale as measured by the APRM system. Initiation of the SLCS requires start signals from both channels A and B of either division of RRCS. Receipt of these signals starts the two in-service pumps and causes the associated squibs to fire, opening the explosive valves. Both pumps will inject borated water into the vessel until the storage tank low level sensors, arranged in two-out-of-two logic, trip the pumps.

The SLCS pump control switches can be used to manually stop SLCS pump injection.<sup>14</sup>

## **2.5 REACTOR CORE ISOLATION COOLING SYSTEM**

The Reactor Core Isolation Cooling System is classified as Safety Class 2, seismic Category I, Quality Group B, and electric Class 1E.

The Reactor Core Isolation Cooling (RCIC) system provides makeup water to the reactor vessel whenever the vessel is isolated from the main condenser and feedwater system. RCIC executes its safety function in a manner similar to HPCI through the use of a steam-driven pump that injects into one of the main FW lines associated with the RPV. However, RCIC operates with a much smaller capacity than the HPCI system.<sup>15</sup>

## **2.6 STANDBY LIQUID CONTROL SYSTEM**

The Standby Liquid Control System is classified as Safety Class 2, seismic Category I, Quality Group B, and electric Class 1E.



The SLCS is a backup method of shutting down the reactor to cold subcritical conditions by independent means other than the normal method using the control rods. Thus, the system is considered a "safe shutdown system." The standby liquid control process equipment and controls essential for injection of the neutron absorber solution into the reactor are designed to seismic Category I criteria. In addition, these controls are Class 1E, meeting the quality requirements of 10CFR50.

The SLCS is a special "plant capability" event system. No single active component failure of any plant system or component would necessitate the operational function of the SLCS. It is included for three special cases:

- a. Plant capability to shut down the reactor without control rods from normal operation
- b. Plant capability to shut down the reactor without control rods from a transient incident
- c. Plant capability to maintain suppression pool water inventory at a pH of 7.0 or greater post LOCA in accordance with Regulatory Guide 1.183, Alternative Source Terms.<sup>16</sup>

The SLCS is manually initiated in the control room, when the operator determines that normal reactivity control systems have not shutdown the reactor as required, by turning the key-lock switch to the run position for either one or both of the two in-service pumps. Indicator lights located near each key-lock switch apprise the operator of the selected system initiation.

Two loops of the SLCS can also be automatically initiated by the RRCS after a time delay, provided that APRM power is not downscale and the key-lock switch is in the center normal position. This automatic initiation overrides the manual initiation signal; however, the manual shutoff signal overrides the automatic initiation signals.<sup>17</sup>

When a SLCS pump is started (manually or automatically), both squibs on its explosive-operated valve fire. Firing of either or both of the two squibs installed on each valve will open the valve. The SLCS is manually initiated in the control room by turning the key-locked switch for either one or both of the two in-service pumps to the run position. Only two SLCS pumps are started to prevent lifting the pressure relief valves(s) on high discharge header pressure with three SLCS pump operation. SLCS manual initiation will change to soft control on the PPS using the Safety Displays.<sup>18</sup>

Under special shutdown conditions, the SLCS is functionally redundant to the control rods in achieving and maintaining the reactor subcritical. Therefore, the SLCS as a system by itself is not required to be redundant. The power buses, pumps and explosive-operated injection valves are redundant so that a single component may be removed from service for maintenance during plant operation.<sup>19</sup>

## **2.7 RG 1.97 INDICATIONS**

RG 1.97, Revision 2 is the licensing basis for LGS. LGS UFSAR Sections 7.5.1.4.2 "Post-accident Monitoring" and Section 7.5.1.4.3, "Additional Instrumentation for Regulatory Guide 1.97 Variables" define the safety-related post accident monitoring, RG 1.97 indications that are available to the Main Control Room (MCR) operators.



### 3 SYSTEM ARCHITECTURE (D.2)

Section 3.1 describes the existing system architecture at LGS that will be replaced. Section 3.2 describes the PPS system architecture. Section 9 describes the architecture for the Distributed Control System (DCS) that performs the functions for RRCS, the Diverse Protection System (DPS), and the Automated Operator Aids. The overall I&C architecture for the LGS Digital Modernization Project is depicted in Figure 3-1. The major systems that comprise the Digital Modernization Project are the:

1. Plant Protection System (PPS)
2. Distributed Control System (DCS)

Sections 3 and 9 go into further detail for these systems.

The notation in Figure 3-1 depicting inputs from the PPS into RRCS and DPS, represents shared sensors between the PPS and these two non-safety systems. The configuration is described in Section 3.5.3. The Ovation remote I/O modules are considered RG 1.75 associated circuits within the PPS. The modules go through an equipment qualification program to ensure they cannot adversely affect the PPS safety function.



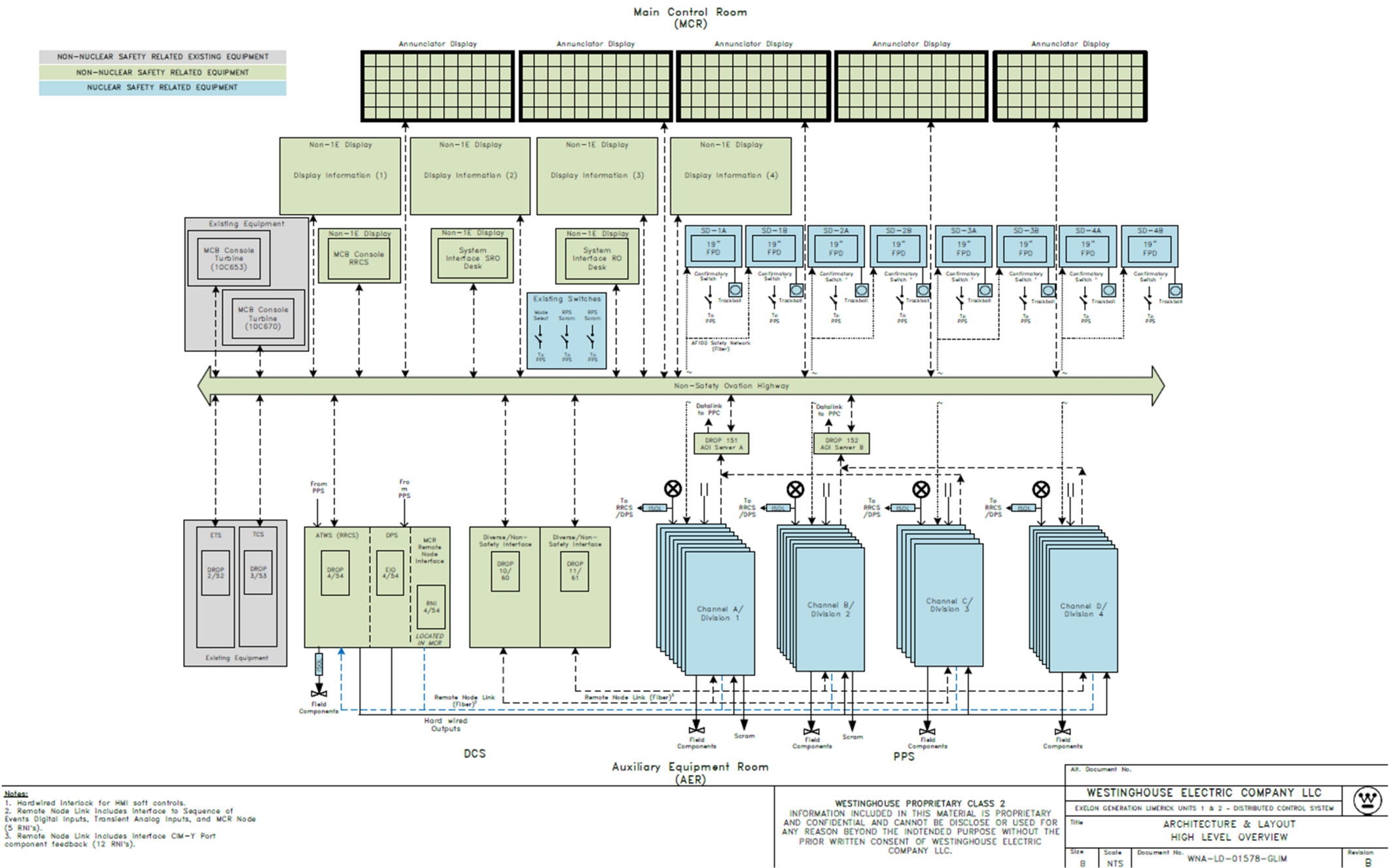


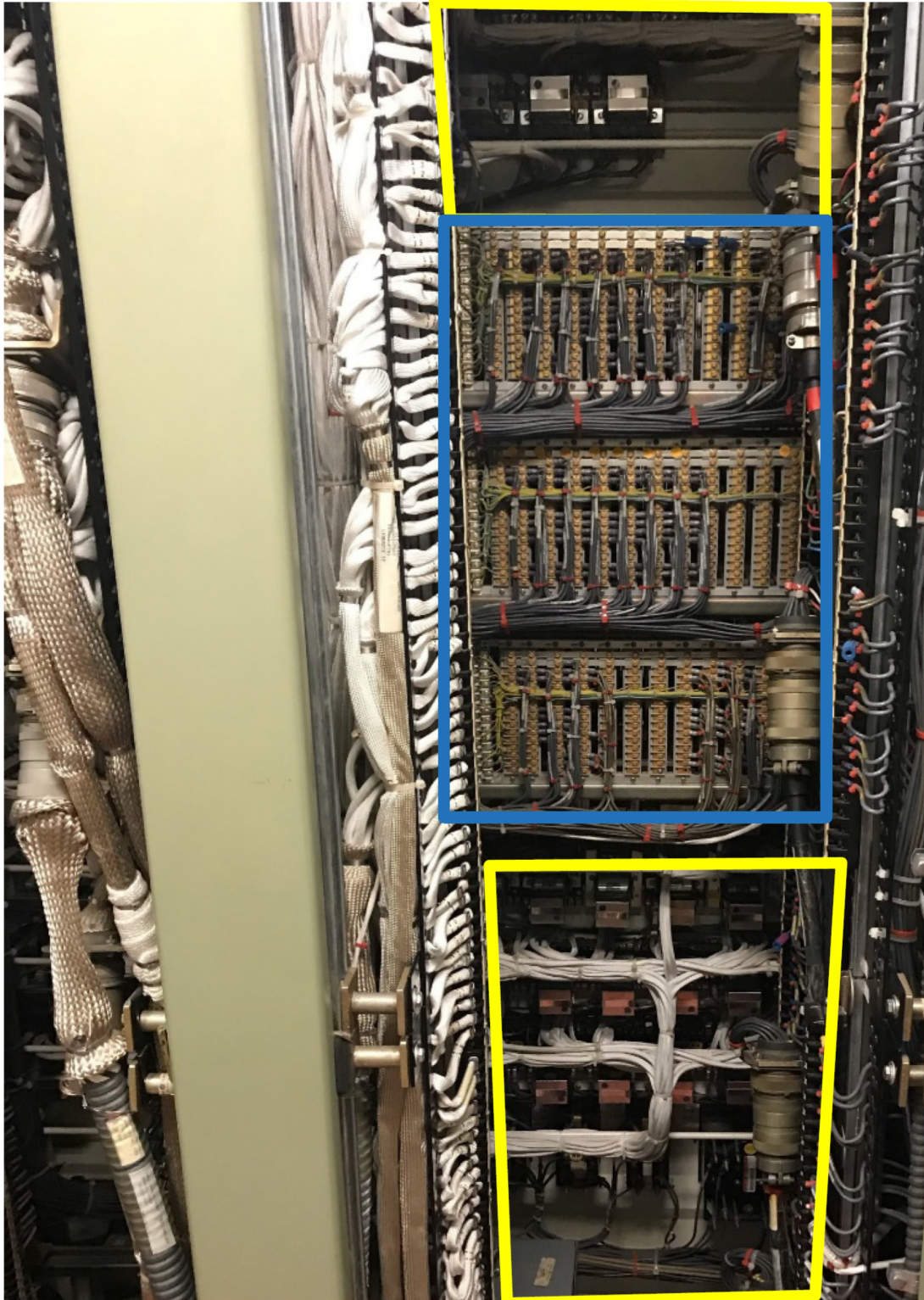
Figure 3-1 LGS Digital Modernization I&C Architecture



### **3.1 EXISTING SYSTEM ARCHITECTURE (D.2.1)**

This section describes the existing architecture of the RPS, PCRVICS, and the ECCS. All of these systems are analog technology that will be upgraded to the digital Common Q Platform. There is some commonality between the three systems. They all have trip units (highlighted in blue in Figure 3.1-1) and actuated relays (highlighted in yellow in Figure 3.1-1).





**Figure 3.1-1 Typical System Trip Unit and Actuating Relay**



### 3.1.1 RPS

The RPS includes sensors, relays, bypass circuitry, and switches that cause rapid insertion of control rods (scram) to shut down the reactor. The RPS also includes outputs to the process computer system and annunciators, which are not part of the RPS.

A completely separate and diverse system, the RRCS, is provided to mitigate the potential consequences of an ATWS event.

Figure 3.1.1-1<sup>20</sup> shows a block diagram of the RPS logic portion. The blocks outlined in red are the components of the RPS that will be replaced with the Common Q platform. Power to each of the two RPS trip systems is supplied by separate buses powered by independent static inverter sets (PWR A and PWR B in Figure 3.1.1-1). The RPS inputs, logic and outputs are electrically separated to avoid any single failure disabling the RPS. There are two sets of Group 1 – 4 outputs for each Trip Logic channel (1 set from Trip Logic A1 and one set from Trip Logic A2 and the same for Trip Logic B). These outputs are depicted in Figure 3.1.1-3<sup>21</sup>. The red outline represents what will be replaced using the Common Q Platform.

Figure 3.1.1-2<sup>22</sup> shows the trip inputs to Trip Logic A1 and the Scram Contactors that open when any of the trip inputs open. The red outline represents what will be replaced using the Common Q Platform.

Trip systems are designated A and B. Trip system A is comprised of

- Instrument channels A, C, E, and G (depicted in Figure 3.1.1-2);
- Trip logics A1 and A2 (as depicted in Figure 3.1.1-1); and the
- Scram contactors A, E, C and G (as depicted in Figure 3.1.1-3).

Trip system B comprises of:

- Instrument channels B, D, F and H (partially depicted in Figure 3.1.1-1);
- Trip logics B1 and B2 (as depicted in Figure 3.1.1-1); and the
- Scram contactors B, D, F and H as depicted in Figure 3.1.1-3.

During normal operation, all sensor and trip contacts essential to safety and corresponding trip logic channel contacts are closed, and the scram contactors are energized. Trip channel bypass contacts are normally open. LGS UFSAR Table 7.2-1 lists the instruments that provide signals for the system, and Figure 2.1-1 summarizes the RPS signals that cause a scram.<sup>23</sup>

The RPS is a normally energized system. Failure of either RPS power supply results in the de-energization of one of the two pilot solenoids associated with each control rod. A complete loss of electrical power to both power supplies results in a scram. Loss of one or both power supplies does not prevent a reactor scram.<sup>24</sup>

There are two dc solenoid-operated backup scram valves that provide a second means of controlling the air supply to the scram valves for all control rods (see Figure 3.1.1-3). When the solenoids for both backup scram valves are energized, the backup scram valves vent the air supply for the scram valves.



This action initiates insertion of any withdrawn control rods regardless of the action of the scram pilot valves. The backup scram valve solenoids are energized (initiate scram) when trip logic A1 or A2 and trip logic B1 or B2 are tripped.<sup>25</sup>

When a channel sensor contact opens, its sensor relay de-energizes, opening its contacts and thereby de-energizing its associated scram contactors. Scram contactors and scram contactor logics for trip systems A and B are shown in Figure 3.1.1-3. When a scram contactor is de-energized, its contacts associated with the pilot solenoids open and those associated with the backup scram valves close. As seen on Figure 3.1.1-3, tripping A1 or A2 or both A1 and A2 trip logics will open the circuits associated with the trip system A pilot solenoids and close corresponding contacts in both trip system A and B backup scram valve circuits. When both trip systems A and B have tripped, all pilot solenoids are de-energized and both backup scram valves are energized, either of which will cause a reactor scram.<sup>26</sup>

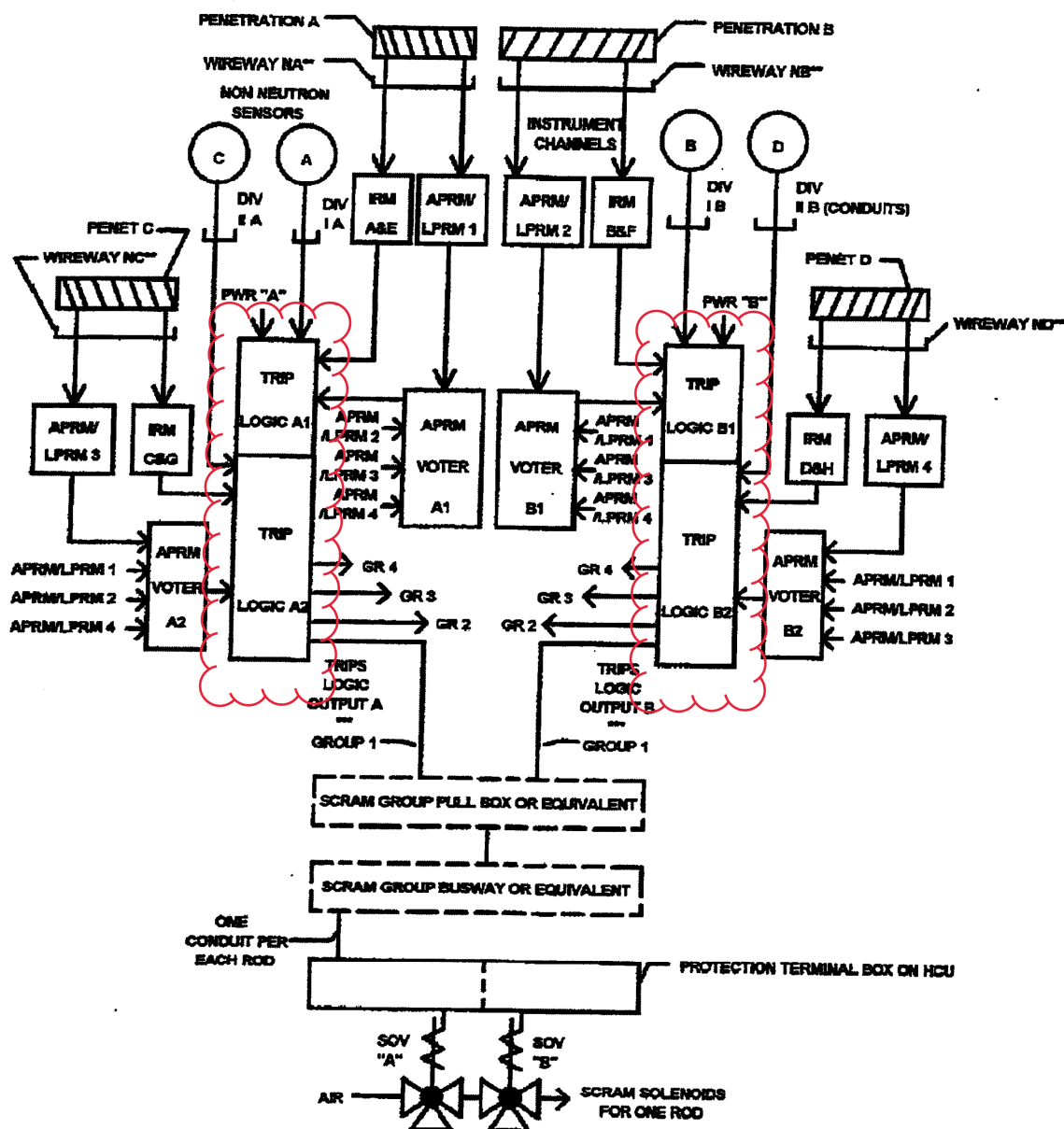
The logic arrangement of the RPS is a basic one-out-of-two-twice. The system is arranged as two separately powered trip systems. Each trip system has two redundant logics, as shown in Figures 3.1.1-2 and 3.1.1-3. Each logic receives input signals from at least one channel for each monitored variable. Each variable is monitored by at least four channels. Power relays for interrupting the scram pilot valve solenoids have high current carrying capabilities. All RPS relays are selected so that the continuous load will not exceed 50% of the continuous-duty rating.

Each trip logic provides inputs into each of the actuator logics of one trip system, as shown in Figures 3.1.1-2 and 3.1.1-3. Thus, either of the two logics associated with one trip system can produce a trip system trip. The arrangement is a one-out-of-two-twice logic. To produce a scram, the actuator logics of both trip systems must be tripped.<sup>27</sup>

To restore the RPS to normal operation following any single trip of the trip logic or a scram, the trip logic must be reset manually. Reset is possible only if the conditions that caused the trip have been cleared. Reset after a scram is permissible only after a 10 second delay. The trip systems are reset by a three-position switch in the control room. Figure 3.1.1-2 shows the functional arrangement of reset contacts for trip system A.<sup>28</sup>

The RPS reset switch is used to momentarily bypass the seal-in contacts of the final actuators of the RPS. The reset is effected in conjunction with auxiliary relays. If a single channel is tripped, the reset is accomplished immediately upon operation of the reset switch. On the other hand, if a reactor scram condition is present, manual reset is prohibited for a 10 second period to permit the control rods to achieve their fully inserted position.<sup>29</sup>





- \* RPS SENSORS A&B MAY BE CONNECTED TO A COMMON PROCESS TAP. C&D MAY ALSO SHARE ONE TAP. RPS SENSORS A&C OR B&D MUST NOT BE CONNECTED TO A COMMON PROCESS TAP.
- \*\* WIREWAYS NA, NB, etc. MAY BE ASSIGNED TO AND ROUTED WITH SEPARATED DIVISIONS AS APPROPRIATE TO PLANT LAYOUT.
- \*\*\* TRIP LOGICS A AND B OUTPUTS FOR EACH SCRAM GROUP MAY BE COMBINED IN A SINGLE CONDUIT

Figure 3.1.1-1 RPS Block Diagram



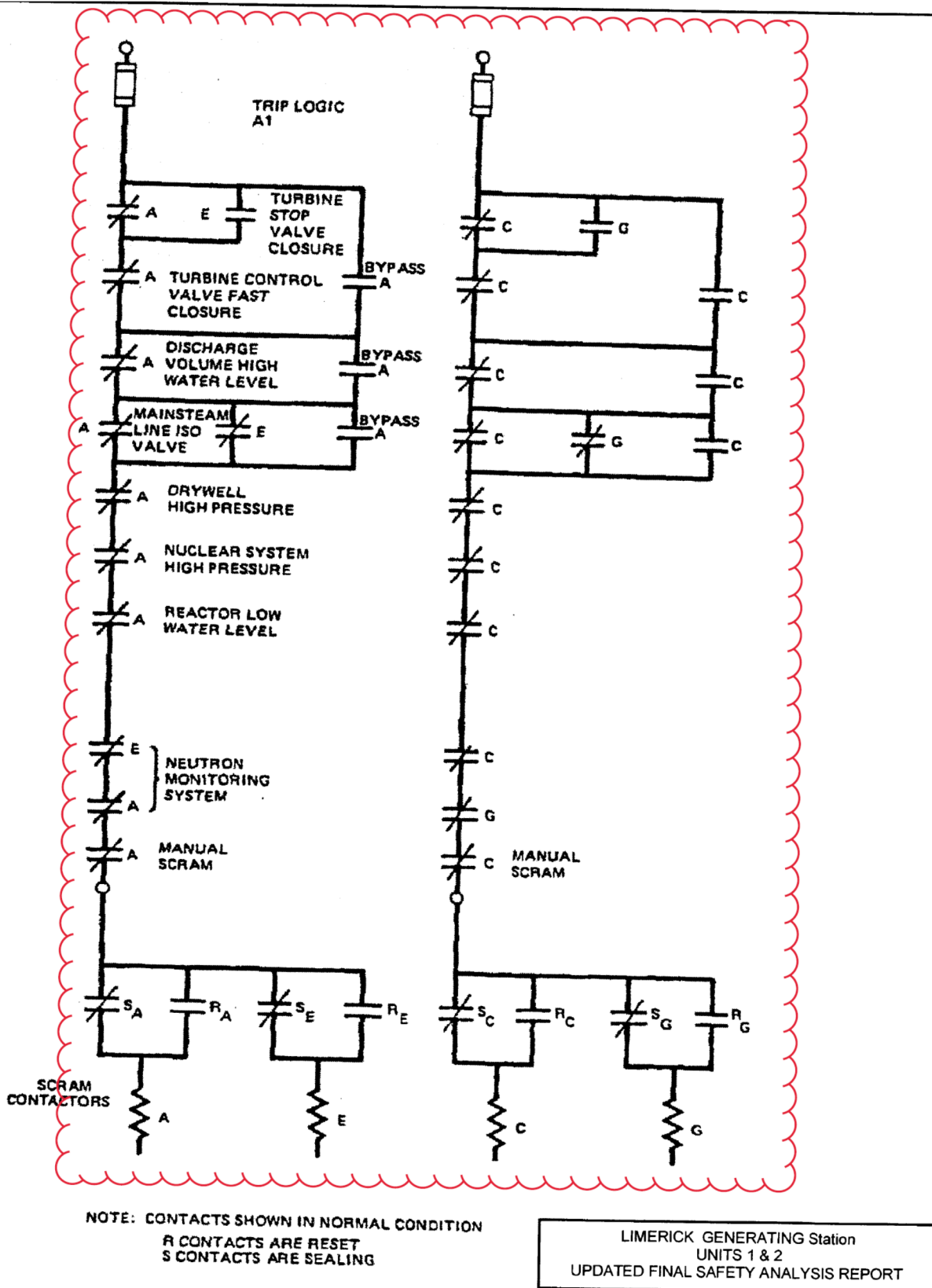


Figure 3.1.1-2 RPS Trip Logic A Scram Outputs



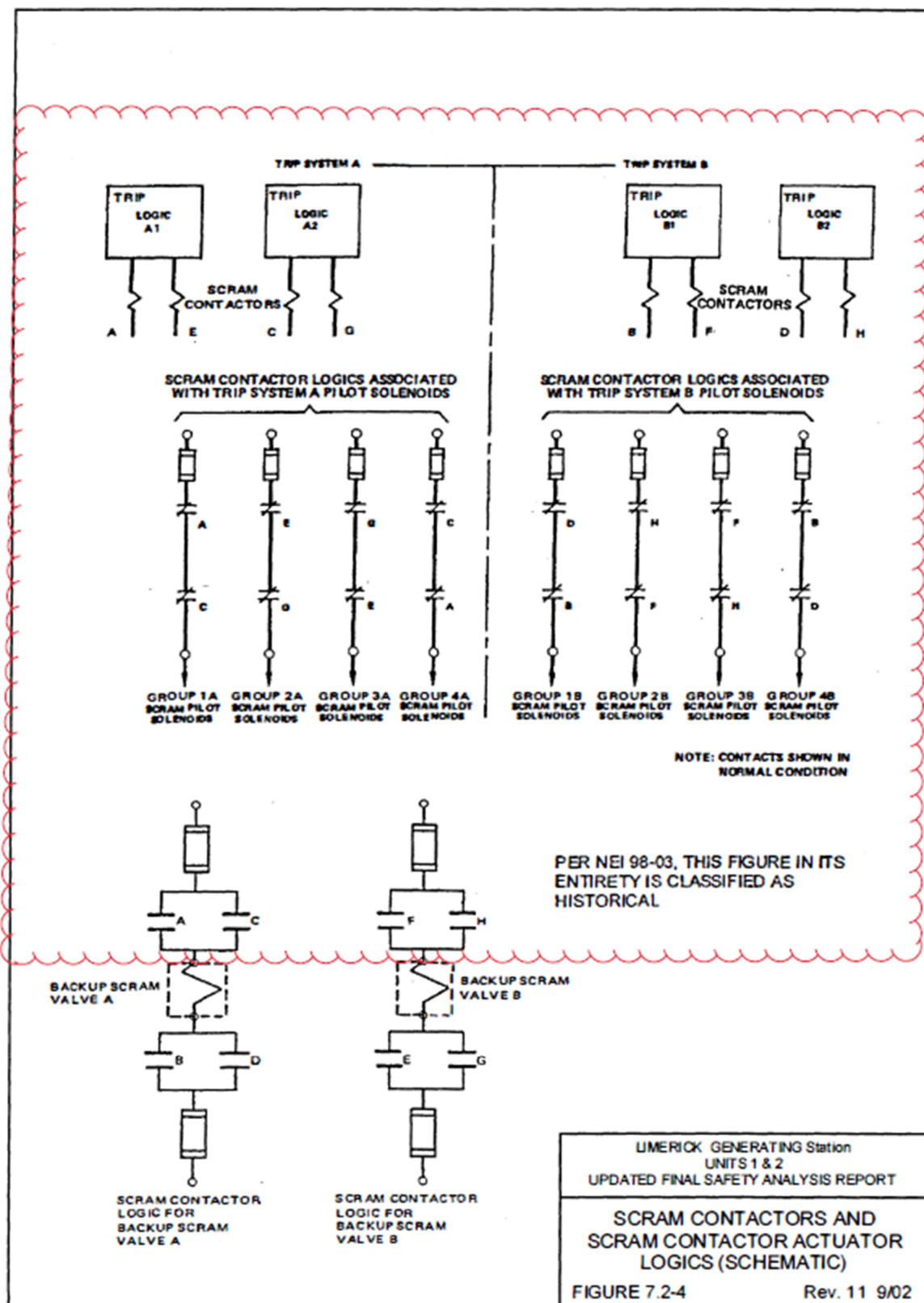


Figure 3.1.1-3 Scram Contactors and Scram Contactor Logics



A number of manual and automatic scram bypasses are provided to accommodate the varying protection requirements that depend on reactor conditions. These are automatically removed when the permissive conditions are not present. In addition, individual channels can be bypassed under administrative control for test and maintenance. All manual bypass switches are in the control room, under the direct control of the control room operator. The operating bypasses are described in the LGS UFSAR Chapter 7.2.1.1.4.4.<sup>30</sup>

The RPS Interlocks include:

- The Scram Discharge Volume (SDV) high water level trip bypass signal interlocks with the Reactor Manual Control System (RMCS) to initiate a rod block. The interlock is isolated by relay contacts so that no failure in the control system can prevent a scram.
- Reactor vessel low water level, reactor vessel pressure, main steam line radiation<sup>31</sup>, turbine stop valve closure, and drywell high pressure signals are shared with the Primary Containment and Reactor Vessel Isolation Control System (PCRVICS). The sensors operate relays in the RPS whose contacts interlock with the PCRVICS.<sup>32</sup>
- An interlock circuit provides an APRM trouble alarm whenever the number of LPRM inputs to an APRM is less than the required minimum.<sup>33</sup>

#### **3.1.1.1 Equipment Arrangement**

Physical separation and electrical isolation among redundant portions of the RPS are provided by separated process instrumentation, separated racks, separated portions of panels, and separated cabling. This separation ensures that environmental factors, electrical transients, and physical events do not impair the ability of the RPS to respond correctly when required.

The RPS has four divisions housed in two panels in the Auxiliary Equipment Room (AER) and one panel in the control room. Each panel has metallic fireproof barriers between divisions. Where equipment from more than one division is in a panel, divisional separation is provided by fire barriers or a physical distance of 6 inches or more where practicable. Where wiring from more than one redundant division is present at a single component, divisional separation is provided by fire barriers on the component, in addition to routing the wiring from the component in separate conduits or by routing wiring in such a way as to prevent any failure within the component from affecting redundant divisions. Separate racks are provided for the reactor protection sensor instrumentation in redundant divisions and they are either installed in different locations or separated by metal barriers.<sup>34</sup>

#### **3.1.1.2 Existing RPS Service and Test Functions**

The Technical Specification (TS) Surveillance Requirements (SRs) for the RPS are specified in the LGS TS 3/4.3.1.

The RPS has components that are not activated or tested during normal operation with an integrated testing procedure. These components are tested using manual test methods which allow for independent checking of individual system components. This testing includes verification of each channel trip, including scram contactors, by using the associated installed sensors and circuits to verify proper



operation. The frequency of these tests and parameters to be verified are identified in the Technical Specifications.<sup>35</sup>

The RPS can be tested during reactor operation by an overlapping series of tests. The following tests listed are those impacted by the replacement of the RPS with the Common Q Platform:

- a. The manual scram test: By depressing the manual scram button for one trip channel, appropriate scram contactors are de-energized, opening contacts in the scram contactor logics. After the first trip channel is reset, the second trip channel is tripped manually and so forth for the four manual scram buttons. The total test verifies the ability to de-energize the scram pilot valve solenoids without scram by using the manual scram push button switches. In addition to control room and computer printout indications, scram group indicator lights verify that the scram contractor contacts have opened and interrupted power in these pilot solenoids.
- b. The overall RPS response time from sensor trip to channel relay de-energization and scram contactor de-energization is verified by test.
- c. A test involves one of two methods for applying test signals to each RPS channel in turn and observing that a logic trip results. This test also verifies the independence of the channel circuitry. The test signals can be applied to the process-type sensing instruments (pressure and differential pressure) through calibration taps, or a calibration input may be applied to each instrument trip unit by use of a built-in calibrator. Calibration and test controls for pressure sensors and differential pressure sensors are located in the turbine enclosure and secondary containment. Calibration controls for the trip units are located in the AER. To gain access to the setting controls for each sensor, a cover plate or sealing device must be removed. The control room operator is responsible for granting access to the setting controls. Only properly qualified plant personnel are granted access for testing or calibration adjustments.

In addition to the above test, the operability of the pressure and level sensors may be verified by cross-checking instrument readouts in the AER at any time during operations.<sup>36</sup>

### 3.1.1.3 Existing RPS Control Room Indication

Each RPS manual and/or automatic RPS input is annunciated in the control room by isolated relay contacts. Trip logic trips also actuate the annunciator system.

When an RPS sensor channel trips, a corresponding red annunciator window on the reactor control panel in the control room indicates the out-of-limit variable. Each trip logic also initiates a corresponding red annunciator window that indicates the trip logic that has tripped. An RPS channel trip also actuates an annunciator system horn, which can be silenced by the operator. The annunciator window lights latch-in until reset manually. Reset is not possible until the condition that caused the trip has been cleared. The location of alarm windows permits the operator to quickly identify the cause of RPS trips and to evaluate the threat to the fuel or RCPB.<sup>37</sup>

The control room area is divided into three floors, the AER, the control room, and the cable spreading room. Each floor is divided into a Unit 1 and Unit 2 section. The RPS control board is located in the control room. The bench board for reactor control contains the reactor mode switch, bypass switches, scram solenoid valve status indicating lights, and manual scram switches. The RPS vertical boards are



located in the AER. The RPS vertical boards contain the trip units, trip channel and logic relays, test switches, trip indicating lights, and terminal boards. The vertical boards are installed on Power Generation Control Complex (PGCC), also referred to as the AER, floor sections and are connected to individual termination cabinets by under-floor cable ducts.<sup>38</sup>

#### 3.1.1.4 Existing RPS Reactor Operator Controls

A multi-position mode switch is provided to select the necessary scram functions for various plant conditions. The mode switch selects the appropriate sensors for scram functions and provides appropriate bypasses. The switch also interlocks such functions as control rod blocks and refueling equipment restrictions, which are not considered here as part of the RPS. The switch is designed to provide separation between the four trip channels. The mode switch positions and their related scram functions are as follows:

- a. Shutdown: Initiates a reactor scram; bypasses main steam line isolation scram. Provides a logic input to enable SDV high level bypass keyswitch function. Actuates RPS 10 second scram seal in time delay. APRM setdown setpoint and inoperable scrams enabled.
- b. Refuel: APRM setdown setpoint and inoperable scrams enabled. IRM scrams enabled, bypasses MSIV closed scram. Provides a logic input to enable SDV high level bypass keyswitch function.
- c. Startup: APRM setdown setpoint and inoperable scrams enabled. IRM scrams enabled, bypasses MSIV closed scram.
- d. Run: APRM setdown setpoint disabled, all other APRM and OPRM scrams enabled, IRM scrams bypassed.<sup>39</sup>

#### 3.1.2 PCRVICES

The PCRVICES (also referred to as the Nuclear Steam Supply Shutoff System or NSSSS) includes sensors, power supplies, trip systems, logic channels, switches, transmitters and remotely operated valve closing mechanisms associated with those valves which affect isolation of primary containment and/or the reactor coolant system. Piping systems that penetrate primary containment and interface directly with the primary containment atmosphere or the reactor coolant system contain two isolation valves. One isolation valve is located inside primary containment and the other isolation valve is located outside primary containment, as close to the containment wall as practical.<sup>40</sup>

The replacement scope is only the logic channels and switches. Sensors, plant power sources, transmitters, valves, and remotely operated valve closing mechanisms are not being replaced.

A trip system is an arrangement of various sensors and associated components which are used to evaluate plant parameters and produce discrete trip outputs when the logic is satisfied. The components within a trip system must maintain electrical and physical separation from the components in the other trip system.

The logic trains that make up a trip system are divided into four separate channels. The PCRVICES logic utilized for MSIV (in Group 1) isolation is arranged in a one-out-of-two-twice manner, similar to the reactor protection system (see Table 2.2-1). The logic is composed of two trip systems (A and B). Trip system A consists of channels A1 & A2 whereas trip system B consists of channels B1 & B2. A full PCRVICES group 1 isolation is defined as concurrent trips of trip systems A & B. This scheme requires at



least one channel in each trip system to trip. This will result in closure of all valves in this group. A 1/2 group isolation is a trip of only one trip system. This satisfies part of the isolation logic for a particular valve group but will not cause valve motion.<sup>41</sup>

For all other isolation logic, unlike the MSIV logic, is arranged with channels A1 & B1 in trip system A and channels A2 & B2 in trip system B. Channels A1 & B1 are associated with inboard isolation valves and channels A2 & B2 are associated with the outboard isolation valves. These groups are referred to as dual trip systems consisting of a two-out-of-two logic (or an inboard-outboard logic). Inboard-outboard logic schemes require both channels of a trip system to trip before initiating a closure of the corresponding inboard or outboard isolation valve. This group logic portion of the PCRVICES responds to signals that could indicate a breach of a specific system.

The power supplies for the PCRVICES are arranged so that the loss of one supply cannot prevent automatic isolation when required.<sup>42</sup> All sensors and trip contacts essential to safety are closed when energized. The trip logic for each isolation group is de-energize to trip.<sup>43</sup>

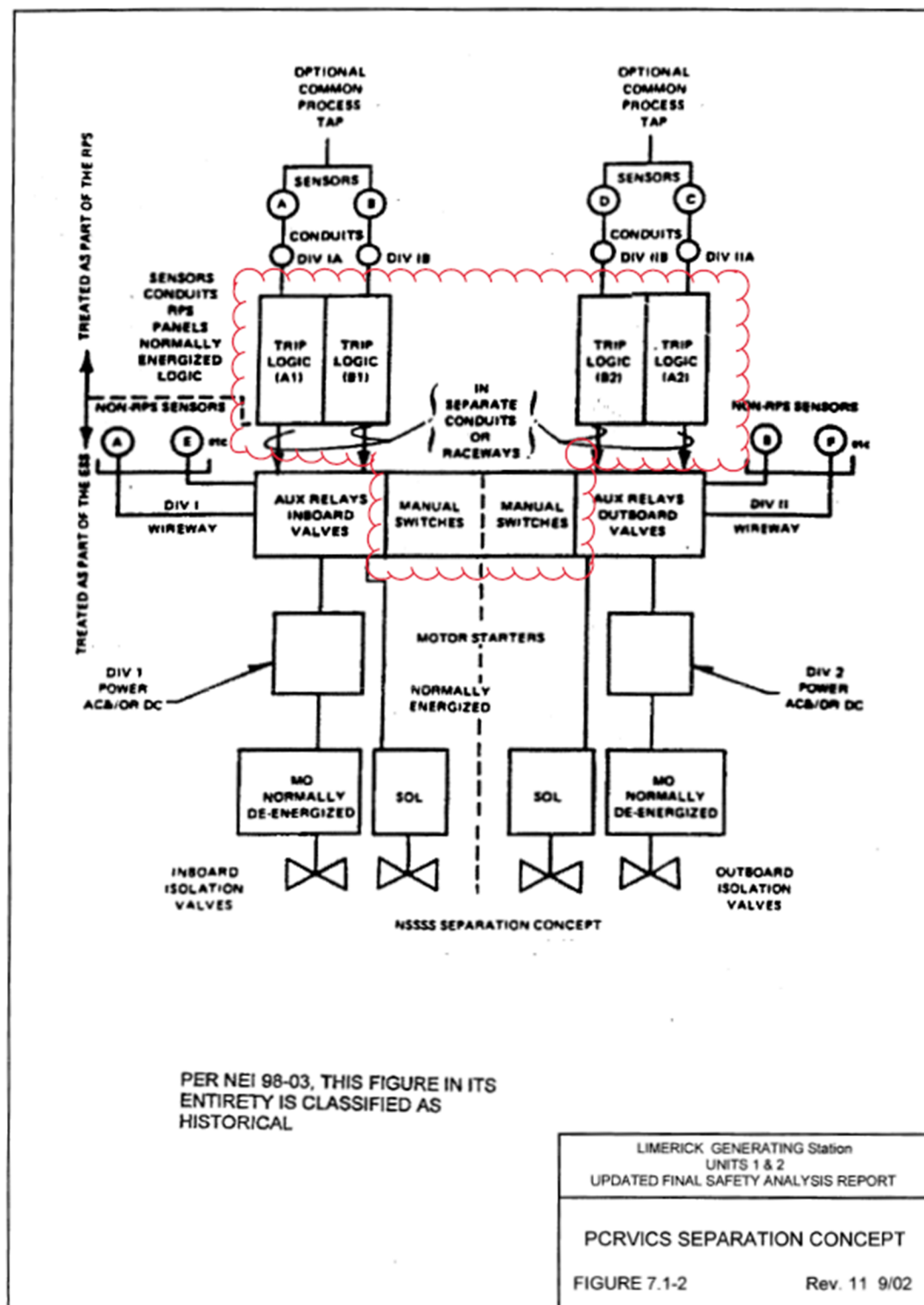
There are four manual isolation pushbutton switches, one for each logic channel. Operation of a manual isolation pushbutton requires two separate actions by the operator. First, the switch is armed by rotating the switch collar located at the base of the switch. Secondly, the pushbutton is depressed to initiate the isolation function.<sup>44</sup>

The MSIV logic, is a contact and relay logic that is in the normal/energized condition. The logic utilized is divided, into four individual logic channels (A1, A2, B1, and B2). Channels A1 & A2 are assigned to trip system A and, B1 & B2 to trip system B. A trip of either channel A1 or A2 will cause de-energization of the A pilot solenoids (120Vac) for inboard MSIVs and B pilot solenoids (125Vdc) for outboard MSIVs. A trip of either channel B1 or B2 will cause de-energization of the A solenoids for outboard MSIVs, and B solenoids for inboard MSIVs. Therefore, both MSIV pilot solenoids must de-energize for an MSIV closure to occur. As a result the trip logic is a one-out-of-two-twice scheme.

Once isolation is initiated, the valve(s) continue to close, even if the condition that caused the isolation is restored to normal. The operator must manually reposition valve control switches in the control room and manually reset the logic in order to reopen a valve that has been automatically closed. This involves placing the valve control switches in the closed position and then depressing the applicable isolation reset switch.<sup>45</sup>

Figure 3.1.2-1 outlines what will be replaced with the Common Q Platform.





**Figure 3.1.2-1 PCRVICS (NSSSS) Block Diagram**

The PCRVICS includes the instrument channels, trip logics, and actuation circuits that activate valve closing mechanisms associated with the valves that, when closed, effect isolation of the primary



containment, secondary containment, or reactor vessel. The PCRVICS instrument channels and logic circuits support the PCRVICS functions in Table 2.2-1.

PCRVICS provides initiation to the following systems:

- a. Standby Gas Treatment System (SGTS, which is described in the LGS UFSAR Chapter 7.3.1.1.7)
- b. Reactor Enclosure Isolation System (REIS) and HVAC support system (which are described in the LGS UFSAR Chapter 7.3.1.1.9)

The purpose of the system is to prevent the gross release of radioactive materials to the environment from the fuel or a break in the RCPB. The PCRVICS automatically isolates the appropriate pipelines that penetrate the primary containment whenever monitored variables exceed preselected setpoints. All other pipelines that penetrate primary containment are manually isolated. The power generation objective of this system is to prevent spurious closure of isolation valves as a result of single failure.<sup>46</sup>

Power for the system instrument channels are supplied from the two nonessential electrical buses that supply the RPS trip systems. Power for the isolation logics of the isolation control system and MSIVs are supplied from the two nonessential electrical buses that supply the RPS trip systems. Each bus has its own inverter and can receive alternate power from an alternate power source. Each bus can be supplied from only one of its power sources at any given time.

The MSIV controls include pneumatic piping and an accumulator for the Air Operating Valves (AOVs) as the isolation motive power source in addition to the springs. Pressure, temperature, and water level sensors are mounted on instrument racks or locally in either the reactor enclosure or the turbine enclosure. Valve position switches are mounted on Motor Operating Valves (MOVs) and AOVs. Switches are encased to protect them from environmental conditions. All signals transmitted to the control room are electrical (no pipe from the nuclear system penetrates the control room). The sensor cables and logic power supply cables are routed to cabinets in the AER, where the system logic is located.<sup>47</sup>

Unless indicated, there are no operational bypasses or interlocks.

### **3.1.2.1 PCRVICS - Reactor Vessel Low Water Level**

This function supports PCRVICS Groups I, IB, IIA-B, III, VIA-C, VIIA-B, and VIIIA-B functions in Table 2.2-1. A low water level in the reactor vessel could indicate that reactor coolant is being lost through a breach in the RCPB and that the core is in danger of becoming overheated as the reactor coolant inventory diminishes.

Three reactor vessel low water level isolation trip settings are used to complete the isolation of the primary containment and the reactor vessel.

Reactor vessel low water level signals used by PCRVICS and RPS are initiated from eight differential pressure sensors, four sensors for the level 1 and level 2 trip and four sensors for the level 3 trip. They sense the difference between the pressure caused by a constant reference leg of water and the pressure caused by the actual water level in the vessel.



### Level 3 sensors

Four sensors are used in the measurement of level 3 and are used by both NSSS and RPS. Each sensor is connected to different reference leg. Sensors A and B share a common variable leg. Sensors C and D share a common variable leg. This arrangement ensures that no single physical event can prevent isolation, if required. The variable legs are different from those used by the level 1 and 2 sensors.

### Level 1 and Level 2 sensors

Four sensors are used in the measurement of level 1 and 2. Signals from these sensors are used by NSSS only. Each of these sensors is connected to the same reference legs as level 3 sensors, with one sensor per reference leg. Each sensor connects to a different variable leg.<sup>48</sup>

### Group IIA, b. Reactor Pressure – High (RHR Valve Permissive)

The containment spray lineup must be manually aligned by the control room operator. To divert a portion of the LPCI mode flow into the - containment spray line, drywell pressure must be -high and reactor vessel water level greater than (2/3) core height. -Requiring the two permissive signals ensures the need for containment spray and an adequate water level in the reactor vessel.<sup>49</sup>

### **3.1.2.2 PCRVICES - Main Steam Line Temperature in Outboard MSIV Room and Turbine Enclosure Main Steam Tunnel High Ambient Temperature**

This function supports PCRVICES Group IA functions in Table 2.2-1. High ambient temperature in the areas in which the main steam lines are located outside of the primary containment could indicate a leak in a main steam line. The automatic closure of various valves prevents the excessive loss of reactor coolant and the release of a significant amount of radioactive material from the RCPB.<sup>50</sup>

High ambient temperature in the areas in which the main steam lines are located outside of the primary containment could indicate a leak in a main steam line. Each main steam line isolation logic channel is tripped by high ambient temperature in the outboard MSIV room or main steam tunnel. The automatic closure of various valves prevents the excessive loss of reactor coolant and the release of a significant amount of radioactive material from the RCPB.

The temperature sensors give an input to temperature indicating switches. The temperature detection system is designed to alarm on steam leaks equivalent to 5 gpm and isolate on steam leaks equivalent to 25 gpm. A total of 4 main steam line high ambient temperature channels are provided in the outboard MSIV room and 32 are provided on the main steam line in the turbine enclosure. Each main steam line isolation logic channel is tripped by high ambient temperature in the outboard MSIV room, or in the turbine enclosure.<sup>51</sup>

When a predetermined increase in ambient temperature is detected, trip signals are transmitted to the PCRVICES. The PCRVICES initiates closure of all main steam line isolation and drain valves. Four instrumentation channels are provided to ensure protective action when needed and to prevent inadvertent isolation resulting from instrumentation malfunctions.



The output trip signal of each logic channel initiates a trip logic division trip. The output trip signals of the trip logic divisions are combined in one-out-of-two-twice for the MSIVs or two-out-of-two logics for the main steam line drains. Logic channels A or C and B or D are required to initiate main steam line isolation. Logic channels A and B or C and D are required to initiate main steam line drain isolation. Thus, failure of any one division does not result in inadvertent action.<sup>52</sup>

### **3.1.2.3 PCRVICS - Main Steam Line High Flow**

This function supports PCRVICS Group IA functions in Table 2.2-1. Main steam line high flow could indicate a breach in a main steam line. Automatic closure of isolation valves prevents excessive loss of reactor coolant and release of significant amounts of radioactive material from the RCPB.

The main steam line high flow trip setting selected is high enough to permit isolation of one main steam line for testing at rated power without causing an automatic isolation of the other steam lines, yet low enough to permit detection of a steam line break. High flow in each main steam line is sensed by four differential pressure sensors that sense the pressure difference across the flow element in that line.<sup>53</sup>

Sixteen differential pressure indicating switches, four for each main steam line, monitor the main steam line flow. Four differential pressure indicating sensors are installed on each main steam line and provide the earliest practicable detection of a main steam line break. One differential pressure circuit for each main steam line is associated with each of four logics.<sup>54</sup>

When a significant increase in main steam line flow is detected, trip signals are transmitted to the PCRVICS. The PCRVICS initiates closure of all main steam line isolation and drain valves on any significant main steam line break.

Four instrumentation logics are provided to ensure protective action when required and to prevent inadvertent isolation resulting from instrumentation malfunctions. The output trip signal of each instrumentation channel initiates a division logic trip. The output trip signals of the logic divisions are combined in one-out-of-two-twice and two-out-of-two logics. Logic divisions A or C and B or D are required to initiate main steam line isolation. Logic divisions A and B or C and D are required to initiate main steam line drain isolation. Failure of any one logic does not result in inadvertent action.<sup>55</sup>

### **3.1.2.4 PCRVICS - Main Steam Line Low Pressure**

This function supports PCRVICS Group IA functions in Table 2.2-1. Low steam pressure at the turbine inlet while the reactor is operating could indicate a malfunction of the steam pressure controller in which the turbine control valves or turbine bypass valves become fully open and cause rapid depressurization of the reactor vessel. The steam pressure at the turbine inlet is monitored.

The low steam pressure isolation setting selected is far enough below normal turbine inlet pressures to prevent spurious isolation, yet high enough to provide timely detection of a pressure controller malfunction.



Main steam line low pressure is monitored by four pressure sensors that sense pressure downstream of the outboard MSIVs. The sensing point is located at the header that connects the four steam lines upstream to the turbine stop valves. Each sensor provides a signal to one isolation logic.<sup>56</sup>

Four pressure channels, one for each main steam line, monitor main steam line pressure. Each channel is associated with one of four trip logics. The locations of the pressure sensors provide the earliest practicable detection of low main steam line pressure.<sup>57</sup> When a predetermined decrease in main steam line pressure is detected, trip signals are transmitted to the PCRVICS. The PCRVICS initiates closure of all main steam line isolation drain valves. The output trip signals of the trip logics are combined in one-out-of-two-twice configuration for the MSIVs and two-out-of-two configuration for the drain valves. Trip logics A or C and B or D are required to initiate main steam line isolation. Trip logics A and B or C and D are required to initiate main steam line drain isolation.<sup>58</sup>

### **Bypasses and Interlocks**

The main steam line low pressure trip is bypassed by the reactor mode switch in the shutdown, refuel, and startup modes of reactor operation. In the run mode, the low pressure trip function is operative.

There are no interlocks to other systems for main steam line low pressure trip signals.<sup>59</sup>

#### **3.1.2.5 PCRVICS - Drywell High Pressure**

PCRVICS monitors the drywell and suppression chamber pressure to limit the amount by which suppression chamber pressure can exceed drywell pressure. It supports PCRVICS Groups IIB, IVB, VB, VIA-C and VIIIA-B functions in Table 2.2-1. High pressure in the drywell could indicate a breach of the RCPB inside the drywell. The automatic closure of various valves prevents the release of significant amounts of radioactive material from the primary containment.<sup>60</sup>

Drywell pressure is monitored by four pressure sensors that are mounted on instrument racks outside the primary containment. Instrument sensing lines that terminate in the reactor enclosure connect the sensors with the drywell interior. Redundant sensors are physically separated and electrically connected to the isolation control systems so that no single event prevents isolation because of primary containment high pressure.<sup>61</sup> When a predetermined increase in drywell pressure is detected, trip signals are transmitted to the PCRVICS for generation of isolation signals.

Four instrumentation channels are provided to ensure protective action when required and to prevent inadvertent isolation resulting from instrumentation malfunctions. The output trip signals of the instrumentation channels are combined in two-out-of-two logic. Instrumentation channels A and B or C and D are required to initiate isolation of either inboard or outboard valves, respectively.<sup>62</sup>

#### **3.1.2.6 PCRVICS - Reactor Enclosure Ventilation Exhaust Radiation Monitoring System**

This system is designed to:

- a. Detect a gross release of radioactive material into the reactor enclosure ventilation duct
- b. Promptly indicate a gross release of radioactive material



- c. Provide, on detection of a gross release of radioactive material:
  - 1. A trip signal for the reactor enclosure fans and closure of the valves to the vent exhaust system
  - 2. A trip signal to isolate the primary containment atmosphere purge and vent lines and start the SGTS
  - 3. An annunciation alarm signal in the control room<sup>63</sup>

This system supports PCRVICES Groups VIA-C and VIIA-B functions in Table 2.2-1.

The purpose of this system is to indicate when excessive amounts of radioactivity exist in the reactor enclosure ventilation exhaust and to provide signals for initiation of appropriate action so that the release of radioactive gases to the environment is limited to levels below the guidelines of published regulations. The radiation monitoring system is described in UFSAR Chapter 11.5 and is not being replaced. The system consists of four independent channels monitoring the reactor zone.<sup>64</sup>

### 3.1.2.7 PCRVICES - Refueling Area Ventilation Exhaust Radiation Monitoring System

This system is designed to:

- a. Detect a gross release of radioactive material into the refueling area ventilation duct
- b. Promptly indicate a gross release of radioactive material
- c. Provide on detection of a gross release of radioactive material:
  - 1. A trip signal for the refueling area fans and closure of the valves to the ventilation exhaust system
  - 2. A trip signal to isolate the primary containment atmosphere purge and vent lines and start the SGTS
  - 3. An alarm annunciation in the control room<sup>65</sup>

This system supports PCRVICES Groups VIA-C and VIII (Refuel Floor HVAC) functions in Table 2.2-1.

The purpose of this system is to indicate when excessive amounts of radioactivity exist in the refueling area ventilation exhaust and to provide signals for initiation of appropriate action so that the release of radioactive gases to the environment is limited to levels below the guidelines of published regulations. The radiation monitoring system is described in UFSAR Chapter 11.5 and is not being replaced. The system consists of independent channels, monitoring the refueling area.<sup>66</sup>

### 3.1.2.8 PCRVICES - RWCU System High Differential Flow

This function supports PCRVICES Group III functions in Table 2.2-1. High differential flow in the Reactor Water Cleanup (RWCU) system could indicate a breach of the RCPB in the cleanup system. The flow at the inlet to the system (suction from "B" recirculation line and bottom head drain) is compared with the flow at the outlets of the system (discharge to feedwater, main condenser, radwaste and CST). High differential flow initiates isolation of the cleanup system.<sup>67</sup> The RWCU system description is in UFSAR Chapter 7.6.1.3.3.4.2 and is not being replaced, however the replacement Common Q system will perform this protective isolation function previously performed by the RWCU.



The RWCU system inlet flow is compared to RWCU outlet flow. A flow element, flow transmitter, and square root converter for each of these three lines provide signals to a common flow summer that trips on a high differential flow condition. Each flow alarm unit starts a timer that, after a time delay to avoid spurious trips, activates isolation. Flow and differential flow indications are provided in the control room.<sup>68</sup>

Using one-out-of-two logic, the RWCU flow comparison monitoring circuit initiates an RWCU system isolation signal after a time delay from the time the flow rate difference exceeds a preset limit.<sup>69</sup>

### **3.1.2.9 PCRVICES - RWCU System Area High Temperature and Differential Temperature**

This function supports PCRVICES Group III functions in Table 2.2-1. High temperature in the equipment room areas of the RWCU system could indicate a breach in the RCPB in the cleanup system. High ambient temperature and high differential temperature in the equipment area ventilation system initiates isolation of the RWCU system.<sup>70</sup> The RWCU system description is in UFSAR Chapter 7.6.1.3.3.4.3 and is not being replaced, however the replacement Common Q system will perform this protective function previously performed by the RWCU.

Twelve ambient temperature and 12 differential temperature sensing circuits monitor the RWCU system area temperatures. Six ambient and 6 differential temperature circuits are associated with each of two instrumentation channels. Six ambient temperature elements are located in the pump-room and the heat exchanger room. Six pairs of temperature elements are located in the ventilation supply and exhaust areas of the above locations. The locations of the temperature elements provide the earliest practicable detection of any RWCU system high temperature leak.<sup>71</sup>

When a significant increase in RWCU system area ambient or differential temperature is detected, trip signals are transmitted to the PCRVICES. The PCRVICES initiates closure of all RWCU system isolation valves.

Two independent instrumentation trip channels are provided to ensure protective action when required. The output trip signal of each instrumentation channel initiates a logic channel and closure of either the inboard or outboard RWCU system isolation valve. In order to close both the inboard and outboard isolation valves, both logic channels must trip. Protection against inadvertent isolation due to instrumentation malfunction is neither required nor provided.<sup>72</sup>

### **3.1.2.10 PCRVICES - Main Condenser Low Vacuum Trip**

This function supports PCRVICES Group IA functions in Table 2.2-1. A main steam line isolation valve trip from a low condenser vacuum instrumentation system is provided. The main turbine condenser low vacuum signal could indicate a leak in the condenser. Initiation of automatic closure of selected valves will prevent excessive loss of reactor coolant and the release of significant amounts of radioactive material from the RCPB.<sup>73</sup>

Four vacuum sensors monitor the main condenser vacuum. Each vacuum sensor is associated with one of four separate trip logics. Four vacuum sensors are installed to provide the earliest practicable detection of a main condenser leak.<sup>74</sup>



When a predetermined decrease in main condenser vacuum is detected, trip signals are transmitted to the PCRVICES. The PCRVICES initiates closure of all main steam line isolation and drain valves.

Four vacuum sensors with associated trip units are provided to ensure protective action when required and to prevent inadvertent isolation resulting from instrumentation malfunctions. The output signals of the trip logics are combined in one-out-of-two-twice logic for the MSIVs and two-out-of-two logics for the main steam line drain valves. Trip logics A or C and B or D are required to initiate main steam line isolation. Trip logics A and B or C and D are required to initiate main steam line drain isolation. Failure of any one trip logic does not result in inadvertent isolation action.<sup>75</sup>

### **Bypasses and Interlocks**

Main condenser low vacuum trip can be bypassed manually when the turbine stop valve is less than 90% open. There are no interlocks to other systems from the main condenser low vacuum trip signals.<sup>76</sup>

#### **3.1.2.11 PCRVICES - HPCI System Isolation Signals**

This function supports PCRVICES Groups IVA-B functions in Table 2.2-1. The HPCI system is constantly monitored for leaks by the following types of monitoring circuits:

- a. Equipment area and pipe chase area ambient and differential temperature monitoring
- b. HPCI steam flow rate monitoring\*
- c. HPCI turbine exhaust diaphragm pressure monitoring
- d. HPCI steam line pressure monitoring

\* will not be an input to the PPS (see Section 3.3)

When limiting conditions are attained an HPCI auto-isolation signal is initiated and an annunciator activated in the control room.

HPCI area temperatures are monitored by instrumentation of the LDS. Monitored temperatures include the following.

- a. HPCI pipe chase area ambient temperatures
- b. HPCI emergency area cooler ambient temperature
- c. HPCI area vent air differential temperature.

Eight ambient temperature elements are installed in the HPCI pipe chase areas. Four sensors are associated with each auto-isolation logic division. Seven temperature elements are installed in the HPCI equipment compartment. Four of these elements form two differential temperature pairs which monitor high ventilation air differential temperature. One pair is associated with one logic division and the other pair is associated with the other logic division. The other three temperature elements monitor the HPCI pump compartment ambient temperature. One ambient temperature element is associated with one logic division and the other two ambient temperature elements are associated with the other logic division.<sup>77</sup>



When any one monitored temperature reaches its setpoint, an HPCI auto-isolation signal is initiated and an annunciator activated in the control room. Closure of the outboard HPCI steam supply isolation valve and the steam line warm-up isolation valve is controlled by one logic division and the inboard steam supply isolation valve by the other logic division. Two instrumentation channels are provided to assure protective action when required. In order to close both the inboard and outboard isolation valves, both logic divisions must trip.<sup>78</sup>

### **3.1.2.12 PCRVICS - RCIC System Isolation Signals**

This function supports PCRVICS Groups VA-B functions in Table 2.2-1. The RCIC system is constantly monitored for leaks by the following types of monitoring circuits:

- a. Equipment area and pipe chase area ambient and differential temperature monitoring
- b. RCIC steam flow rate monitoring
- c. RCIC steam line pressure monitoring
- d. RCIC turbine exhaust diaphragm pressure monitoring

When limiting conditions are attained an RCIC auto-isolation signal is initiated and an annunciator activated in the control room.<sup>79</sup>

Setpoints are predetermined which indicate a possible leak. If the setpoint is reached, an RCIC auto-isolation signal is initiated and an annunciator activated in the control room.<sup>80</sup>

### **3.1.2.13 Existing PCRVICS Service and Test Functions**

Portions of PCRVICS are not activated or tested during normal operation with an integrated testing procedure. These portions of the system are tested using manual test methods which allow for independent checking of individual components. This testing includes monitoring of installed sensors and circuits to verify proper operation, to assure that isolation will occur when needed. The frequency of these tests and the parameters to be verified are identified in the Technical Specifications.

PCRVICS is capable of complete testing in overlapping portions during power operation. Operation of the level, pressure, flow, differential flow, and vacuum sensors may be verified by cross-comparison of instrument channels. In addition, these transmitters may be valved out of service one at a time and functionally tested using a test pressure source. The channel trip units and trip relays can be calibrated and tested by injecting a calibration signal.

The MSIV logic relays can be tested either by tripping a transmitter or trip unit or by actuating the manual isolation switch in a given logic division. The MSIV indicator lights and trip annunciators indicate a logic trip. Other isolation valve logic can be likewise tested in conjunction with logic test switches provided for this purpose. Indicator lights will indicate a logic trip.<sup>81</sup>

### **3.1.3 ECCS**

The ECCS is a network of four systems:



- HPCI system
- ADS
- Core spray system
- LPCI mode of the RHR system

The ECCS instrumentation detects a need for core cooling systems operation, and the trip systems initiate the appropriate response.

The instrumentation and controls of the ECCS network system are powered by the 125 V dc and 120 V ac systems. The redundancy and separation of these systems are consistent with the redundancy and separation of the ECCS functional requirements.<sup>82</sup>

Separation within the ECCS is designed so that no single occurrence can prevent core cooling when required. Control and instrumentation equipment wiring is segregated into separate divisions designated 1, 2, 3, and 4. Similar separation requirements are also maintained for the control and motive power required. Separation is as follows:



**Table 3.1.3-1 ECCS Divisions**

<u>Division 1</u>	<u>Division 2</u>	<u>Division 3</u>	<u>Division 4</u>
Core spray A	Core spray B	Core spray C	Core spray D
RHR "A"	RHR "B"	RHR "C"	RHR "D"
	HPCI*		HPCI**
ADS "A"		ADS "C"	

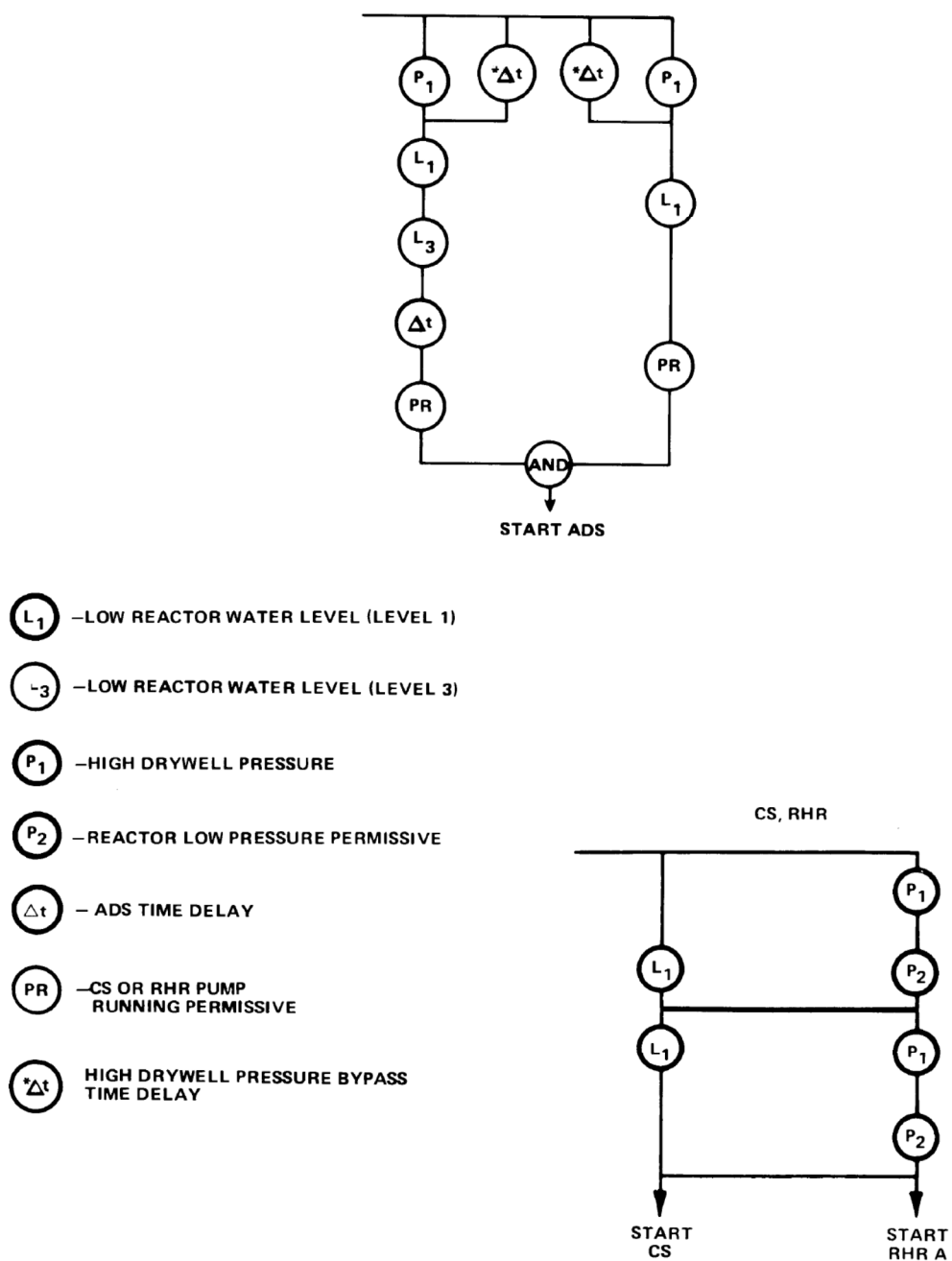
\*Including system controls outboard isolation valves

\*\* Inboard isolation valves only

The ADS, combined with the low pressure ECCS (Core Spray and RHR), is considered a backup for HPCI.<sup>83</sup>

Figure 3.1.3-1 summarizes the ECCS activations. The Common Q Platform would replace the scope of this diagram.





**Figure 3.1.3-1 ECCS activations (CS=Core Spray)<sup>84</sup>**

Figure 3.1.3-2 depicts the divisional arrangement of the ECCS functions. The red outline in the figure represents the scope of the Common Q Platform replacement.



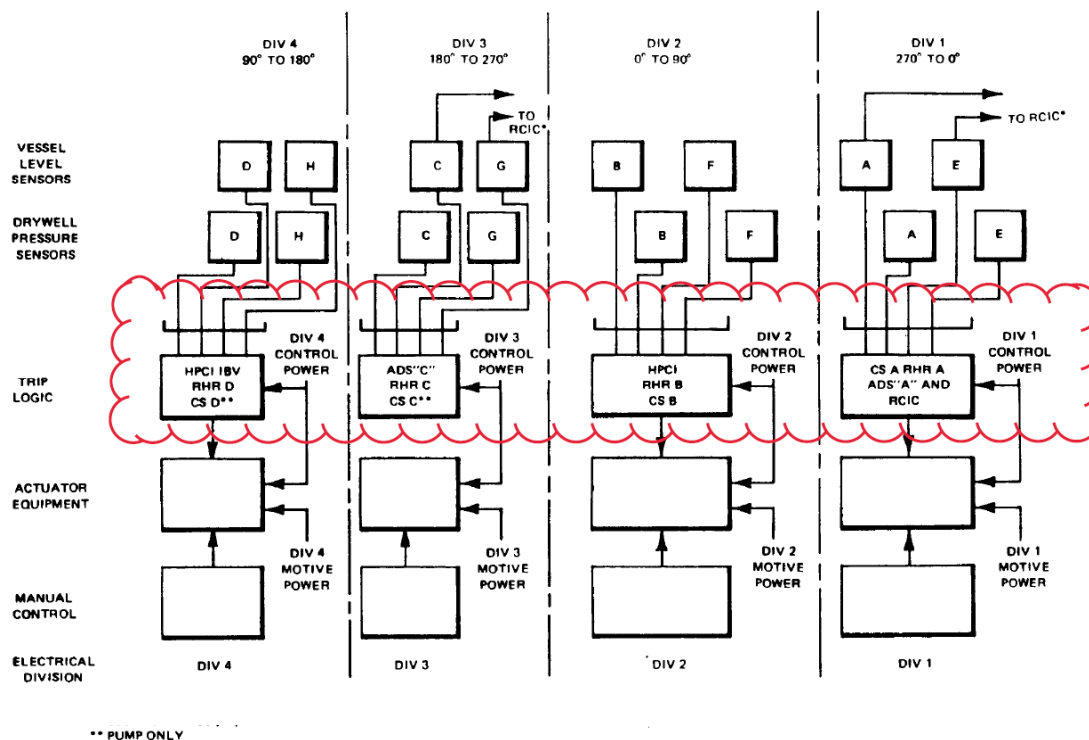


Figure 3.1.3-2 ECCS Divisional Arrangement (CS=Core Spray)<sup>85</sup>

### 3.1.3.1 HPCI

Pressure and level transmitters used in the HPCI system are located on racks in the reactor enclosure. The only active component for the HPCI system located inside the primary containment is the inboard HPCI system turbine steam supply line isolation valve. The rest of the HPCI system control and instrumentation is located outside the primary containment. A full flow functional test of the system can be conducted during normal reactor power operation; however, the controls are configured such that the system can be realigned automatically to fulfill its safety function regardless of the test being conducted (there are three exceptions to this outlined in the UFSAR).<sup>86</sup>

Reactor vessel low water level is monitored by four level sensors that sense the difference between the pressure due to a constant reference leg of water and the pressure due to the actual height of water in the vessel. Each level sensor provides an input to a trip unit. The four trip units are connected in a one-out-of-two-twice logic to provide an automatic HPCI initiation signal. Two lines, attached to taps above and below the water level on the reactor vessel, are required for the differential pressure measurement for each pair of level sensors. The lines terminate outside the primary containment and inside the reactor enclosure. The sensors are physically separated from the ADS sensors and tap off the reactor vessel at points widely separated from the ADS sensors. These same lines are also used for pressure and water level instruments for other systems. A similar arrangement of the ADS instrumentation initiates the ADS system. The arrangement ensures that no single event can prevent reactor vessel low water level from initiating both the HPCI system and the ADS.



Primary containment pressure is monitored by four pressure sensors that are mounted on an instrument rack outside the drywell, but inside the reactor enclosure. Pipes from the drywell interior to the sensors provide the sensing lines. Each drywell high pressure sensor provides an input into a trip unit. The four trip units are connected in a one-out-of-two-twice logic to provide an automatic HPCI initiation signal. The relay contacts from the trip units are arranged so no single event can prevent containment high pressure from initiating the HPCI system and ADS. The sensors are physically separated from the ADS pressure sensors and tap off the containment at points widely separated from the ADS pressure sensors.

The HPCI system controls automatically start the HPCI system from the receipt of a reactor vessel low water level signal (Level 2) or primary containment drywell high pressure signal and bring the system to its design flow rate within 60 seconds. The system can also be initiated by use of a system-level remote manual switch or an individual remote manual switch for each valve and the auxiliary oil pump which provides the initial hydraulic fluid for the turbine stop and governor valves. In all initiation modes, the system is prevented from operating above high water level (Level 8) using one-out-of-two-twice logic. The controls then function to provide design makeup water flow to the reactor vessel until the amount of water delivered to the reactor vessel is adequate (Level 8), at which time the HPCI system automatically shuts down. The system is designed to automatically cycle between these two levels. The controls are arranged to allow remote manual startup, operation, and shutdown.<sup>87</sup>

Either reactor vessel low water level (Level 2) or primary containment (drywell) high pressure can automatically start the HPCI system. Reactor vessel low water level is an indication that reactor coolant is being lost and that the fuel is in danger of being overheated. Primary containment high pressure is an indication that a breach of the nuclear system process barrier has occurred inside the drywell.<sup>88</sup>

The HPCI actuated devices are automatically controlled by logic circuitry or manually controlled by switches in the control room. Motor Operated Valves (MOVs) are provided with appropriate limit and/or torque switches to turn off the motors when the fully open or fully closed positions are reached. Valves that are automatically closed on isolation signals are equipped with remote manual reset devices so that they cannot be reopened without operator action. All essential components of the HPCI system controls operate on dc power or ac power supplied by an inverter that is part of the ECCS.<sup>89</sup>

The existing HPCI control logic circuitry (including bypass) and operator manual control interfaces, as well as interfaces to plant equipment (sensors and plant actuating equipment) will be replaced by the Common Q-based PPS.

#### **3.1.3.1.1 HPCI Bypasses and Interlocks**

To prevent the turbine-pump from being damaged by overheating at reduced HPCI pump discharge flow, a pump discharge minimum flow line is provided to route the water being discharged from the pump to the suppression pool. On high HPCI flow, stop valve closure, or steam supply valve closure, the valve is closed, and on low flow, provided pump discharge pressure is above a pressure permissive setpoint (indicates pump is running) the valve is opened. The flow transmitter and trip units that measure the pressure difference across a flow element in the HPCI pump discharge pipeline provide the control signal for this valve.



To prevent the HPCI steam supply pipeline from filling up with water and cooling, a condensate drain pot, steam line drain, and appropriate valves are provided in a drain pipeline arrangement just upstream of the turbine supply valve. Upon receipt of a HPCI initiation signal and subsequent steam supply valve opening, the drainage path is isolated. The water level in the steam line condensate drain pot is controlled by a level switch, a flow orifice, and an air-operated steam trap bypass drain valve that allows condensate to flow out of the pot.<sup>90</sup>

The preferred source of water for the HPCI is the CST. The HPCI system will realign to suppression pool suction upon receipt of a CST low level or suppression pool high level signal. Either of these signals open the HPCI suppression pool suction valves HV-55-\*F041 and F042, if closed, which in turn sends a signal to close the CST suction valve HV-55-\*F004 when both are fully open.

Closure of either or both of the steam inboard/out valves requires operator action to properly sequence their opening. An alarm sounds when either of these valves leaves the fully open position.

The HPCI test return to condensate storage line valve HV-55-\*F011 is normally kept closed except during HPCI or RCIC system flow testing. If during testing either a low reactor water level (level 2) or high drywell pressure condition initiates HPCI system operation, valve HV-55-\*F011 and in series test return valve HV-55-\*F008 are automatically closed. In addition, HPCI valve HV-55-\*F011 is automatically closed if one of the HPCI or RCIC pump suppression pool suction valves HV-55-\*F041, HV-49-\*F029 or F031 fully opens. The \*F011 is not automatically closed if the suppression pool to pump suction PCIV, HV-055 \*F042 is open.

#### **3.1.3.1.2 Existing Service and Test Functions**

The TS SRs for the HPCI system are included in the LGS TS 3/4.3.3.

The HPCI system has components that are not activated or tested during normal operation with an integrated testing procedure. These components are tested using manual test methods which allow for independent checking of individual system components. This testing includes verification of flow using the installed return piping such that the turbine and pump are operated. A system functional test, including simulated automatic actuation of the system, with verification that automatic valves in the injection flow path move to the correct position, is also performed. Associated sensors and circuits are monitored to verify proper operation. The frequency of these tests and the parameters to be verified are identified in the Technical Specifications.

The HPCI instrumentation and control system is capable of being tested during normal unit operation to verify the operability of each system component. Testing of the initiation sensors that are located outside the drywell is accomplished by valving out each sensor, one at a time, and applying a test pressure source. This verifies the operability of the sensor. Trip units located in the AER are calibrated individually by a calibration source with verification of setpoint by a digital readout located on the calibration module.

Test jacks are provided to test the logic. Annunciation is provided in the control room whenever a test plug is inserted in a jack to indicate to the control room operator that the HPCI system is in the test status. Operation of the test plug switches can initiate or isolate the HPCI system. Injection into the reactor on an initiation signal is prevented by an interlock, actuated only when the test plug is inserted, which prevents



the opening of one of the HPCI discharge valves. The test can be repeated with the other discharge valve interlocked closed. The manual initiation switch can also be tested at this time. This sequence of tests ensures that all components are tested. A logic test of the HPCI does not interfere with the operation of other ECCS equipment if required by an initiation signal.

During testing, the operation of the HPCI system can be observed in the control room by panel lamps, indicators, recorders, annunciators, and computer printout.<sup>91</sup>

### **3.1.3.1.3 Existing Control Room Indication**

In addition to the control room indications and controls described, a detection system continuously confirms the integrity of the HPCI injection piping to the reactor vessel. If integrity is lost, increasing differential pressure initiates an alarm in the main control room. Pressure in the HPCI pump suction line is monitored by pressure transmitters, which initiate alarms in the control room on high or low suction pressure and also provide signals to indicators in the control room.<sup>92</sup>

### **3.1.3.2 ADS**

The ADS automatically controls five of the Safety Relief Valves (SRVs) that are installed on the main steam lines inside the primary containment.<sup>93</sup> ADS is a Division 1 (ADS A) and Division 3 (ADS C) system (see Table 3.1.3-1) except that only one set of relief valves is supplied. Each relief valve can be actuated by either of two solenoid valves supplying gas to the relief valve operator. One of the solenoid valves is actuated by trip system A and the other by trip system C. Logic relays, manual controls, and instrumentation are mounted so that Division 1 and Division 3 separation is maintained.<sup>94</sup>

The five SRVs associated with the ADS are equipped with remote manual switches so that the entire system can be operated manually as well as automatically. The valves also prevent RCPB over-pressurization by their built-in mechanical action.<sup>95</sup> The valves are dual-purpose in that they relieve pressure by normal mechanical action or by automatic action of an electric-pneumatic control system. The relief by normal mechanical action is intended to prevent over-pressurization of the RCPB. The depressurization by automatic action of the control system is intended to reduce the pressure during a LOCA in which the HPCI system is not available so that the Core Spray system and/or LPCI system can inject water into the reactor vessel.

The control system consists of pressure and water level sensors arranged in trip systems that control dual solenoid valves. The dual solenoid valves control the pneumatic pressure applied to an actuator that controls the SRV directly. An accumulator is included with the control equipment to store pneumatic energy for SRV operation. Cables from the sensors lead to the control structure, where the logic arrangements are formed in cabinets. The electrical control circuitry is powered by dc from the plant safeguard batteries. The power supplies for the redundant control circuits are selected and arranged to maintain tripping ability if there is an electrical power circuit failure. Electrical elements in the control system energize to cause the opening of the SRV. The instrument gas supply to the accumulators is furnished from a seismic Category I gas supply if the normal supply is lost. Seismic Category I backup gas supply is required to be connected at all times during normal operation.<sup>96</sup>



The pressure and level sensors used to initiate ADS are separated from those used to initiate the HPCI system. The ADS function is initiated automatically by low reactor water level and high drywell pressure signals or low reactor water level with the high drywell pressure bypass timer timed out. The ADS function can also be initiated by system-level remote manual switches. In either mode, the ADS valves are prevented from opening unless both pumps in either of the two Core Spray loops, or any of the four RHR pumps, are running. In addition, each individual ADS valve can be opened manually without restriction from permissive sensors.

Reactor vessel low water level (Level 1) is monitored by four level sensors that sense the difference between the pressure due to a constant reference leg of water and the pressure due to the actual height of water in the vessel. Each level sensor provides an input to a trip unit. Two pairs of lines, attached to taps above and below the water level on the reactor vessel, are required for the differential pressure measurement for the level sensors. The lines terminate outside the primary containment and inside the reactor enclosure. They are physically separated from the HPCI sensors and tap off the reactor vessel at points widely separated from the HPCI sensors. These same lines are also used for pressure and water level instruments for other systems. Two additional level sensors are piped individually to confirm reactor vessel low water level (level 3) so that an instrument line break inside containment does not inadvertently initiate auto blowdown. The relay contacts from the trip units are arranged so that a set of sensors sensing low water level initiates the ADS system and a separate pair of sensors initiates the HPCI. This arrangement ensures that no single event due to reactor vessel low water level can prevent the initiation of both the HPCI system and the ADS.

Primary containment pressure is monitored by four pressure sensors that are mounted on instrument racks outside the drywell, but inside the reactor enclosure. Pipes from the drywell interior to the sensors provide the sensing lines. Each drywell high pressure sensor provides an input into a trip unit. The sensors are grouped in a manner similar to the level sensors and are electrically arranged so that no single event due to primary containment high pressure can prevent the initiation of both the HPCI and the ADS systems.

Discharge pressure on the Core Spray and RHR pumps is monitored by twelve pressure sensors; one sensor is at the discharge of each Core Spray pump and two sensors are at the discharge of each RHR pump. Each pressure sensor provides an input to a trip unit.

A timer is used in each of the two ADS trip systems. The time delay setting before actuation of the ADS is long enough so that the HPCI system has time to operate, yet not so long that the LPCI and Core Spray systems are unable to adequately cool the fuel if the HPCI system fails to start. An alarm in the control room is annunciated when either of the timers is timing. Resetting the ADS initiating signals recycles the timers. A manual reset switch is provided in each trip system to reset the timer to delay ADS initiation. Within each trip system, if the reactor level is restored before the timer times out, the timer automatically resets, and auto depressurization is aborted. Should additional reactor level dips occur below the setpoints, the timer is again initiated.<sup>97</sup>

Two initiation signals and one permissive signal are used for the ADS: reactor vessel low water level; drywell high pressure; and RHR and/or Core Spray pumps running. If all signals are present, the ADS SRVs will open after the ADS timer runs out. If the high drywell pressure signal is not present, the ADS SRVs can open after the high drywell pressure bypass timer and ADS timer run out. There are two reactor



vessel low water level signals associated with the ADS system; one (Level 3) prevents undesired system operation, and the other (Level 1) initiates the ADS. Primary containment high pressure indicates a breach in the RCPB inside the drywell. A permissive signal indicating RHR or Core Spray pump discharge pressure is also required. Discharge pressure on any one of the RHR pumps or both pumps of either Core Spray loop is sufficient to give the permissive signal, which permits automatic depressurization when the LPCI or Core Spray systems are operating.

The ADS is composed of four logics, arranged with the A and E logics in ADS trip system A and the C and G logics in ADS trip system C. Each trip system controls one of the two solenoid valves associated with each SRV. As shown in Figure 3.1.3.2-1, both logics in a trip system must be enabled to energize the solenoid valves associated with that trip system. The logic represented in Figure 3.1.3.2-1 will be replaced by the Common Q Platform implementation.

After receipt of the initiation signals and a delay provided by timers, one or both of the solenoid valves are energized. This allows pneumatic pressure from the accumulator to act on the cylinder operator. The pneumatic cylinder operator holds the relief valve open. Lights in the control room indicate when the solenoid valves are energized to open an SRV.

Manual reset circuits are provided in the ADS initiation logic. By manually resetting the initiation signal, the delay timers are recycled. The operator can use the reset push buttons to delay or prevent the automatic opening of the relief valves if such delay or prevention is prudent.

A manual inhibit switch is provided in each division of the ADS initiation logic. By placing this switch in the inhibit position, the automatic depressurization will be inhibited, and it will be indicated by a white status light and annunciator window in the control room. If the ADS has already begun and is sealed-in, the inhibit switch does not break the seal-in and does not terminate the ADS.

Once opened by an ADS initiation, the ADS SRVs will return to their normal (closed) position if both ADS reset buttons dedicated to valve closure are depressed. If, however, the ADS initiating signal has not reset or the signal recurs, a subsequent time-delayed ADS trip and valve opening logic sequence will commence.

Control switches are available in the control room for manual operation of each SRV, including each ADS valve.

The ADS has two independent and redundant trip systems as shown in Table 3.1.3-1 with redundant initiating trip circuits. Each trip system controls one of the two independent and redundant solenoid valves associated with each ADS valve.<sup>98</sup> Division 1 sensors for low reactor water level and high drywell pressure initiate ADS A, and Division 3 sensors initiate ADS C.<sup>99</sup>



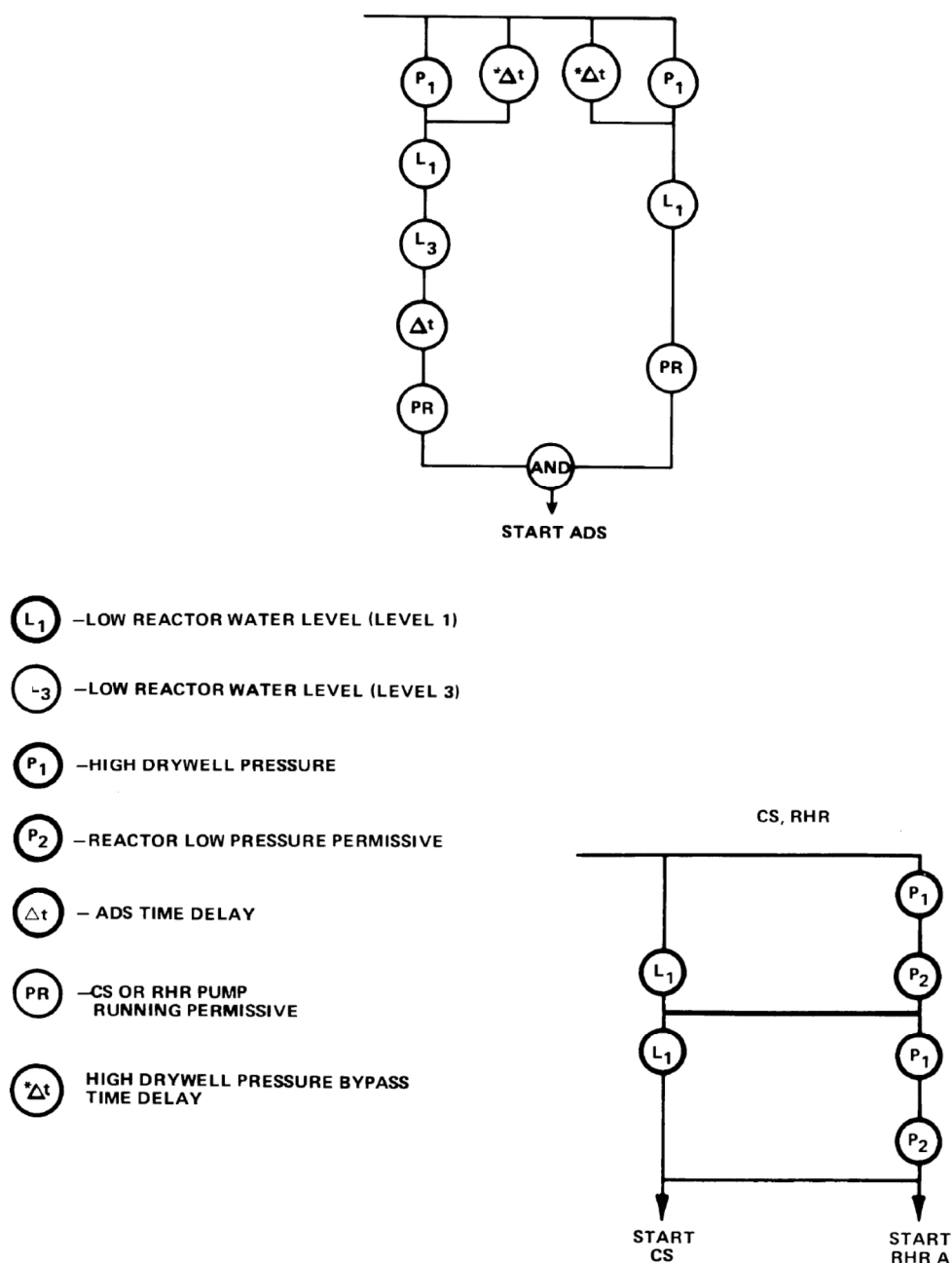


Figure 3.1.3.2-1 System Level Automatic Initiation Logic – ADS, Core Spray (CS in figure), RHR<sup>100</sup>

### 3.1.3.2.1 ADS Bypasses and Interlocks

It is possible for the operator to manually delay the depressurizing action by the trip system reset switches. This would reset the timers to zero seconds and prevent depressurization until the timers have timed out. The operator would make this decision based on an assessment of other plant conditions.



The high drywell pressure bypass timer is actuated on low water level (Level 1). When this timer runs out, the high drywell pressure trip is bypassed, and the ADS timer is initiated on low water level alone. If the low water level signal clears before the high drywell pressure bypass timer runs out, the bypass timer will automatically reset.

ADS is interlocked with the Core Spray and RHR systems by pressure sensors located on the discharge of these pumps. This interlock ensures that at least one of the RHR pumps or both pumps of either Core Spray loop are capable of delivering water into the vessel.<sup>101</sup>

#### **3.1.3.2.2 Existing Service and Test Functions**

The TS SRs for the ADS are included in the LGS TS 3/4.3.3.

The ADS has two divisional trip systems, and either one can initiate automatic depressurization. Each trip system has two trip logics, both of which must trip to initiate ADS. Four test jacks are provided, one in each trip logic. During testing, only one trip logic is actuated at a time to prevent spurious ADS operation. The test plug switch disables one trip logic of a trip system while the other is undergoing test. Actuation of appropriate trip units in the trip logic being tested closes one of the two series relay contacts in the valve solenoid circuit. This causes a panel light to come on, indicating proper trip logic operation and also continuity of the solenoid electrical circuit. Testing of the other trip logic and trip system is similar. Annunciation is provided in the control room whenever a test plug is inserted in a jack to indicate to the reactor operator that the ADS is in a test status. Testing in one division of the ADS does not interfere with automatic operation of the other division if required by an initiation signal.

Integrated testing of the ADS solenoid valves and circuitry is not performed with the plant operating at power, which is consistent for safety systems where the final actuating device(s) would cause temporary modification of plant processes such as fluid injection or discharge. The Technical Specifications provide for a functional partially integrated test without valve actuation. The transmitter/ trip units that provide sensory inputs to the ADS are checked by station personnel. The logic chain up to the solenoid is tested by manually inserting a trip signal and observing the trip logic lights which indicate both continuity of the solenoid circuit and proper trip logic operation.<sup>102</sup>

#### **3.1.3.2.3 Existing Control Room Indication**

Recorders and indicators in the control room provide information regarding reactor water level and drywell pressure. Each manual and automatic ADS input is provided to the annunciator system. Annunciation is also provided on initiation of the ADS timers, tripping of each logic, and system out-of-service indication. All interface with the annunciator system is through isolated contacts.<sup>103</sup>

#### **3.1.3.3 Core Spray System**

Core Spray (CS) is a four-pump, two-loop system that is backed up by the four-loop LPCI mode of the RHR system. The Core Spray system two spray loops are independent and redundant.<sup>104</sup> Each loop includes two ac motor-driven pumps, each with a separate suction path from the suppression pool, necessary control and instrumentation devices and valves, and a discharge path connected directly to the



reactor which is common to both pumps.<sup>105</sup> Each of the four pumps has its own independent logic and control power.<sup>106</sup>

The circuitry for the Core Spray pumps provides for detection of normal power available, so that all pumps are automatically started in sequence. Each pump can be manually controlled by a control room remote switch or the automatic control system.<sup>107</sup>

Trip units associated with two reactor vessel low water level sensors and two drywell high pressure sensors in conjunction with two reactor low pressure sensors are electrically connected in a one-out-of-two-twice arrangement for each Core Spray pump, so that no single event can prevent initiation of Core Spray. The following discussion describes the initiation and operation of the 'A' core spray loop. The 'B' loop is initiated and operated similarly and independently of the 'A' loop. The 'A' loop is automatically initiated when a LOCA condition (low reactor vessel level or high drywell pressure coincident with low reactor vessel pressure) exists. The 'A' core spray loop can also be manually initiated by arming and depressing the 'A' and 'C' core spray initiation switches ('B' & 'D' switches for B loop).

Upon receipt of either of the above loop initiation signals in their respective divisions of initiation logic, the 'A' and 'C' core spray pumps start automatically, the core spray test return line to the suppression pool is automatically isolated, and a signal to open the inboard and outboard loop injection valves is initiated. However the normally-closed inboard injection valve (also referred to as the injection valve) and the normally-open outboard injection valves are interlocked to prevent opening if reactor pressure is greater than the pressure permissive setpoint (determined by monitoring reactor pressure) or if power is not available at the 4 kV bus to which the 'A' core spray pump is connected.

When the 4 kV bus is energized and reactor pressure has decreased to below the pressure permissive setpoint the injection valves will automatically open. The pressure permissive setpoint prevents over-pressurizing the low pressure portions of core spray.

Each of the components in the core spray flow path can also be manually operated from the control room by means of the component's individual control switch. The inboard injection valve is interlocked to prevent opening unless either:

- its respective loop initiation signal with 4kV power and pressure permissive is present (as described above), or
- the associated outboard injection valve is closed.

Three initiating variables are used for the Core Spray system: reactor vessel low water level; drywell high pressure; and reactor vessel low pressure.<sup>108</sup>

Reactor vessel low water level is monitored by eight level sensors that sense the difference between the pressure that is due to a constant reference leg of water and the pressure that is due to the actual height of water in the vessel. Each level sensor provides an input to a trip unit located in the control structure. The lines terminate outside the primary containment and inside the reactor enclosure.<sup>109</sup>



Drywell pressure is monitored by eight sensors mounted on instrument racks in the reactor enclosure. Four sensing lines that terminate in the reactor enclosure allow the sensors to measure the drywell interior. Each drywell high pressure sensor provides an input to a trip unit located in the control structure.

Reactor pressure is monitored by twelve pressure sensors mounted on racks in the reactor enclosure. Four of the pressure sensors are used to develop system initiation signals, four are used in development of injection valve open-permissive interlocks, four provide inputs to both system initiation and injection valve open-permissive interlock logic. Four sensing lines that terminate in the reactor enclosure allow the sensors to measure the reactor vessel. Each pressure sensor provides an input to a trip unit located in the control structure.

The LOCA signal that initiates the Core Spray also initiates the corresponding diesel generator.<sup>110</sup> If offsite power is available to the Class 1E 4 kV buses, these breakers (except for the RHR pump motor feeder breakers and the incoming source breakers) are tripped for load shedding. For a total loss of offsite power (LOOP), all Class 1E 4 kV breakers are tripped. Load sequencing is accomplished by using time-delays on individual breaker control circuits.

Non-Class 1E 440 V loads that are fed from Class 1E Motor Control Centers (MCCs) use a shunt trip device on the MCC breaker or a trip logic in the combination starter controls to isolate the circuit on a LOCA signal from the unit from which they are powered.<sup>111</sup>

The Core Spray initiation logic is a one-out-of-two-twice network using level and pressure sensors. The initiation signal is generated when:

- a. Both level sensors are tripped.
- b. Four pressure sensors are tripped (two high drywell pressure and two low reactor vessel).
- c. Either of two combinations of one level sensor and two pressure sensors (one high drywell and one low reactor vessel) are tripped.

The Core Spray system can also be manually initiated.

Once an initiation signal is received by the Core Spray control circuitry, the signal is sealed-in until manually reset. The pressure permissive signal for opening the respective injection valve is provided by four division (1) or four division (2) pressure sensors that monitor reactor vessel pressure. Two of these sensors are the ones to initiate the Core Spray system in conjunction with high drywell pressure. The other two sensors are located on the same sensing lines and provide signals to trip units located in the control structure. These pressure signals are arranged in a one-out-of-two-twice logic.<sup>112</sup>

The testable check valves are the only control and instrumentation components for the Core Spray system that are located inside the primary containment that must operate in the environment resulting from a LOCA. All other components of the Core Spray system that are required for system operation are outside the drywell and are selected in consideration of the normal and accident environments in which they must operate.<sup>113</sup>

#### **3.1.3.3.1 Core Spray Bypasses and Interlocks**



The Core Spray pump motors and inboard injection valves are provided with manual override controls that allow the operator to control the system following automatic initiation.

A pressure transmitter is installed upstream of each pump discharge check valve. These pressure signals are used in the ADS to indicate that core spray pumps are running, allowing actuation of the ADS.

The Core Spray initiation signal also initiates the corresponding diesel generator and is used to trip the drywell chillers.<sup>114</sup>

To meet LGS licensing basis commitment to BTP ICSB 3, the normally closed core spray inboard injection valves and the normally open outboard injection valves are interlocked by high reactor pressure (one-out-of-two-twice logic) to prevent their receiving an opening signal on automatic system initiation. The inboard injection valve is interlocked by limit switch with outboard injection valve position to permit testing, such that it may be opened manually only if the outboard valve is closed. The outboard valve is interlocked so that during an automatic CS system initiation, the outboard valve close circuit will be disabled.<sup>115</sup>

#### **3.1.3.3.2 Existing Service and Test Functions**

The TS SRs for the Core Spray System are included in the LGS TS 3/4.3.3.

The Core Spray System has components that are not activated or tested during normal operation with an integrated testing procedure. The components are tested using manual test methods which allow for independent checking of individual components. This testing includes verification of flow using the installed test piping such that the motors and pumps are operated. A system function test, including automatic actuation of the system, with verification that automatic valves in the injection flow path move to the correct position, is also performed. Associated sensors and circuits are monitored to verify proper operation. The frequency of these tests and the parameters to be verified are identified in the Technical Specifications.

The Core Spray system is capable of being tested during normal operation by an overlapping series of tests. All sensors are individually valved out of service and subjected to a test pressure. This verifies the operability of the sensors as well as the calibration range. The trip units mounted in the AER are calibrated individually by a calibration source with verification of setpoint by a digital readout located on the calibration module.

Test jacks are provided to test the logic. Annunciation is provided in the control room whenever a test plug is inserted in a jack to indicate to the control room operator that the Core Spray system is in the test status. Operation of the test plug switches initiates the system. Injection into the reactor is prevented by an interlock actuated when the test plug is inserted. This will prevent the automatic opening of either the inboard or the outboard injection valve, depending on the position of the test switch that is used to select which valve to test. The manual initiation switches can also be tested. This sequence of tests ensures that all components are tested. A logic test of one Core Spray loop does not interfere with the operation of the other Core Spray loop if required by an initiation signal.



During testing, Core Spray operation can be observed in the control room by panel lamps, indicators, recorders, annunciators, and computer printout.<sup>116</sup>

### 3.1.3.3 Existing Control Room Indication

Sufficient temperature, flow, pressure, and valve position indications are available in the control room for the operator to accurately assess Core Spray system operation. Valves have indications of fully open, intermediate, and fully closed position. The pump has indications for pump running and pump stopped. A detection system continuously confirms the integrity of the Core Spray A and B injection line piping to the reactor vessel. A differential pressure sensor measures the pressure difference between the two injection lines. If the Core Spray A and B piping is sound, the pressure difference will be very small between these lines. If integrity is lost, an increase in differential pressure initiates an alarm in the control room. Pressure in each Core Spray pump suction line is monitored by a local pressure indicator to determine suction head and pump performance. Pressure in the discharge line of each Core Spray loop is monitored by a pressure indicator in the control room to determine pump performance.<sup>117</sup>

### 3.1.3.4 LPCI Mode of RHR System

LPCI is an operating mode of the RHR system. The LPCI mode of the RHR system is designed to provide water to the reactor vessel following the design basis LOCA.<sup>118</sup>

Control and instrumentation required for the operation of the LPCI mode are electric Class 1E and seismic Category I.

LPCI, an operating mode of the RHR system, consists of four independent and redundant loops. Each loop contains a separate suction path from the suppression pool, a motor-driven pump, necessary control and instrumentation devices and valves, and a separate injection path that discharges directly into the reactor. Except for the LPCI testable check valves, the components pertinent to LPCI operation are located outside the primary containment.

LPCI is arranged for automatic operation and for remote manual operation from the control room. The equipment provided for manual operation of the system allows the operator to take action independent of the automatic controls if there is a LOCA.<sup>119</sup>

Two automatic initiation signals are provided for the LPCI mode of operation of the RHR systems:

- Reactor vessel low water level and
- Drywell high pressure with a reactor vessel low pressure permissive.

Either will initiate the LPCI mode of operation. The same sensors and trip units used for initiation of the Core Spray system are used to initiate LPCI. The low water level or high drywell pressure coincident with reactor low pressure initiation signal for LPCI is a one-out-of-two-twice arrangement.

The LPCI mode is not required for normal operation. When it is required for accident conditions, it is initiated automatically. No operator action is required for at least 10 minutes following initiation. The operator may manually control the RHR system after a 3 minute delay (for the RHR heat exchanger



bypass valve open command timers) to use its capabilities in the other modes of the RHR system, provided the core is being cooled by other portions of the ECCS.<sup>120</sup> Each of the components in the LPCI flow path can also be manually operated from the control room by means of each component's individual control switch.<sup>121</sup>

#### **3.1.3.4.1 LPCI Bypasses and Interlocks**

LPCI valve is interlocked to prevent opening if reactor pressure is greater than the RHR piping design maximum pressure. The interlocks and control devices used in this manner are the same as those used for automatic operation.<sup>122</sup>

The valves that allow the diversion of water for suppression pool spray are automatically closed upon receipt of an LPCI initiation signal. The manual controls for these valves are interlocked so that opening the valves by manual action is not possible unless the reactor vessel injection valve in its respective RHR loop is closed or the LPCI initiation signal is not present.

The valves that allow diversion of water for containment spray are normally closed. The manual controls for these valves are interlocked so that opening both valves in one drywell spray loop by manual action is not possible unless an LPCI initiation signal is present, the reactor vessel injection valve in its respective RHR loop is closed, and drywell pressure is high.<sup>123</sup>

For RHR to meet LGS licensing basis BTP ICSB 3, RHR shutdown cooling suction outboard and inboard valves are two manually activated MOVs in series. Both valves are inhibited from opening and close automatically if primary system pressure is above setpoint. Reactor pressure is also indicated in the control room. The logic components for both valves are independent. Each valve control circuit requires two reactor low pressure permissives before valves can open; this results in a four-out-of-four logic to open the suction line. Removal of one signal (one-out-of-four logic) isolates the line. The pressure permissive components rely on the transmitter trip unit combination which is testable from the control room.<sup>124</sup>

RHR shutdown cooling injection outboard valves are manually activated MOVs in series with testable check AOVs. These MOVs (loop A and B) are inhibited from opening and close automatically if primary system pressure is above setpoint. Both valves use the same valve control circuit, which requires two reactor low pressure permissives before the valves can open. Removal of one pressure permissive signal will close the valves.

#### **3.1.3.4.2 Existing Service and Test Functions**

The LPCI mode of the RHR system has components that are not activated or tested during normal operation with an integrated testing procedure. These components are tested using manual test methods which allow for independent checking of individual system components. This testing includes verification of flow using the installed test piping such that the motors and pumps are operated. A system function test, including automatic actuation of the system, with verification that automatic valves in the injection flow path move to the correct position, is also performed. Associated sensors and circuits are monitored to verify proper operation. The frequency of these tests and the parameters to be verified are identified in the Technical Specifications.



Test jacks are provided to test the logic. Annunciation is provided in the control room whenever a test plug is inserted in a jack to indicate to the control room operator that the RHR system is in the test status. Operation of the test plug switches initiates LPCI. Injection into the reactor is prevented by an interlock, actuated only when the test plug is inserted, which prevents the opening of the LPCI discharge valve. After the RHR pump is tripped, the LPCI discharge valve can be opened to ensure its operability. The manual initiation switches can also be tested. This sequence of tests ensures that all components are tested. A logic test of one LPCI loop does not interfere with the operation of the other LPCI loops if required by an initiation signal.

During testing, LPCI operation can be observed in the control room by panel lamps, indicators, recorders, annunciators, and computer printout.<sup>125</sup>

#### **3.1.3.4.3 Existing Control Room Indications**

Sufficient temperature, flow, pressure, and valve position indications are available in the control room for the operator to accurately assess the LPCI system operation. A detection system continuously confirms the integrity of the injection line piping to the reactor vessel. Differential pressure sensors sense the pressure differential between injection lines of RHR A and C loops and between the B and D loops. If the piping is sound, the pressure differential is very small between these lines. If integrity is lost, an increase in differential pressure initiates an alarm in the control room. Valves have indications of fully open, intermediate, and fully closed positions. Pumps have indications for pump running and pump stopped.<sup>126</sup>

### **3.1.4 Reactor Core Isolation Cooling System**

The RCIC system is a safety system that consists of a turbine, pump, piping, valves, accessories, and instrumentation designed to ensure that sufficient reactor water inventory is maintained in the reactor vessel to permit adequate core cooling to take place. This prevents reactor fuel overheating during the following conditions: a. The vessel is isolated and maintained in the hot standby condition. b. The vessel is isolated, accompanied by loss of coolant flow from the reactor feedwater system. c. A complete plant shutdown under conditions of loss of normal feedwater system is started before the reactor is depressurized to a level at which the shutdown cooling system can be placed into operation.

Following a reactor scram, steam generation continues at a reduced rate due to the core fission product decay heat. At this time the turbine bypass system diverts the steam to the main condenser, and the feedwater system supplies the makeup water required to maintain the reactor vessel inventory.

If the reactor vessel is isolated and the feedwater supply is unavailable, relief valves are provided to automatically (or remote manually) maintain vessel pressure within desirable limits. The water level in the reactor vessel drops due to continued steam generation by decay heat. On reaching a predetermined low level, the RCIC system is initiated automatically. The system then functions to restore adequate vessel water levels. On reaching a predetermined high level, the RCIC steam admission valve (F045) automatically closes, resulting in turbine shutdown. RCIC will automatically restart if the level returns to the low level trip point. The turbine-driven pump supplies makeup water from the CST to the reactor vessel. If the CST level falls below a predetermined low level, an alternate source of water is automatically made available from the suppression pool. The turbine is driven with a portion of the decay heat steam from the reactor vessel, and exhausts to the suppression pool. Suppression pool water may not



be of condensate quality and hence it is preferred that it only be used if sources of condensate quality water are not available.

During RCIC operation, the suppression pool acts as the heat sink for steam generated by reactor decay heat. This results in a rise in pool water temperature. The RHR system heat exchangers are used to maintain pool water temperature within acceptable limits by cooling the pool water.

For design basis events RCIC needs to operate for a maximum of six hours in order to fulfill its safety functions.

RCIC is automatically initiated when RPV Level decreases to the Level 2 setpoint. It can also be manually initiated. The RCIC system meets the following design criteria:

- a. Sufficient coolant can be maintained in the reactor vessel in case of an isolation with a loss of main feedwater flow.
- b. Provisions are made for automatic and remote manual operation of the system.
- c. Components of the RCIC system are designed to satisfy seismic Category I design requirements.
- d. The power supply for the system is from immediately available energy sources of high reliability.
- e. Provision is made so that periodic testing can be performed during plant operation.

The RCIC system is designed to initiate and discharge, within 55 seconds, a specified constant flow into the reactor vessel over a specified pressure range. The temperature of the RCIC water discharged into the reactor vessel varies between 40°F and 140°F. Station Blackout (SBO) procedures direct the operation of the RCIC System for Reactor Pressure Level Control for the SBO 4-hour coping duration with water supply from the Suppression Pool. During the SBO event, the Suppression Pool water may reach up to 180 degrees F. The mixture of the cool RCIC water and the hot steam accomplishes the following:

- a. Quenches the steam
- b. Removes reactor residual heat by reducing the heat level (enthalpy) due to the temperature difference between the steam and water
- c. Replenishes reactor vessel inventory

The HPCI system performs the same functions, thereby providing single failure protection. Both systems use different electrical power sources of high reliability, which permits operation with either onsite or offsite power.

The RCIC system design includes interfaces with redundant leak detection devices:

- a. A high pressure drop across a flow device in the steam supply line equivalent to 300% of the steady-state steam flow at 1197 psia
- b. A high area temperature, using temperature switches as described in the leak detection system; high area temperature is alarmed in the control room
- c. A high pressure between the turbine exhaust rupture diaphragms
- d. Reactor low pressure



These devices, activated by the redundant power supplies, automatically isolate the steam supply to the RCIC turbine.

The RCIC system is located in a different area of the reactor enclosure and uses different divisional power (with separated electrical routings) than its redundant system (HPCI).

Two RCIC lines penetrate the primary containment and form a part of the Reactor Cooling Pressure Boundary. The first is the RCIC steam supply line, which branches off the B main steam line between the reactor vessel and the inboard MSIV. This line has two automatic motor-operated isolation valves, which are key-locked open. One is located inside and the other outside primary containment.

The RCIC pump discharge line is the other line that forms a part of the Reactor Cooling Pressure Boundary; however, it indirectly connects to the Reactor Pressure Vessel.

The RCIC pump suction line, minimum flow pump discharge line, turbine gland seal system vacuum pump discharge, and turbine exhaust line all penetrate the primary containment and terminate below the suppression pool water level.<sup>127</sup>

For Unit 1, ten ambient temperature elements are installed in the RCIC pipe chase areas. Five sensors are associated with each auto-isolation logic division. For Unit 2, eight ambient temperature elements are installed in the RCIC pipe chase areas. Four sensors are associated with each auto-isolation logic division. Seven temperature elements are installed in the RCIC equipment compartment. Four of these elements form two differential temperature pairs which monitor high ventilation air differential temperature. One pair is associated with one logic division and the other pair is associated with the other logic division. The other three temperature elements monitor the RCIC pump compartment ambient temperature. One ambient temperature element is associated with one logic division and the other two ambient temperature elements are associated with the other logic division.<sup>128</sup>

Closure of the outboard RCIC steam supply isolation valve and steam line warm-up isolation valve is controlled by one logic division and the inboard steam supply isolation valve by the other logic division.

Two instrumentation channels are provided to ensure protective action when required.

In order to close both the inboard and outboard isolation valves, both logic divisions must trip. Protection against inadvertent isolation due to instrumentation malfunction is not required or provided.<sup>129</sup>

#### **3.1.4.1 Bypasses and Interlocks**

The following electrical interlocks are provided:

- a. There are four key-locked valves (F007, F008, F060, and F002) and two key-locked resets (the isolation resets).
- b. Limit switches on valves F029 and F031 activate such that when both valves are fully open, F010 closes.
- c. A limit switch on valve F060 activates when fully open and clears a permissive so valve F045 can open.



- d. The limit switch on valve F045 actuates when F045 is partially open. The limit switch causes the valve to stop at the partially open position and also initiates a time delay relay. The valve remains in the partially open position until the time delay relay times out and activates the opening of the F045 valve. The time delay relay also initiates the ramp generator.
- e. A limit switch on valve F045 activates when F045 is not fully closed, initiates startup ramp function and acts to lock out the following alarms for 15 seconds: RCIC pump low flow, RCIC low oil pressure, and RCIC vacuum tank low vacuum. This ramp resets each time F045 is closed.
- f. The F045 limit switch activates when fully closed to permit valves F004, F005, F025, and F026 to open and causes valves F013 and F019 to close.
- g. The turbine trip throttle valve (part of the turbine assembly) limit switch activates when fully closed and causes valves F013 and F019 to close.
- h. The combined pressure switches at reactor low pressure and high drywell pressure, when activated, close valves F080 and F084.
- i. High turbine exhaust pressure, low pump suction pressure, or an isolation signal, actuate to close the turbine trip throttle valve; when the signal is cleared, the trip throttle valve must be reset from the control room.
- j. 124% overspeed trips both the mechanical trip at the turbine and the trip throttle valve; the former is reset at the turbine, and then the latter is reset in the control room
- k. An isolation signal closes valves F007, F008, F076, and other valves, directly or indirectly, as noted in items f and h above.
- l. An initiation signal opens valves F010 (if closed), F013, and F046; starts the barometric condenser vacuum pump; and causes valve F022 to close, if open.
- m. A high RCIC steam line drain pot level signal causes valve F054 to open. The valve recloses when the high level signal clears.
- n. The combined signal of low flow plus pump discharge pressure opens and, with increased flow, closes valve F019. See also items e and f above.
- o. The switches for reactor low pressure, high turbine exhaust diaphragm pressure, steam line high differential pressure, or high area temperature, when activated, close valves F007, F008 and F076.
- p. Limit switches on valves F029 and F031 activate such that when either valve is open, F022 closes.
- q. High water level in the reactor vessel (level 8) initiates closure of the F045 and F046 valve

RCIC Test Loop Operation is manually initiated by the operator. Operator action is required as defined by surveillance test procedures and system operating procedures. The RCIC test return shares a common path with the HPCI system and is unusable if a HPCI initiation signal is present due to HPCI injection interlocks prevailing.

The manual bypass switch bypasses the temperature leak detection signal from the RCIC isolation logic. The RCIC isolation is arranged such that a trip of any one of the temperature indicating switches results in RCIC isolation and RCIC turbine trip. The bypass switch allows testing without isolating the RCIC system. Administrative control is provided by a two-position key-lock bypass switch, with the key removable in the normal position. Separate switches are provided for each of the redundant divisions.

Each RCIC-LDS temperature monitor point has bypass capabilities, but this function is not used.



Divisional level of bypass is indicated automatically in the control room when the respective divisional switch is placed in bypass position. System level annunciation of "RCIC system out-of-service" is automatically annunciated in the control room when either of the bypass switches is placed in the bypass position.

The RCIC isolation function will still be available from the redundant logic. Manual capability to actuate system level annunciation of "RCIC system out-of-service" is provided by separate NORMAL-INOP switches for the redundant divisions. Annunciation will occur when either of the divisional switches is placed in the INOP position.<sup>130</sup>

#### **3.1.4.2 Existing Control Room Indication**

When parts of the RCIC system have been bypassed or otherwise deliberately rendered inoperable. These conditions are automatically indicated in the control room at the system level. Capability for manual initiation of system level indication exists for items not readily automated.

When any one monitored temperature reaches its setpoint, an RCIC auto-isolation signal is initiated and an annunciator activated in the control room.<sup>131</sup>

#### **3.1.5 Standby Liquid Control System**

The instrumentation and controls for the Standby Liquid Control System (SLCS) are designed to initiate and continue injection of a liquid neutron absorber into the reactor when manually initiated or automatically initiated by the RRCS. This equipment also provides the necessary controls to maintain this liquid chemical solution well above saturation temperature in readiness for injection.

The instrumentation and controls are also designed to provide sufficient sodium pentaborate to the reactor vessel to maintain suppression pool pH at 7.0 or greater following a LOCA when manually initiated.<sup>132</sup>

The SLCS process equipment and controls essential for post LOCA pH control in accordance with Regulatory Guide 1.183 (AST) are designed to Seismic Category I criteria and controls are Class 1E.<sup>133</sup>

The SLCS pumps, valves, heaters, and associated controls are powered from Class 1E power supplies. The power supply to the explosive operated injection valves and injection pumps are from separate emergency buses. The power supply to both the control room bench board indicator lights and the level and pressure sensors is powered from an emergency instrument bus.<sup>134</sup>

SLCS operates automatically when both channels A and B of either RRCS (division are tripped). This will change to 2oo4 with the non-safety implementation of RRCS. Normally only SLCS pumps A and B are aligned to receive the start signal (key-lock switches in the normal position) with SLCS pump C automatic start signal blocked (key-lock switch in the stop position and the key removed). However, when either the A or B SLCS pump is out-of-service, then the C SLCS pump can be aligned to receive the automatic start signal (key-lock switch positioned to normal). For the Digital Modernization Project, the keylock switches become soft controls on the PPS Safety Displays. Only by administrative procedure is a 3-pump automatic alignment prevented. For the Digital Modernization Project the DCS will automatically prevent this 3-pump automatic alignment.



For automatic operation, all SLCS pumps aligned for automatic start receive a start signal and their associated squibs fire, on their injection valve, when both channels A and B of either RRCS division are tripped..

The SLCS is provided with instrumentation and control (now in the PPS) to automatically shut off the SLCS pumps when the solution level in the storage tank is below the low level limit. This low level pump shutoff signal is provided by two-out-of-two logic (now 2oo3 logic in the PPS). Three sets of storage tank level monitoring devices are provided to automatically shut off the SLCS pumps. Each set consists of two independent transmitters and trip units. There is a separate external line for each set of transmitters; this prevents a single instrument line problem from affecting all three SLCS pumps.<sup>135</sup>

### **3.1.5.1 SLCS Bypasses and Interlocks**

Initiation of SLCS pump A or C will close the inboard isolation valve of the RWCU system. Initiation of SLCS pump B will close the RWCU outboard isolation valve.<sup>136</sup>

### **3.1.5.2 Existing SLC Service and Test Functions**

The instrumentation and control system of the SLCS is tested when the system test is performed (see UFSAR Section 9.3.5)<sup>137</sup>

### **3.1.5.3 Existing Control Room Indications**

The SLCS is automatically initiated by the RRCS or manually initiated by keylocked switches located in the control room. The SLCS pumps will automatically stop on SLC storage tank low level or they may be stopped manually from the key-locked switches after an automatic initiation.<sup>138</sup> Manual initiation and control will migrate to soft control on the PPS Safety Displays.

After the SLCS is initiated, the operator has several indicators and alarms to determine proper system operation. Indicator lights show which system was initiated, explosive valve continuity, isolation valve position, and inboard maintenance valve position. The control room annunciators indicate:

- a. Isolation valve not fully open
- b. Loss of continuity to the squib valves
- c. SLCS storage tank Hi/Lo temperature
- d. SLCS storage tank Hi/Lo level
- e. SLCS A, B or C pump motor overload or loss of power.

Analog information is also available for the storage tank level and for pump pressures. At the local panel, additional operator information is available, such as storage tank level, system pressure, and storage tank temperature.<sup>139</sup>



Monitoring of SLCS operational status will migrate to the PPS Safety Displays.

### 3.1.6 RRCS

The RRCS consists of vessel pressure and level sensors, solid-state logic, control room cabinets and indications, and interfaces with several systems actuated to mitigate an ATWS event. The solid-state logic is divided into Divisions 1 and 2, each of which is subdivided into channels A and B. The logic is energized to trip, and both channels A and B of either division must be tripped to initiate the RRCS protective actions. The system can be manually initiated by depressing two push buttons (tripping both channels A and B) in the same division. This manual initiation function is designed so that no single operator action can result in an inadvertent initiation. The push button collar must be rotated to arm the switch before depressing will trip the logic. The manual initiation push buttons are located in the control room near the RPS manual scram push buttons. There are four RRCS manual initiation push buttons.<sup>140</sup>

The system consists of control panels, their associated ATWS detection and actuation logic, and the necessary interface logic to the recirculation system, the feedwater system, the SLCS, the RWCU system and the ARI components of the CRD system required to perform specific functions in response to an ATWS event. The RRCS is completely separate and diverse from the RPS to provide mitigation of the potential consequences of an ATWS event.<sup>141</sup>

RRCS Division 1, channels A and B are powered by the 125 V dc Bus A (Division 1), and RRCS Division 2, channels A & B are powered from 125 V dc Bus B (Division 2). The power supplies to the RRCS functions are available during all potential ATWS initiating events, including those events involving loss of normal power supplies.<sup>142</sup>

#### 3.1.6.1 RRCS Bypasses and Interlocks

There is no RRCS bypass or operating bypass.<sup>143</sup>

#### 3.1.6.2 RRCS Reset

Each RRCS channel can be manually reset by depressing the RRCS reset push buttons (four, one for each tripped channel), provided that a specified time delay has elapsed since RWCU isolation and SLCS initiation. When the RRCS is reset, the following seal-in signals are broken:

- a. RWCU isolation
- b. Low water level 2
- c. Manual initiation
- d. High reactor pressure
- e. Feedwater runback signal
- f. SLCS initiation

The RRCS ARI function is reset by the RRCS ARI reset push buttons. This second set of four push buttons (one for each channel) will enable the reset of the ARI logic 30 seconds after initiation of ARI, provided that initiating signals have cleared. This 30 second time delay before the ARI reset permissive appears is designed to ensure that the RRCS ARI scram goes to completion.<sup>144</sup>



### 3.1.6.3 RRCS Service and Test Functions

The RRCS is continually checked by a solid-state microprocessor based self-test system. This self-test system checks the RRCS sensors, logic, and protective devices and itself.<sup>145</sup>

## 3.2 PPS - NEW SYSTEM ARCHITECTURE (D.2.2)

Collectively, the logic circuits for RPS, PCRVICS, and ECCS are integrated into one safety system referred to as the Plant Protection System (PPS). The architecture of the PPS integrates the logic processing for the functions of RPS, ECCS, PCRVICS (also referred to as Nuclear Steam Supply Shutoff System or NSSSS), RCIC, and manual initiation of SLCS into a common system. The architecture (Figure 3.2-1) consists of the following channel/division configurations in accordance with the definition of Channel and Division in IEEE Std 603:

- Four Channels of bistable processing
- Four Divisions of voting logic and actuation

The logic for the following safety systems comprises the PPS:

- Reactor Protection System (RPS)
- Emergency Core Cooling System (ECCS):
  - High Pressure Coolant Injection (HPCI) System
  - Residual Heat Removal (RHR) including Low Pressure Coolant Injection (LPCI), shutdown cooling, and several other previously manual modes
  - Automatic Depressurization System (ADS)
  - Core Spray (CS)
  - Emergency Diesel Generator (EDG) divisional start function
- PCRVICS (NSSSS)
- Reactor Core Isolation Cooling (RCIC)
- Manual initiation of SLCS

The Common Q<sup>TM</sup> platform is used for the PPS architecture. This platform is described in WCAP-16097, “Common Qualified Platform Topical Report” (Reference 4).

The PPS performs the following functions:

- Acquires and analyzes sensor inputs required for RPS, NSSSS, and ECCS actuation calculations
- Performs computations and logic operations on variables based on acquired inputs
- Performs coincidence logic voting
- Initiates a Reactor Trip (SCRAM) via the SCRAM termination matrix
- Provides NSSSS and ECCS actuation commands to applicable components
- Permits manual SCRAM/trip or bypasses of each individual automatic safety function
- Provides indication and annunciation signals
- Provides data to external systems
- Performs the high pressure low pressure interlock in accordance with BTP ICSB 3<sup>146</sup>



- Enables Emergency Operating Procedure (EOP) or Severe Accident Guideline (SAG) overrides of system interlocks to allow operation of specific equipment under administrative control

Figure 3.2-1 shows the functions of each level of the PPS architecture in the respective channel/division pairing in greater detail.



a,c

5

**Figure 3.2-1 PPS 3-Level Architecture**



The PPS architecture is made up of four channels (A-D) and four divisions (1-4). The four channels are considered Level 1 of the architecture; and Level 2 and 3 are considered the Division in the architecture. Each channel and division pair (e.g., A and 1, B and 2, etc.) share the AF100 bus that allows the sharing of data between the channel and division pair with the Maintenance and Test Panel (MTP), Interface and Test Processor (ITP) and Safety Displays (SDs) assigned to that channel/division.

### Level 1

Level 1 is the Bistable Processing Logic (BPL). The BPL AC160 in each channel (A, B, C, D) acquires data from field sensors (e.g., contact, 4-20 mA, and thermocouple inputs) and performs the protective function calculations for the RPS, ECCS, and PCRVICS functions. The results of the calculations are the input to the signal comparators (bistables) which compare each value to an allowable setpoint. The outputs of these comparisons are provided as High Speed Link (HSL) signals to the Local Coincidence Logic (LCL) AC160 (Level 2) in all four divisions that performs coincidence logic processing of the bistable signals. The BPL also sends a set of bypass statuses for each trip/actuation signal for appropriate processing in the LCL

The RPS Fast-trip protective functions (which have a  $\leq 50$  ms response time) bypass the BPL and go directly to the LCL AC160 which provides both the bistable function and the coincidence logic processing for these fast-trip functions. In this case the input signals going into the LCL are the channels as defined by IEEE Std 603 and the LCL equipment is considered the division as defined by IEEE Std 603.

### Level 2

Level 2 is the LCL. The LCL in each division receives the bistable output signals from each channel's BPL AC160. The LCL performs coincidence logic on each of the RPS, ECCS, and PCRVICS process protection functions. The LCL sends the RPS trip output to the RPS Matrix and then to the RPS Termination Unit (TU). As stated earlier, the RPS fast-trip protective functions (which have a  $\leq 50$  ms response time) are processed directly in the LCL AC160 providing both the bistable function and the coincidence logic processing for these fast-trip functions. The LCL sends the ECCS and PCRVICS outputs (i.e., system level actuations) to the Integrated Logic Processor (ILP) AC160 (Level 3).

### Level 3

Level 3 is the ILP and Component Interface Module (CIM). The ILP AC160s in each division of the PPS receive system-level ECCS and PCRVICS actuation commands from the LCL and component-level commands directly from the Safety Displays. The ILPs translate system commands into component commands, implement component control logic and monitor component feedback signals. The ILP interfaces with the CIM via the Safety Remote Node Controller (SRNC). The SRNC data communication uses the same HSL unidirectional protocol as the AC160.

The CIM provides the component control interface for ECCS and PCRVICS components and performs the PPS priority logic function described in DI&C-ISG-04. Each CIM interfaces to a single safety actuating component in the plant. It's a simple FPGA (Field Programmable Gate Array)-based component that has 3 ports: an X-port to receive the safety actuation signal from the PPS, a Y-Port for non-credited safety component maneuvers, and a Z-port which is the highest priority signal (for DPS and



RRCS actuations). The Y-port will be used to support Automated Operator Aids functions (see Section 9.8) and safety component feedback to support SRM-SECY-93-087 Position 4 displays. The CIM also provides the capability for local manual control, at the module, independent of the X, Y, and Z-ports.

### Safety Display

There are redundant Safety Displays (SDs) providing indication of the safety system parameters and actuation status in the Main Control Room (MCR). The SDs are used to initiate soft controls of applicable safety components and ECCS and PCRVICS manual system level actuations. The manual ECCS and PCRVICS system level actuations include a hardwired confirm switch terminated at the LCL that signals the initiation of the ECCS or PCRVICS system level actuation. The manual reactor scram and mode select will remain as hardwired switches on the main control board. The Common Q Flat Panel Display System (FPDS) is used for the SDs.

### Maintenance and Test Panel (MTP)

The MTP in each channel/division of the PPS provides the human system interface to the safety system and is used for maintenance and test functions and is also used as necessary for loading PPS application AC160 software. In addition, the MTP provides an isolated unidirectional Ethernet interface between the PPS in each channel/division to the non-safety distributed control system (DCS) plant data highway.

### Interface and Test Processor (ITP)

The ITP in each division of the PPS provides a means of monitoring the operation of the PPS and verifying that the accuracy of the system variables and other constants are within the system requirements. The ITP monitors system health such as door alarms, power supply status and cabinet temperature. The ITP is also used to support system test features. The ITP communicates with safety subsystems within its own division/train via AF100 and with other divisions via the unidirectional HSL.

### AF100

The AF100 is a data network that connects all subsystems (AC160s and FPDSs) within a channel/division to support communications within a division for display, testing, and manual component control and system level actuation. The AF100 network does not cross channel/division boundaries.

Figure 3.2-2 is a detailed architecture drawing of the PPS showing the configuration of each AC160 and additional detail of the CIM structure.



a,c



Figure 3.2-2 PPS Architecture<sup>147</sup>



### 3.2.1 Bistable Processing Logic

The Bistable Logic Cabinets (BLCs) contain the BPL AC160s. There is one BLC per channel. The BPL provides unidirectional HSL outputs to the LCL. Isolated discreet digital outputs from this cabinet are connected to the LCL for the fast-trip RPS signals.

#### 3.2.1.1 Bistable Logic Cabinet Configuration

There is one BLC per channel that consists of an AC160 base subrack and an I/O extension subrack. The following is the module configuration for the BPL AC160:

- Three PM646A Processor Modules: Two of the PM646A Processor modules redundantly perform the bistable logic function for RPS, ECCS and PCRVICS as described (see Level 1 description in Section 3.2). The third PM646A processes the RG 1.97 variables for display on the SDs.
- One CI631 AF100 Communications Module for AF100 communication (see Section 4.4 in the Common Q Topical Report (Reference 4))
- Three AI687 Low Level Analog Input Modules (for low level signals such as thermocouple input signals)
- Two AI688 High Level Analog Input Modules (e.g., 0-10 vdc and 4-20 ma input signals)
- Two DI621 Digital Input Module for contact inputs including the Reactor Mode Switch positions
- Four DO620 Digital Output Modules to support fast RPS trip functions (see Section 3.4.1)

The MTP (see Section 3.2.7) is used to apply Manual Partial Trips (MPTs) and Manual Partial Bypasses (MPBs) to safety functions. Of the three PM646A processor modules, two of them redundantly compare the input signals to setpoints and generate a safety actuation signal to the LCL. Along with these signals, the BPL provides the MPT and MPB statuses for each safety actuation signal for the LCL to process for coincidence voting.

The BLC houses the Ovation Sequence of Events (SOE) modules, Ovation remote Analog Input modules, and Ovation Remote Node Interface (RNI) (see Section 3.5.3). The SOE data is sent to the non-safety Ovation system (the Redundant Reactivity Control System [RRCS] and the Diverse Protection System [DPS]) via the Remote Node Interface (RNI) via SOE modules located within the BLC (see Section 3.5.4).

### 3.2.2 Local Coincidence Logic

There is one Coincident Logic Cabinet (CLC) per division that consists of an AC160 base subrack and an I/O extension subrack. The following is the module configuration for the LCL AC160:

- Four PM646A Processor Modules: Two of the PM646A processor modules are dedicated to performing the coincidence logic for the RPS functions, and two processor modules are dedicated to performing the coincidence logic for ECCS and PCRVICS (NSSSS) as described in the Level 2 description in Section 3.2).
- Three CI631 AF100 Communications Module for AF100 communication (see Section 4.4 in the Common Q Topical Report, Reference 4) and Global Memory. This is a new configuration to increase reliability of both the AF100 and Global Memory, two distinct functions of the CI631



(see Sections 4.4 and Figure 4-1 in the Common Q Topical Report, Reference 4). These two functions are segmented in the PPS architecture. Two CI631 modules are located in slots 1 and 2 to support the Global Memory function and one CI631 module is in slot 9 to support the AF100 bus function (see Figure 3.2.2-1)

- Three DI621 Digital Input Modules for [ ]<sup>a,c</sup>, Reactor Shutdown Panel inputs, and inputs from the BPL for fast RPS trip functions (see Section 3.4.1)
- Four DO620 Digital Output Modules for interfacing to the RPS TU (see Sections 3.2.3 and 3.5.6)

a,c

**Figure 3.2.2-1 LCL CI631 Configuration**

The LCL subsystem consists of the coincidence voting process of the partial RPS and NSSSS/ECCS actuations (i.e., one division) for functional trips and actuations respectively. The LCL has four PM646A processor modules segmented by function. Two are dedicated for RPS functions and perform the coincidence logic for RPS redundantly. Two other PM646A processor modules are dedicated for NSSSS and ECCS coincidence logic and perform the logic redundantly (see Section 3.5.1.1).

The redundant safety function bistable signals from the BPL subsystems in all four channels are received by the LCL subsystem via HSLs for coincidence voting of RPS system-level actuations. The MPTs and MPBs are applied to the appropriate redundant channel safety actuation signals received from the BPL. The redundant data from each BPL is “ORed” prior to coincidence voting with other BPL safety actuation signals. A single system level actuation (e.g., RPS, NSSSS, ECCS) signal is generated from each applicable division based on the protection function and coincidence logic.

There are exceptions to this process for fast RPS trip functions. These exceptions are described in Section 3.4.1.



The RPS signals are generated from both RPS PM646A processor modules to corresponding DO modules. The DO outputs are hardwired to the RPS SCRAM Matrix that provides the interface to the automatic and manual actuations (see Section 3.5.6). The RPS TU (see Sections 3.2.3 and 3.5.6) is housed in the Local Coincidence Logic cabinet.

Each division's LCL logic for NSSSS actuation is dependent on the type of isolation actuation. Voting logic performs either 2oo4, 2oo2, 1oo2, or 1oo1 voting logic for isolated groups. See Table 5.2-1 in the PPS System Requirements Specification (Reference 2) for the list of isolation groups and the divisions involved. Table A-2 in the PPS System Requirements Specification (Reference 2) lists the BPL signals (A-D) that are available for coincidence voting for an NSSSS actuation. The two PM646A processor modules that are dedicated for NSSSS (along with ECCS) perform the coincidence logic redundantly. Those divisions that actually perform the isolation function send their redundant system level isolation actuation signals to the ILP via the HSL.

The ECCS/NSSSS PM646A processor module also performs the coincidence voting logic for the ECCS functions. The LCL for ECCS coincidence voting for system level actuation receives 4 redundant BPL safety actuation signals and performs a 2oo4 vote on those signals. All four PPS divisions have interfaces to the ECCS functions with the exception of HPCI, RCIC and ADS. Division 1 interfaces with RCIC actuating equipment and inboard isolation valves, and Division 3 interfaces with RCIC outboard isolation valves only. Divisions 2 interfaces with HPCI actuating equipment and inboard isolation valves and Division 4 interfaces with HPCI outboard isolation valves only. Division 1 interfaces with Division 1 ADS solenoids, and Division 3 interfaces with Division 3 ADS solenoids. In those cases, only those divisions will send their actuation signals to their corresponding ILPs.

The LCL limits bypasses to 1 BPL channel (i.e., two MPB in one channel). If a second bypass request is made for the same BPL function, it will remain pending. The ITP monitors this condition and will generate an alert when this occurs. All bypass requests are latched within each LCL processor module. This warning will indicate that a bypass request is pending until the 1<sup>st</sup> bypass is removed. The exception to this process is those functions that have a 1oo4 coincidence logic (e.g., Source Range Monitor trip function). In those 1oo4 coincidence cases, up to two channels can be bypassed to maintain the single failure criteria.<sup>148</sup>

The SDs have the capability to manually initiate a system level protection function at its division. To do this manual action, a hardwired confirm switch is required to actually initiate the protective action for the division. [

]<sup>a,c</sup> The LCL will OR the division manual system level actuation signal with the resulting division coincidence logic for automatic initiation. That resulting signal is transmitted to the ILPs via the HSL for component fanout for the system level actuation.

Section 3.3 of the PPS System Design Specification (Reference 21) provides the functional requirements of each LCL. Each LCL implements Level 2 functionality described in Section 3.2.

### 3.2.3 Reactor Scram Matrix

Each division has a Reactor Scram Matrix (see Figure 3.2.3-1) that is part of the RPS Termination Unit (RPS TU). The LCL in each division performs 2oo4 coincidence logic on the RPS trip functions



calculated in the four BPL channels (see Section 3.2.3.1). There are exceptions to this described in Section 3.2.2. As described in Section 3.5.1.1, the LCL is segmented into four PM646A processor modules. Two of these PM646A processor modules are dedicated to performing the 2oo4 coincidence logic for all RPS functions. If any RPS trip function passes the 2oo4 coincidence logic (with the exception of IRM and APRM 2oo4 Voter), then the RPS PM646A processor modules will de-energize two redundant Digital Output (DO) module channels that interface with the Reactor Scram Matrix. This is represented by four DO inputs into the Reactor Scram Matrix in Figure 3.2.3-1 from two PM646A processor modules. The RPS Scram Matrix is arranged such that at least one DO channel from each RPS PM646A processor module needs to de-energize before the RPS Scram Matrix will actuate in that division. The RPS Scram Matrix is also wired to the Window Watchdog Timer (WWDT) relay of each RPS LCL PM646A processor module. Should both LCL RPS PM646A processor modules fail, activating the WWDT relay, then the Reactor Scram Matrix in that division will generate a reactor scram signal to the RPS TU described in Section 3.5.6.

The output of the RPS Scram Matrix in each division interfaces with the RPS TU solid state relays as shown in Figure 3.5.6-1 in Section 3.5.6. When the RPS Scram Matrix logic is satisfied (contacts open), the RPS TU solid state relays are de-energized. The Division 1 and 3 RPS TUs are OR'd together so that if the RPS TU solid state relays are de-energized in either division, the power will be removed from the "A" scram pilot solenoid valves. Similarly, the Division 2 and 4 RPS TUs are OR'd together so that if the RPS TU solid state relays are de-energized in either division, the power will be removed from the "B" scram pilot solenoid valves. Power needs to be removed from both the "A" and "B" scram pilot solenoid valves in order to have a full reactor scram by means of fast control rod insertion. If only one RPS TU initiates a reactor scram, this will result in power being removed from either the "A" or "B" scram pilot solenoid valves, which results in only a "Half Scram". When a scram signal is present the backup scram valves are energized to block and vent the CRD air headers to scram the rods should the "A" and "B" scram pilot solenoid valves fail to do so.

Additionally, the RPS Scram matrix in each Division has an interface with a Reactor Scram Pushbutton located in the MCR (see Figure 3.2.3-1). Depressing two out of four of these pushbuttons (the Division 1 OR 3 pushbuttons AND Division 2 or 4 pushbuttons) results in a reactor scram using the same method of de-energization described above.



a,c

**Figure 3.2.3-1 Reactor Scram Matrix****3.2.3.1 Exceptions to RPS 2004 Logic**

There are two exceptions to the 2004 coincidence logic for the PPS RPS: APRM/OPRM 2004 Voter and IRM High Neutron Flux.

**3.2.3.1.1 APRM/OPRM Reactor Scram**

APRM 2004 coincidence logic will remain within the APRM 2004 Voter Modules. APRM configuration to each APRM 2004 Voter Module will not change. The APRM 2004 Voter Modules will continue to vote APRM High Neutron Flux and OPRM Upscale inputs independently.

As described in Section 3.4.1, the APRM 2004 Voter trip contact inputs are wired directly into the LCL DI modules due to the response time requirements for this trip. Each division LCL will read the APRM 2004 Voter channel contact inputs.

The channel/divisional assignments for the APRM 2004 Voter outputs are as follows:

- APRM 2004 Voter 1 channel input assigned to Division 1 LCL
- APRM 2004 Voter 2 channel input assigned to Division 2 LCL
- APRM 2004 Voter 3 channel input assigned to Division 3 LCL
- APRM 2004 Voter 4 channel input assigned to Division 4 LCL

When the APRM 2004 Voter contact channel input closes (indicating an APRM/OPRM trip), the LCL in that division will issue a trip signal to its associated RPS TU.



As described in the previous section, Divisions 1 and 3 provide an output to the “A” pilot scram valve solenoid at each control rod drive hydraulic power unit via the RPS TUs. Divisions 2 and 4 provide an output to the “B” pilot scram valve solenoid at each control rod drive hydraulic power unit via the RPS TUs. A full APRM-initiated reactor scram will occur when there is a trip signal present from Divisions 1 OR 3 AND there is a trip signal present from Divisions 2 OR 4. This will result in de-energizing both “A” and “B” scram valve solenoids for a reactor scram.

It should be noted that when the Source Range Neutron Flux Reactor Scram is enabled by the operator (via the SD), the APRM 2oo4 Voter scram logic reverts to a 1oo4 across the four PPS divisions. As each APRM 2oo4 Voter channel input is terminated in the LCL, the signal is then hardwired to the to other Division LCLs via Class 1E isolation devices so that the 1oo4 coincidence can be performed. In this configuration, a reactor scram will occur if any of the APRM 2oo4 Voter channel inputs to the PPS are true (contact closed). This is consistent with the LGS design basis which currently utilizes shorting links to enable the Source Range Neutron Flux Reactor Scram.

### 3.2.3.1.2 IRM High Neutron Flux Reactor Scram

Each BPL channel reads two IRM High Neutron Flux scram contact inputs. These inputs are comprised of both the IRM High Neutron Flux Trip signal and the IRM Inoperable Trip signal (which are OR’d externally to the PPS). Both IRM Neutron Flux Scram contact inputs in each BPL are OR’d together (1oo2 logic) to generate a Reactor Scram signal out of the associated channel to the LCL. The channel assignments for the IRM Scram Inputs are as follows:

- BPL-A receives IRM-A and IRM-E inputs which are OR’d (1oo2) and the resulting output is sent to LCL-1
- BPL-B receives IRM-B and IRM-F inputs which are OR’d (1oo2) and the resulting output is sent to LCL-2
- BPL-C receives IRM-C and IRM-G inputs which are OR’d (1oo2) and the resulting output is sent to LCL-3
- BPL-D receives IRM-D and IRM-H inputs which are OR’d (1oo2) and the resulting output is sent to LCL-4

As a result, a full scram will occur when there is a trip signal present from Divisions 1 OR 3 AND a trip signal present from Divisions 2 OR 4, de-energizing both “A” and “B” scram valve solenoids for a reactor scram.

It should be noted that when the Source Range Neutron Flux Reactor Scram is enabled by the operator (via the SD), the IRM Neutron Flux scram logic reverts to a 1oo4 across the four PPS divisions. In this configuration, a reactor scram will occur if any of the IRM inputs to the PPS are true (contact closed). This is consistent with the LGS design basis which currently utilizes shorting links to enable the Source Range Neutron Flux Reactor Scram.

## 3.2.4 Integrated Logic Processor

Each division will have a specific number of Integrated Logic Processor cabinets depending on the actuating components assigned to each division:



[

] <sup>a,c</sup>

In each Integrated Logic Processor cabinet is one ILP that consists of an AC160 base subrack. The following is the module configuration for the ILP AC160:

- Two PM646A Processor Modules: Two of the PM646A processor modules redundantly perform the component fanout actuation commands, for a given PCRVICS (NSSSS) and ECCS system level actuation, to the CIM as described in the Level 2 description in Section 3.2).
- Three CI631 AF100 Communications Module for AF100 communication and Global Memory (see Section 4.4 in the Common Q Topical Report, Reference 4). This is a new configuration to increase reliability of both the AF100 and Global Memory, two distinct functions of the CI631 (see Sections 4.4 and Figure 4-1 in the Common Q Topical Report, Reference 4). These two functions are segmented in the PPS architecture. Two CI631 modules are located in slots 1 and 2 to support the Global Memory function and one CI631 module is in slot 9 to support the AF100 bus function (see Figure 3.2.2-1)
- Multiple DO620 Digital Output Modules for those actuating equipment interfaces that do not require a CIM for multiple access to the component.
- Multiple DI621 Digital Input Modules are used to read inputs for display or for component feedbacks. There are some digital inputs that initiate system actions (see Table 3.2.4-1)
- One AI688 analog input module is used to read analog signals for display or for generating a protection function.
- Two AO650 analog output modules. One is used for RCIC flow control and the other is used for HPCI flow control.

Due to the location where existing sensor inputs used for actuation, they are terminated in the Integrated Logic Processor cabinet. The purpose of these signal channels is explained in Table 3.2.4-1. Some of these channels are redundant as noted in Table 3.2.4-1. For the non-redundant analog and digital channel, the ILP will perform a bistable function that initiates the associated function. For those analog and digital channels that are redundant, they are redundant within the same division, so a 1oo2 coincidence is performed on those redundant channels within the division ILP. Table 3.2.4-1 lists the signals that will be processed by the ILPs. These inputs are primarily used for asset protection functions. The Notes column explains how the function is performed by the ILPs with these channel inputs when the function is more than just for asset protection. If the Note is blank, then the function performed is an asset protection function. Table 3.2.4-1 excludes signals that are read for annunciation, alarming, or display.

**Table 3.2.4-1 PPS Input Signals Processed by the ILPs**

System	Description	Sensor	Notes
CS	CS Loop Flow (CSF1)	FT-052*N051A/B	



System	Description	Sensor	Notes
CS	D*1 Safeguard Bus Power Monitor	144X-115, 144X-116, 144X-117, 144X-118	Safeguards bus power is required for the applicable CS/RHR Pumps and associated injection valves to function.
CS	D*1-Bus-07 Output Breaker	152S/152H-11#507, 152S/152H-11607, 152S/152H-11707, 152S/152H-11807	Having the Diesel Breaker close status will cause the RHR and CS pumps to start sooner (since there doesn't need to be a delay to wait for the breaker to close).
CS	CS Pump Running	152S-11#506, 152S-11606, 152S-11706, 152S-11806	Part of the HV-052-*F031 (CS min flow valve) auto open circuit). Used when flow is not capable to inject while CS is starting up.
HPCI	HPCI Pump Flow 1 (HPF1)	FT-055*N051	
HPCI	Suppression Chamber Level (SCL)  ILP performs 1oo2 coincidence within the actuating division.	LT-055*N062B/F	Suppression Chamber Level (SCL) is necessary for the HPCI suction transfer. When CST level is low, the HPCI suction source



System	Description	Sensor	Notes
			transfers to the suppression pool as long as there is enough inventory available.
HPCI	HPCI Turbine Steam Supply Pressure (HTSSP)	PT-055*N013	
HPCI	HPCI Pump Discharge Pressure (HPDP)	PT-055*N050	
HPCI	HPCI Pump Suction Pressure (HPSP1)	PT-056*N053	
HPCI	HPCI Turbine Exhaust Pressure (HTEP) ILP performs 1oo2 coincidence within the actuating division.	PT-056*N056B/F	
HPCI	HPCI Cond Vac Tank Level	LSH-056-*20	
HPCI	Steam Line Drain Pot	LSH-055-*N014	
HPCI	HPCI Pump Loop Flow (HPF1)	FT-055-*N008	Required for HPCI flow control and valve control
RCIC	Vacuum Tank Level	LSH-050-*20	
RCIC	RCIC Steam Drain Level	LSH-049-*N010	
RCIC	RCIC Pump Flow (RPF2)	FT-049*N051	
RCIC	RCIC Pump Discharge Pressure (RPDP)	PT-049*N050	
RCIC	RCIC Pump Suction Pressure Low (RCICP1)	PT-050*N053	
RCIC	RCIC Turbine Exhaust Pressure (RTEP)	PT-050*N056A/E	



System	Description	Sensor	Notes
	ILP performs 1oo2 coincidence within the actuating division.		
RCIC	RCIC Pump Discharge Flow (RPF1)	FT-049-*N003	Required for RCIC flow control
RHR/LPCI	RHR Pump Motor Breaker Closed	152S-11#504a, 152S-11604a, 152S-11704a, 152S-11804a	HV-051-*F007A/B/C/D (RHR min flow valves) interlocks (similar to CS above)
RHR/LPCI	RHR Loop Discharge Flow (RLDF)	FT-051*N052A/B/C/D	Closes min flow valve for proper injection flow
RHR/LPCI	RHR Injection Valve Differential Pressure (RIDVP)	PDT-051-*N058A/B/C/D	RHR Injection Valve High/Low Interface interlock

The redundant ILPs in a division of the PPS receive system-level NSSSS and ECCS actuation commands via the HSLs from the LCL in its division. The ILPs in each division of the PPS receive safety component-level manual control commands via the AF100 from the Safety Display. The ILPs in each division of the PPS communicate to the CIM via the safety remote node controller (SRNC). Safety component-level manual control (for components not controllable from the SD) is provided directly into the CIM from the DCS. The DCS is the Ovation-based system that includes the RRCS and the DPS among other functions for non-safety Nuclear Steam Supply System (NSSS) control.

Both SD manual system level actuations and automatic system level actuations take priority over SD manual component control. Each ILP interfaces with components for NSSSS or ECCS functions via the CIMs or digital outputs. Using the CIM SRNC, the ILP addresses the appropriate CIM with a command based on the specific system level actuation or component control from the SD.

Each ILP receives component status feedbacks from each actuating component via the CIM or DI620 digital input module. Each ILP in turn provides component status to the SDs via the AF100.



Each ILP also provides the CIM internal status to the MTP via the AF100. CIM status is also provided to the DCS via the CIM Y-Port.

During initialization of the PPS, the ILP outputs are set to the non-actuate condition.

Each ILP implements Level 3 functionality assigned to it as described in the Detailed Functional Diagrams listed in References 48 and 49.

### 3.2.5 Component Interface Module

The CIM is an FPGA-based component that performs the priority module function described in NRC interim staff guidance DI&C-ISG-04, "COMMAND PRIORITIZATION" (ML083310185). The CIM system is designed to interface a field component to the PPS and the RRCS/DPS. The CIM priority logic function arbitrates between PPS and RRCS/DPS demands. The CIM component control logic generates a component demand based on the priority logic outputs and field component feedback signals.

The Double Width Transition Panel (DWTP) connects [ ]<sup>a,c</sup> CIM base plates to the SRNC base, Ovation RNI assembly, and redundant 24 Vdc power feeds. The Single Width Transition Panel (SWTP) connects one CIM base plate branch to the DWTP.

Communication with the PPS is accomplished with the SRNC assembly. [ ]<sup>a,c</sup> The SRNC module accepts a high speed link (HSL) connection. [ ]<sup>a,c</sup>

The SRNC communicates with each CIM through a safety bus known as the X bus. The X bus is an independent, bidirectional link between the CIM and the SRNC. [ ]

[ ]<sup>a,c</sup> The PPS can send an open, close, or stop demand. In addition to the PPS demands received over port X, the PPS can also send three configuration commands to the CIM. These commands are port Y enable, maintenance mode, and output test enable. [ ]<sup>a,c</sup>

The CIM feedback and status signals are transmitted to the SRNC via the X bus. The CIM and SRNC status and feedback signals are transmitted to Common Q via the HSL.

The CIMs communicate with the DCS through an Ovation® Remote Node Interface (RNI). The Ovation RNI interfaces to the CIM Y port. The CIM can receive DCS demands via the CIM Y port to support Automated Operator Control Aids (see Section 9.8), and the CIM can transmit status feedback to the DCS via the same CIM Y port. The Ovation RNI (interfacing to the CIM Y port) and the SRNC are physically different modules, designed and built by different companies. The Ovation equipment is a standard Emerson Process Management product. The SRNC (and CIM) have been developed by Westinghouse initially for the AP1000 application. The SRNC modules do not fit into or connect with the Ovation RNI modules or base plate assembly. The Ovation RNI connection is a fiber optic connection, while the SRNC connection is a DB-25 copper connection. The physical differences between the Ovation RNI and SRNC preclude maintenance errors.



A manual control located on each CIM provides local maintenance and test features for each field component. [ ]<sup>a,c</sup> A status bit is sent to the PPS and DCS processors when local mode is enabled.

The CIM has two Z port digital inputs that can be used for protection function demand signals from the RRCS/DPS in case the PPS fails to generate the required safety signal due to a CCF. [ ]<sup>a,c</sup>

The technical description of the CIM can be found in WCAP-17179 (Reference 8). It also includes the disposition of the ten NRC staff positions on “Command Prioritization” in DI&C-ISG-04, Section 2. Table 3.2.5-1 dispositions are specific to the LGS PPS design.

**Table 3.2.5-1 DI&C-ISG-04, Section 2 Compliance**

Position Number	Position Description	Disposition
1	A priority module is a safety related device or software function. A priority module must meet all of the 10 C.F.R. Part 50, Appendix A and B requirements (design, qualification, quality, etc.) applicable to safety-related devices or software.	The CIM was developed to meet 10 CFR 50 Appendix A and B requirements to the extent practicable for a single component. The CIM development was reviewed and approved by the NRC staff as part of the AP1000 ITAAC process.
2	Priority modules used for diverse actuation signals should be independent of the remainder of the digital system, and should function properly regardless of the state or condition of the digital system. If these recommendations are not satisfied, the applicant should show how the diverse actuation requirements are met.	For the LGS PPS, the CIM is used for diverse actuation signals and is independent of the remainder of the Common Q-based PPS, regardless of the state or condition of the PPS. The CIM is not susceptible to a Common Q CCF because of its diversity in design. The CIM interfaces to the Common Q-based PPS via a unidirectional HSL from the ILPs. The CIM Safety Remote Node Controller handles all PPS data communication separate from the component interface module itself.
3	Safety-related commands that direct a component to a safe state must always have the highest priority and must override all other commands. Commands that originate in a safety-related channel but which only cancel or enable	The CIM is designed such that the Z-port has the highest priority. The DPS/RRCS actuation signals go to the Z-port. These signals are not merely cancelling of the PPS signal, but an actual override of the PPS signal to drive the safety-related component to the safe state.



Position Number	Position Description	Disposition
	<p>cancellation of the effect of the safe-state command (that is, a consequence of a Common-Cause Failure in the primary system that erroneously forces the plant equipment to a state that is different from the designated “safe state.”), and which do not directly support any safety function, have lower priority and may be overridden by other commands. In some cases, such as a containment isolation valve in an auxiliary feedwater line, there is no universal “safe state:” the valve must be open under some circumstances and closed under others. The relative priority to be applied to commands from a diverse actuation system, for example, is not obvious in such a case. This is a system operation issue, and priorities should be assigned on the basis of considerations relating to plant system design or other criteria unrelated to the use of digital systems. This issue is outside the scope of this ISG. The reasoning behind the proposed priority ranking should be explained in detail. The reviewer should refer the proposed priority ranking and the explanation to appropriate systems experts for review. The priority module itself should be shown to apply the commands correctly in order of their priority rankings, and should meet all other applicable guidance. It should be shown that the unavailability or spurious operation of the actuated device is accounted for in, or bounded by, the plant safety analysis.</p>	<p>[</p> <p style="text-align: center;">]<sup>a,c</sup> The D3 analysis covers the unlikely event that the DPS/RRCS spuriously actuates a protection function through the Z-port.</p>
4	<p>A priority module may control one or more components. If a priority module controls more than one component, then all of these provisions apply to each of the actuated components.</p>	<p>Each CIM controls only one component.</p>



Position Number	Position Description	Disposition
5	Communication isolation for each priority module should be as described in the guidance for interdivisional communications.	<p>Each Y-port signal interface with the RRCS/DPS is via the Ovation Remote Node Interface (RNI) and fiber optic cable. The Ovation RNI is considered an RG 1.75 associated circuit in the PPS and undergoes equipment qualification to ensure the RNI does not adversely impact the safety function of the PPS. The fiber optic cable provides electrical isolation between the RRCS/DPS and the PPS.</p> <p>The Z-port signal interface with the RRCS/DPS is a hardwired contact input with a 1E isolator providing electrical isolation between the RRCS/DPS and the PPS.</p>
6	Software used in the design, testing, maintenance, etc. of a priority module is subject to all of the applicable guidance in Regulatory Guide 1.152, which endorses IEEE Standard 7- 4.3.2-2003 (with comments). This includes software applicable to any programmable device used in support of the safety function of a prioritization module, such as programmable logic devices (PLDs), programmable gate arrays, or other such devices. Section 5.3.2 of IEEE 7-4.3.2-2003 is particularly applicable to this subject. Validation of design tools used for programming a priority module or a component of a priority module is not necessary if the device directly affected by those tools is 100% tested before being released for service. 100% testing means that every possible combination of inputs and every possible sequence of device states is tested, and all outputs are verified for every case. The testing should not involve the use of the design tool itself. Software-based prioritization must meet all requirements (quality	The CIM was developed using a safety-related software development process that was reviewed and approved by the NRC via the AP1000 ITAAC. The testing performed for the CIM is summarized in Reference 11 and is compared to the test acceptance criteria in BTP 7-19.



Position Number	Position Description	Disposition
	requirements, V&V, documentation, etc.) applicable to safety-related software.	
7	<p>Any software program that is used in support of the safety function within a priority module is safety-related software. All requirements that apply to safety-related software also apply to prioritization module software.</p> <p>Nonvolatile memory (such as burned-in or reprogrammable gate arrays or random-access memory) should be changeable only through removal and replacement of the memory device.</p> <p>Design provisions should ensure that static memory and programmable logic cannot be altered while installed in the module. The contents and configuration of field programmable memory should be considered to be software, and should be developed, maintained, and controlled accordingly.</p>	<p>All CIM logic was developed as safety-related software. The contents of the programmable logic are not changeable when the CIM is installed in the system.</p>
8	<p>To minimize the probability of failures due to common software, the priority module design should be fully tested (This refers to proof-of-design testing, not to individual testing of each module and not to surveillance testing.). If the tests are generated by any automatic test generation program then all the test sequences and test results should be manually verified. Testing should include the application of every possible combination of inputs and the evaluation of all of the outputs that result from each combination of inputs. If a module includes state-based logic (that is, if the response to a particular set of inputs depends upon past conditions), then all possible sequences of input sets should also be tested. If testing of all possible sequences of input sets is not considered</p>	<p>Reference 11 summarizes the extensive testing performed on the CIM and compares that testing to the test acceptance criteria in BTP 7-19.</p>



Position Number	Position Description	Disposition
	<p>practical by an applicant, then the applicant should identify the testing that is excluded and justify that exclusion. The applicant should show that the testing planned or performed provides adequate assurance of proper operation under all conditions and sequences of conditions. Note that it is possible that logic devices within the priority module include unused inputs: assuming those inputs are forced by the module circuitry to a particular known state, those inputs can be excluded from the “all possible combinations” criterion. For example, a priority module may include logic executed in a gate array that has more inputs than are necessary. The unused inputs should be forced to either “TRUE” or “FALSE” and then can be ignored in the “all possible combinations” testing.</p>	
9	<p>Automatic testing within a priority module, whether initiated from within the module or triggered from outside, and including failure of automatic testing features, should not inhibit the safety function of the module in any way. Failure of automatic testing software could constitute common-cause failure if it were to result in the disabling of the module safety function.</p>	<p>The automatic testing functions of the CIM were developed and tested as safety-related software. The automatic test features are considered safety-related requirements that are fully tested to ensure correct operation.</p> <p>The CIM and SRNC have continuous diagnostics that indicate the health of the FPGA and the readiness of the module to perform the safety function. CIM internal self-diagnostic testing CIM is required to immediately abort and allow the execution of a safety system command.<sup>151</sup></p>
10	<p>The priority module must ensure that the completion of a protective action as required by IEEE Standard 603 is not interrupted by commands, conditions, or failures outside the module’s own safety division.</p>	<p>The component control logic within the CIM latches commands from the safety system. All commands from the non-safety system are blocked when a safety system command is active.<sup>152</sup></p>



The NRC staff positions in DI&C-ISG-04, Section 3, Multidivisional Control and Display Stations, also apply to the PPS architecture. The non-safety DCS that includes the RRCS and DPS have the capability to control individual safety components in multiple PPS divisions. In addition to the requirements for Sections 1 and 2 of DI&C-ISG-04, the falling unique staff positions in Section 3 are addressed in Table 3.2.5-2.

**Table 3.2.5-2 DI&C ISG-04 Section 3 CIM Y-Port Compliance**

Staff Position	Disposition
The nonsafety station should access safety-related plant equipment only by way of a priority module associated with that equipment. Priority modules should be designed and applied as described in the guidance on priority modules.	When the PPS and DCS control the same components, the non-safety DCS accesses safety plant equipment only by way of the CIM which performs the DI&C-ISG-04 priority module function. See Table 3.2.5-1 for the disposition of the DI&C-ISG-04 NRC staff positions on priority modules.
A nonsafety station should not affect the operation of safety-related equipment when the safety-related equipment is performing its safety function. This provision should be implemented within the safety-related system, and must be unaffected by any operation, malfunction, design error, software error, or communication error in the nonsafety equipment.	When the PPS needs to actuate safety equipment to perform a safety function, the CIM disables the associated CIM Y-Port for that equipment until the safety function is reset. The CIM Y-Port communication is electrically isolated from the PPS using fiber optic media, [ ] <sup>a,c</sup> so that any operation, malfunction, design error, software error, or communication error in the non-safety DCS will not impact the PPS actuation of the same safety equipment.
The nonsafety station should be able to bypass a safety function only when the affected division has itself determined that such action would be acceptable.	Bypass of a PPS safety function can only be performed by the MTP in that PPS division.
The nonsafety station should not be able to suppress any safety function. (If the safety system itself determines that termination of a safety command is warranted as a result of the safety function having been achieved, and if the applicant demonstrates that the safety system has all information and logic needed to make such a determination, then the safety command may be reset from a source outside the safety division. If operator judgment is needed to establish the acceptability of resetting the safety command, then reset from outside the safety division is not	The PPS is the means for resetting the safety function and not the non-safety DCS.



Staff Position	Disposition
acceptable because there would be no protection from inappropriate or accidental reset.)	
The nonsafety station should not be able to bring a safety function out of bypass condition unless the affected division has itself determined that such action would be acceptable.	Bringing a safety function out of bypass can only be performed by the MTP in that PPS division.
Safety-related stations controlling the operation of equipment in other safety-related divisions.	There are no safety stations controlling the operation of equipment in other safety divisions.
Malfunctions and Spurious Actuations	The LGS Digital Modernization Project (DMP) D3 Analysis, Reference 11, analyzes the potential consequences of both a PPS and RRCS spurious actuation, the coping mechanisms available to address them.
Human Factors Considerations	INL is performing the HFE evaluation of the MCR including the his involved with safety component control via the non-safety DCS.
Diversity and Defense-In-Depth (D3) Considerations	The DMP D3 Analysis, Reference 11, analyzes the need for Diverse Protection System (DPS) and RRCS access to the safety equipment, but this is only through the CIM Z-Port that accepts only a contact input.

On loss of power the CIM outputs go to the open state (de-energized). Other failure modes upstream of the CIM will default to a specific state based on the failure (e.g., the LCL and ILP will fail ECCS outputs to the as-is state).

The CIM interfaces with the High Amperage Relay Panel (HARP) to allow it to actuate high amperage loads (see Section 3.5.9).

### 3.2.6 Interface and Test Processor

Each division's ITP consists of an AC160 base subrack. The following is the module configuration for the ILP AC160:

- Two PM646A Processor Modules: Two of the PM646A processor modules execute the diagnostic functions. The primary reason that there are two processor modules is to accommodate the number of HSL links needed for cross channel communication.
- One CI631 AF100 Communications Module for AF100 communication and Global Memory (see Section 4.4 in the Common Q Topical Report, Reference 4).



- One DI621 Digital Input Module is used read feedbacks

The ITP in each division of the PPS provides a means of monitoring the operation of the PPS and verifying that the accuracy of the plant protection system variables and other constants are within the system requirements. The PPS can perform its safety function without the ITP being operable.

The ITP performs the following functions:

- Monitor failure and diagnostic information from each of the other subsystems in its division.
- Monitor status of each leg of the SCRAM termination unit interface and initiation logic.
- Set an alert if a SCRAM demand at the LCL PM does not result in a corresponding change in the SCRAM matrix output providing indication that there is a failure in the reactor trip path.
- Communicates the status of each coincidence vote performed within the LCLs between divisions including voting coincidence logic results and bypass requests. This provides the ability to monitor the status of any divisional voter on any divisional MTP.
- Monitor door limit switches of all the cabinet doors in the division to provide door open output signals.
- Monitor internal cabinet temperature sensors of all the cabinets in the division to detect over-temperature conditions. The temperature sensor output is an analog value that is compared to an alarm setpoint.
- Monitor the status of all internal circuit breakers for all cabinets in the division in order to detect open breakers that could affect cabinet status.
- Monitor the output of the power supply failure detection circuits of all power supplies in the division.
- Monitor MTP health via the AF100bus.
- Generate the division summary signals.
- Generate system fault division summary signals.
- Generate partial trip division summary signals.
- Generate partial bypass division summary signals.
- Read system level actuation status from the other three divisions' ITPs.
- In the event that a manual partial bypass is not granted in any of the redundant LCLs, the ITP generates alerts at the MTP and MCR to indicate that a manual partial bypass request has been latched but not granted. The alert in the MCR warns the operator of a “pending request” that could potentially be granted at a later time without administrative supervision. Procedures will instruct the operator to remove the bypass.

Alarms are provided at both the MTP and MCR via the AOI.

### 3.2.7 Maintenance and Test Panel

The MTP in each division of the PPS provides the human-interface to the safety system for maintenance and test functions. The MTP is a Common Q Flat Panel Display System located in the same cabinet as the ITP in the AER. Its access is controlled via locked cabinet doors.

It provides the human interface to assist in diagnostics/maintenance functions including displaying system performance analysis data (e.g., CPU load for each PM646A in the PPS), the status of PPS



communication links (e.g., HSLs), and system health displays (e.g., I/O module channel status). The MTP automatically resets diagnostic alarms when the errors are corrected/cleared. These errors are tracked in a system event log in the case that the operator or technician wants to see them later.

The MTP facilitates testing the PPS to help diagnose errors annunciated by self-diagnostics. Testing includes exercising PPS outputs such as the scram solenoid valves.

The MTP includes a Function Enable (FE) keyswitch. The MTP requires the FE keyswitch to be in the ENABLE position for changing setpoints, calibration data, configuration data (e.g., bypasses – including operational bypasses), and testing the PPS. A visual alert is generated on the SD when the keyswitch is in the Enable position. The status of the FE keyswitch is also sent over the AOI to the DCS to enable an MCR indication when the keyswitch is in the Enable position.

When changing setpoints, the MTP establishes an allowable range for each setpoint. The MTP provides the ability to save setpoints and calibration data to a Universal Serial Bus (USB) bulk storage device for storage outside of the PPS.

The MTP is designed to have the following display functions:

- Process variables related to the RPS/NSSSS/ECCS
- Manual initiation commands by the PPS (e.g., MPB, MPT, manual system level actuations, component control commands)
- Actuated device status and indication
- PPS System Health diagnostics including power supply status

A self-diagnostic performed by the MTP is the comparison of process values from redundant BPLs within the same division. To offload the ITP, the MTP in the LGS PPS architecture perform the Inter-channel Comparison Application self-diagnostic.<sup>153</sup>

Other functions the MTP performs include:

- Transmitting data over the AOI gateway to the non-safety DCS using the unidirectional User Datagram Protocol/Internet Protocol (UDP/IP)
- Trip an individual logic channel
- Trip all logic channels
- Insert and/or remove an operational or maintenance bypass
- Inject simulated signals for testing
- Inter-channel sensor comparisons to detect failures that could be caused by transmitter failures, loop power supply failures, input signal conditioning, and analog to digital conversion (ADC) failures.

### AC160 Software Loading

AC160 software can be loaded using the MTP. A Software Load Enable (SLE) keyswitch is required to be in the Enable position before AC160 software can be loaded in the PM646A processor module. The Common Q Topical Report, Reference 4, provides a full description of the MTP SLE keyswitch. To meet



the DI&C-ISG-04 requirements for a hard disconnect of the programming cable connected between the MTP and the AC160 PM646A, the programming cable shall be disconnected manually prior to declaring the PM646A processor module operable.<sup>154</sup>

### 3.2.8 Safety Displays

Two Safety Displays (SD) are located in the MCR per each of the four (4) divisions for a total of eight (8) SDs. Each SD provides communications and display functions using the Common Q Flat Panel Display System. The two SDs in each division are redundant performing the same functions and having the same displays available on both. The PPS can perform its automatic safety functions should the SDs become inoperable.

The SD is designed to have the following display capability:

- Mimics of plant systems
- Implemented control logic
- Component controls and the state of the components based on feedback received from the ILPs
- Display channel and division data

The SD is designed to have the following control capability:

- Safety component control sending command signals to the ILP. The component control command can be cancelled prior to actuation. Section 3.8.2 of the PPS System Design Specification (Reference 21) describes the components controlled by the SD.
- Soft controls to replace existing hand switch / indication light configurations (e.g., RPT Inhibit Switches, MSIV Closure Scram Test Switches, Turbine Stop Valve Closure SCRAM Test Switches, and SCRAM Discharge Volume Isolation Valve Test Switches). These are defined in the System Design Specification (Reference 21), Appendix E, Table E-1. The types of hand switches being replaced include:
  - Maintained contact – 2 position
  - Keylock switch – 2 position
  - Keylock switch – 3 position
  - Spring return to center – 3-position
  - Pull-out, Spring return to center – 3-position
  - Spring return from stop position – 3-position
- Soft controls for RPS, NSSSS, and ECCS system level commands. A confirmatory switch initiates the system level command in conjunction with the soft control. [

] <sup>a,c</sup> Each SD in a division has a confirm switch for system level actuations.

#### 3.2.8.1 RG 1.97 Variable Display

The PPS SDs will display the safety-related post accident RG 1.97 variables. Any spatial dedication requirements for trending and display specified in the UFSAR will be evaluated as part of the INL Human

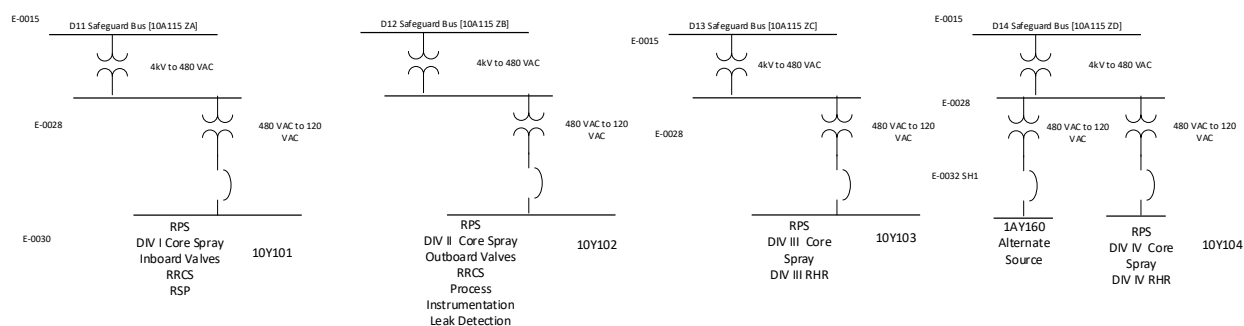


Factors evaluation. Certain diverse displays to the PPS RG 1.97 displays may be required to cope with a postulated PPS Common Cause Failure (CCF). These diverse backup RG 1.97 displays would be classified as non-safety since the postulated PPS CCF is considered beyond design basis. These necessary diverse RG 1.97 indications will be identified from the Defense-in-Depth and Diversity (D3) CCF Coping Analysis (Reference 11).

### 3.2.9 Power Supply

The Plant Protection System (PPS) cabinets receive LGS plant safety power from two diverse sources. The alternating current (AC) source is 120VAC  $\pm$ 10% and the direct current (DC) source is 125VDC  $\pm$ 15%. The LGS Class 1E power system for each unit consists of four independent divisions, which provide power to the four divisions of Class 1E loads. There are four independent, four-division Class 1E DC systems for each unit: two 125/250 V three-wire systems for Division I and II and two 125 V two-wire systems for Divisions III and IV. Figure 3.2.9-1 depicts these four, 4-division Class 1E DC systems as well as the AC plant power configuration. In addition, each unit has a 250 V non-Class 1E DC system, which are separate and independent from the Class 1E DC systems.

#### Safety AC Bus and Loads



#### Safety DC Bus and Loads

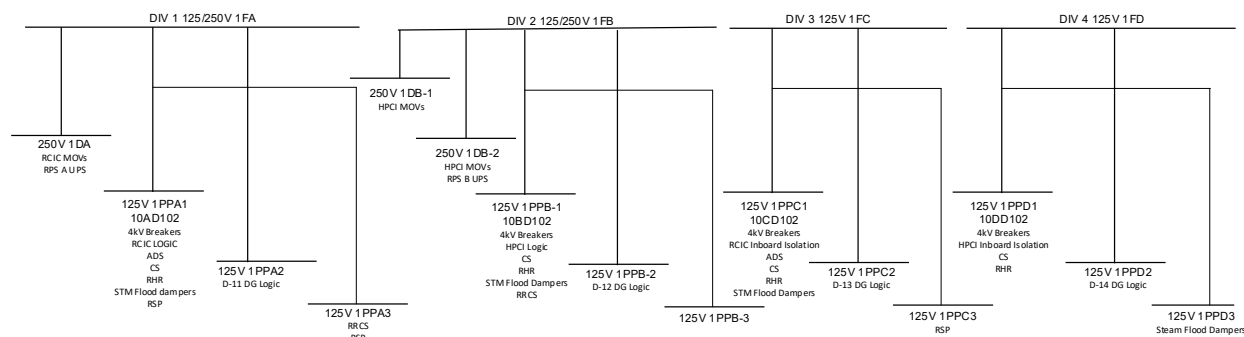


Figure 3.2.9-1 LGS Plant Power Configuration

Each PPS cabinet receives two separate power feeds:



1. 120 VAC  $\pm$  10% (108 to 132 VAC) 60Hz  $\pm$  5% (57 to 63 Hz)
2. 125 VDC  $\pm$  15%

The PPS cabinets will remain powered during a Loss of Offsite Power (LOOP through the AC power feeds sourced from Emergency Diesel Generators. Each division of PPS cabinets will receive the different LGS AC and DC division power. For cabinet DC feeds, the LGS plant power feed will come from 10xD102 subsystem, where x = A, B, C, or D (see Figure 3.2.9-1). The PPS cabinets will ride through the LOOP on 125VDC power until the associated diesel generator output breaker closes and restores 120VAC to the cabinet in about 10 seconds. The grounds that run between suited cabinets will be sealed between cabinets to meet fire separation and will be terminated on each end of the run. Figure 3.2.9-2 depicts the PPS cabinet power distribution for the Maintenance and Test Cabinets (MTCs), Bistable Logic Cabinets (BLCs), Integrated Logic Cabinets (ILCs), and the Coincidence Logic Cabinets (CLCs). Figure 3.2.9-3 depicts the PPS Safety Display power distribution in the MCR.

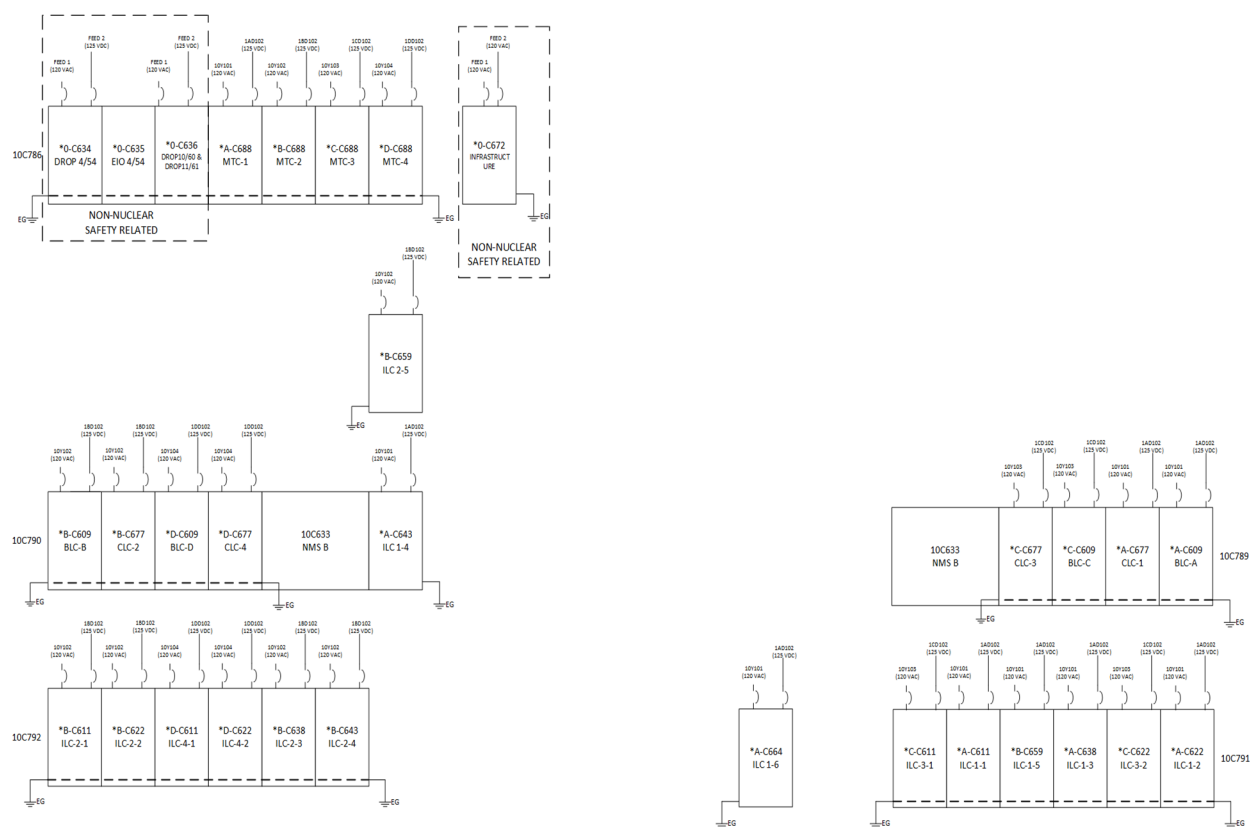
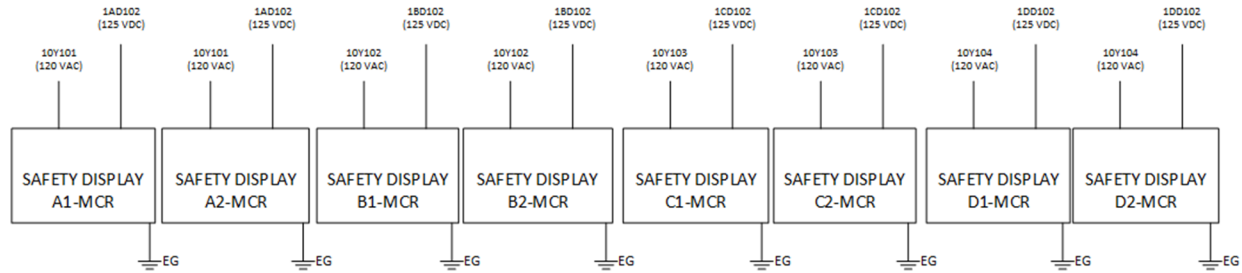


Figure 3.2.9-2 PPS Cabinet Power Arrangement





**Figure 3.2.9-3 MCR Safety Display Power Configuration**

For PPS equipment that requires low DC voltage (e.g., 24 Vdc for AC160s, Flat Panel Display Systems [i.e., MTP and SDs], and CIMs), a diode auctioneered pair of diverse power supplies are used, one to convert the LGS plant AC power to low DC levels and the 2nd to convert 125 Vdc to low DC levels. This cabinet power supply system also powers the sensor input loops. The two diverse power supplies are:

- Phoenix Contact QUINT-PS/1AC/24DC/20
- [ ]<sup>a,c</sup>

These power supplies are designed and manufactured by two different companies. This diversity between the two power supplies alleviates the concern of a potential CCF of the internal PPS power supply system.

Sufficient hold up time (at least [ ]<sup>a,c</sup>) is provided to allow momentary loss of external power due to bus transfer.

Each power supply has protection features for overvoltage and over current. Alarm contact outputs from the power supply modules are monitored by the PPS.

The power supply assembly includes local monitoring features, such as lamps, to aid in diagnosing individual power supply problems.<sup>155</sup>

### 3.2.10 HVAC Requirements

The PPS cabinets will be in the AER and the MCR which are mild environments controlled by the existing HVAC system used for those areas. Westinghouse provides Constellation with a heat load calculation for the PPS to confirm that the new PPS equipment does not surpass the existing HVAC system requirements.

### 3.2.11 PPS Design Function

The existing RPS, NSSSS, and ECCS design functions are replicated in an integrated Plant Protection System. The same protection design bases are retained. However, the PPS incorporates a number of enhancements, which include transmitter consolidation to eliminate duplicate transmitters that measure the same parameters (see Section 3.5.1), the trip logic is two-out-of-four of the same parameter to eliminate false trips, and pressure compensation of all RPV water level measurements to improve



accuracy (see Section 3.3). Table 3.3-1 lists these design functions. The design functions are implemented in a 3-tier architecture as described in Section 3.2.

### 3.2.12 Service/Test Functions

The PPS service and test functions are primarily the function of the MTP as described in Section 3.2.7. This section provides a further description of some of these service and test functions.

#### 3.2.12.1 System Health/Diagnostic Interfaces

This service and test function provides the technician detailed status of PPS system health for the AC160, MTP and SD subsystems. System health data includes hardware and software faults detected by self-diagnostics, and cabinet status variables such as door open, circuit breaker open, and temperature.

This service and test function also includes displaying the status of the CIM and its Safety Remote Node Controller (the CIM interface to the ILP).

#### 3.2.12.2 CRC/SysLoad

This page provides a dynamic display of the status of the PM646A Cyclic Redundancy Check (CRC) diagnostic and the processor loading. The processor load alarm occurs when the CPU load exceeds 70%. There are two CRC values displayed for each AC160 PM646A processor module. One value is the baseline CRC value recorded on the Software Release Record for the PM646A software that has been certified. The second value is a runtime calculation of the CRC on the PM646A firmware stored in the PM646A processor module. Should these ever differ, it implies that in some way the PM646A processor module firmware has been corrupted. Should this occur, a PPS Division Fault Alarm will be generated.

This display also provides the PM646A processor module loading (CPU load). The PM646A processor load shall not exceed 70%. Should it exceed this limit, the PPS Division Fault Alarm will be generated.

#### 3.2.12.3 Setpoint and Calibration Data Modification

The MTP facilitates the changing of setpoint and calibration data referred to as addressable constants. [

] <sup>a,c</sup> As described in the Common Q Surveillance Elimination WCAP (Reference 54), [

] <sup>a,c</sup> Any deviations in either the CRC validation [ <sup>a,c</sup> will result in division fault alarm.

#### 3.2.12.4 System Event List

The System Event List provides one or more pages of dynamic alarm and status information. This list includes all PPS Division current diagnostic failure (error) conditions. There is also a System Event Log



that provides one or more pages of historical alarm and status information. It includes historical logging of diagnostic system failures. The log can be cleared with the FE key switch in the enable position.

### **3.2.12.5 FPD Status List**

Each flat panel display (OM, MTP) contains a diagnostics page applicable to that display.

### **3.2.13 Separation and Independence**

Each redundant PPS channel/division is electrically independent and isolated from adjacent channels/divisions. There are HSL unidirectional data communication links from each channel's BPL to every division's LCL to accommodate coincidence voting of the bistable trip/actuation signals. Each division's LCL maintains electrical independence by using HSL fiber optic cables. Each division can maintain functional independence because each data link is redundant. Even if both data links from a BPL channel are lost, the LCL can process the data from the other channels for a reactor trip or ECCS/NSSSS actuation.

The PPS provides safety to non-safety communication through the MTP. This data link is called the Advant to Ovation Interface (AOI). The MTP contains a fiber optic modem and provides a single fiber transmit only link out of the PPS division. The fiber optical cabling provides electrical isolation to prevent external fault propagation back into the transmitting PPS channel. The MTP employs a UDP protocol over an Ethernet connection to achieve this unidirectional communication link and thus prevent any destination device from communicating back to the PPS.

The PPS shares sensors with the non-safety RRCS/DPS. For analog inputs, the sensor cabling is terminated at the PPS cabinet and then split between the PPS analog input module and the Ovation Remote Node Interface described in Section 3.5.3. For shared contact inputs, the signal is terminated at the PPS cabinet and then split between the PPS AC160 Digital Input module and a 1E isolator. The digital signal through the 1E isolator continues to the RRCS/DPS.

### **3.2.14 Cross Divisional Interfaces**

Cross Divisional Interfaces are discussed in Section 3.5.2.

### **3.2.15 Connections to Human-System Interfaces**

There are two types of Human System Interfaces (HSIs) in each PPS division: an MTP and an SD. Each PPS division has redundant SDs for reliability. The MTP and SDs are interconnected with the AC160 controllers as described in Section 3.5, using the AF100 bus. The PPS division has a redundant AF100 bus that provides communication among the PPS division subsystems.<sup>156</sup> The AF100 bus was reviewed and approved by the NRC and is described in Reference 3.

The MTP is used for the service and test functions described in Sections 3.2.7 and 0. It is in one of the PPS cabinets in the AER along with the AC160 controllers.



The SDs are the primary HSI for the control room operator. The functions of the SDs described in Section 3.2.8.

The SD AF100 uses a fiber optic interface to the AER MTP and AC160 controllers.<sup>157</sup>

### **3.2.16 Connections between Safety-Related Systems**

The only external connection between safety-related systems is the interconnections between PPS divisions. This is discussed in Section 3.2.21

### **3.2.17 Connections between Safety-Related and Non-Safety-Related Systems**

Section 3.5 discusses the PPS external interfaces to non-safety-related systems.

### **3.2.18 Temporary connections**

The PPS includes standard termination units which provide the capability to connect test PPS equipment without disconnecting terminations.<sup>158</sup>

### **3.2.19 Interfacing with Supporting Systems**

The two supporting systems for the PPS are the nuclear plant vital power and the HVAC for the main control room and AER. Each PPS division receives AC plant power from a separate 1E power supply channel as described in the LGS FSAR Chapter 8. The power supplies discussed in Section 3.2.9 convert the ac power into dc to power to the subsystems within the PPS channel.

Section 3.2.9 describes the power supplies the PPS divisions and Section 3.2.10 describes the Westinghouse Heat Load Calculation that will be used to ensure the existing HVAC requirements are sufficient for the PPS equipment.

### **3.2.20 Physical Location of System Equipment**

The PPS control equipment cabinets are located in the AER replacing the legacy RPS/ECCS/NSSSS logic equipment. New PPS cabinets will be installed to replace the existing RPS/ECCS/NSSSS logic equipment. The PPS SDs and their associated manual system level confirm switches are located on the main control board in the control room (see Section 3.2.8).

### **3.2.21 Communications**

The data communications for the Common Q PPS are:

- HSL communication of BPL trip signals from each BPL channel to each PPS Division LCL.<sup>159</sup>
- AOI , a UDP Ethernet communication from the OM and MTP to the non-safety DCS.<sup>160</sup>
- AF100 bus communication within a division connecting the MTP, OM and the AC160 controllers to share data<sup>161</sup>



- Component control shared between RRCS/DPS and PPS (using the CIM)
  - Y-Port – DCS [ ]<sup>a,c</sup>
  - X-Port – PPS [ ]<sup>a,c</sup>
  - Z-Port – Hard wired contact from DCS<sup>164</sup>
- Network Time Synchronization (IRIG-B input)<sup>165</sup>
- SOE Modules connected to PPS Digital Outputs<sup>166</sup>

The Ovation Sequence of Events (SOE) modules are located in the PPS cabinet. The AC160 digital outputs are hardwired to these Ovation SOE modules to capture time sequences of data for post trip or actuation evaluation in the DCS. They are not included in the ISG-04 Table 3.2.21-1 because it is not data communication. The data communication exists between the SOE modules and the DCS network, which is considered non-safety to non-safety data communication. The SOE modules are considered associated circuits within the PPS. They do not need to function in order for the PPS to perform its safety function, and the SOE modules go through equipment qualification to demonstrate they will not have an adverse effect on the PPS safety functions when residing in the PPS cabinet.

Similarly for shared sensor analog inputs, the PPS TU has a second termination for the Ovation remote I/O Analog Input Module (AI). The remote AI module interfaces with the Ovation Remote Node Interface (RNI) to transmit AI signals to the DPS/RRCS (see Section 3.5.3). The data communication exists between the RNI modules and the DCS network, which is considered non-safety to non-safety data communication.

The Common Q Topical Report (Reference 4), Sections 4.4, 5.3.1.4, and 5.4.1.4 describe the functionality and capability of the AF100 bus. The AF100 bus provides the following communication between the SDs in the MCR, the MTP, and AC160 controllers in the AER:

- AC160 data for display at the MTP and SDs (including diagnostic data)
- MTP/SD Addressable constants for use by the AC160 controllers
- SD soft control commands for component control
- SD system level actuation identification for manual system level actuations

The topical report section 5.3.2.1 describes the UDP/IP Ethernet communication from the MTP and OM, referred to herein as the AOI. Since this interface is unidirectional, it is not necessary address this interface in table 3.2.21-1. Topical report sections 4.5, 5.3.1.3, and 5.4.1.3 describe the functionality and capability of the HSL.

The CIM Technical Report (Reference 8) describes the functionality of the CIM.

HSL communication is used for PPS interdivisional communication between the BPLs in each channel and the LCLs in each division (see discussion on Level 1 and 2 functionality in Section 3.2). It is also used for interdivisional communication between the ITPs (see Section 3.2.6 for a discussion on the ITP functions). The Common Q Topical Report Section 5.6 addresses the compliance for the HSL communication protocol to the twenty communication criteria established in DI&C-ISG-04 (Reference 9). Table 3.2.21-1 DI&C-ISG-04 Compliance describes the difference in disposition of the criteria for the PPS application. As stated in the topical report, in all cases the AF100 will not apply to the positions



because the AF100 is contained within the channel. In the case of the UDP/IP Ethernet communications, there is no inbound communications into the safety system using this interface.

The time synchronization data link uses the inter-range instrumentation group (IRIG) input to the MTP in each channel. This input communication channel is fiber optically isolated.<sup>167</sup> This input is used to provide a common time reference between the PPS and DCS.<sup>168</sup> Time Synchronization is not required for the PPS to perform its safety related functions. The time synchronization input is fiber optically isolated [ ]<sup>a,c</sup> The primary reason for including the time sync signal in the PPS is to facilitate consistent time stamping for the cyber security log file transfer from the Safety Displays and MTP to the non-safety DCS<sup>169</sup>. The DCS will aggregate all of the logs files from the various sources.

The time synchronization aligns the MTP and SD clocks in all four divisions.

Table 3.2.21-1 DI&C-ISG-04 Compliance also includes the disposition of the IRIG communication channel to the 20 criteria in DI&C-ISG-04.

Section 2 of DI&C-ISG-04 provides guidance applicable to a prioritization module, that receives actuation commands from multiple safety and non-safety sources, and sends the command having highest priority to the actuated device. The ISG provides ten staff positions in this section. The dispositions to these positions are documented in Section 3.2.5. Similarly, DI&C-ISG-04 Section 3 are NRC staff positions on MultiDivisional Control and Display Stations. The CIM Y-port communications is the only part of the PPS architecture that falls under this category. Compliance to DI&C-ISG-04, Section 3 can be found in Section 3.2.5 .

The CIM Technical Report (Reference 8), Section 3.2 addresses compliance to DI&C-ISG-04 (Reference 9), Sections 1 and 2. Only the Y-Port is considered the safety/non-safety communication and is addressed in the in the CIM Technical Report. The Z-Port is a contact input from the RRCS/DPS through a qualified 1E isolator. Table 3.2.21-1 describes the difference in disposition of the criteria for the PPS application.

Citations in the dispositions to section numbers are to the sections in this document unless a specific document is mentioned.



**Table 3.2.21-1 DI&C-ISG-04 Compliance**

Position Number	Position Description	Disposition
1	A safety channel should not be dependent upon any information or resource originating or residing outside its own safety division to accomplish its safety function. This is a fundamental consequence of the independence requirements of IEEE603. It is recognized that division voting logic must receive inputs from multiple safety divisions.	<p><u>HSL</u></p> <p>There are redundant HSL unidirectional data communication links from each channel's BPL to every division's LCL to accommodate coincidence voting of the bistable trip/actuation signals to perform coincident voting on the four channel trip signals. Each division's LCL maintains electrical independence by using HSL fiber optic cables. Each division can maintain functional independence because each data link is redundant and when both redundant data links are lost, the LCL will default to a trip/actuate state for RPS/NSSSS signals and default the ECCS signals to a non-actuate state for the coincidence logic.<sup>170</sup></p> <p>The processing section (PS) of the PM646A is designed to execute the safety application.<sup>171</sup> The PS has access to the process I/O via the AC160 backplane bus BIOB.<sup>172</sup> For exchange of data with other divisions the HSL is used. The separate communication section (CS) of the PM646A is designed for this purpose and includes one transmit and two received channels. [</p> <p style="text-align: right;">] <sup>a,c</sup> and is always informed about the status of the links (i.e., the data to be sent has left the CS in a reasonable time and received data is error free and updated). When communication problems are detected, the application program in the PS can be designed to react toward the safe direction.<sup>173</sup> The PM646A architecture is shown in the Common Q Topical Report (Reference 4) Figure 5-21.</p> <p><u>IRIG</u></p>



Position Number	Position Description	Disposition
		<p>The IRIG channel is only used [ ]<sup>a,c</sup> Any corruption of IRIG data will only affect the MTP [ ]<sup>a,c</sup> Even if the MTP was somehow incapacitated by this data corruption, the AC160 controllers running the protection algorithms are unaffected by this failure mode because they run independent of the MTP.</p> <p><u>CIM</u></p> <p>The CIM performs the priority module function as described in DI&amp;C-ISG-04. Its function is described in Section 3.2.4. The PPS sends the signals through the X-port to the CIM to actuate safety-related components for ECCS and NSSSS actuations. The CIM is not dependent upon any information or resource originating or residing outside its own safety division. All logic required to perform the safety function is contained within the safety system. The logic in the CIM allows the non-safety system to control the component if a command from the safety system is not present.<sup>174</sup></p>
2	<p>The safety function of each safety channel should be protected from adverse influence from outside the division of which that channel is a member. Information and signals originating outside the division must not be able to inhibit or delay the safety function. This protection must be implemented within the affected division (rather than in the sources outside the division), and must not itself be affected by any condition or information from outside the affected division. This protection must be sustained despite any operation, malfunction, design error,</p>	<p><u>HSL</u></p> <p>The topical report disposition directly applies to the PPS application without modification.</p> <p><u>IRIG</u></p> <p>Any inappropriate IRIG data would only affect the MTP [ ]<sup>a,c</sup> and no other function in the PPS channel. If the MTP [ ]<sup>a,c</sup> was corrupted, so would be the times on the time stamp reports provided</p>



Position Number	Position Description	Disposition
	communication error, or software error or corruption existing or originating outside the division.	<p>over the AOI. The safety functions of the PPS executing in the AC160 controllers are independent of the MTP.</p> <p><u>CIM</u></p> <p>The CIM technical report disposition directly applies to the PPS application without modification.</p>
3	<p>A safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function. Receipt of information that does not support or enhance the safety function would involve the performance of functions that are not directly related to the safety function. Safety systems should be as simple as possible. Functions that are not necessary for safety, even if they enhance reliability, should be executed outside the safety system. A safety system designed to perform functions not directly related to the safety function would be more complex than a system that performs the same safety function, but is not designed to perform other functions. The more complex system would increase the likelihood of failures and software errors. Such a complex design, therefore, should be avoided within the safety system. For example, comparison of transmitter receiver readings from sensors in different divisions may provide useful information concerning the behavior of the sensors (for example, On-Line Monitoring). Such a function executed within a safety system, however, could also result in unacceptable influence of one division over</p>	<p><u>HSL</u></p> <p>There are redundant HSL unidirectional data communication links from each channel's BPL to every division's LCL to accommodate coincidence voting of the bistable trip/actuation signals. The coincidence voting on the four channel BPLs' trip signals is performed to avoid spurious actuations. Each division's LCL maintains electrical independence by using HSL fiber optic cables. Each division can maintain functional independence because each data link is redundant and when both redundant data links are lost, the LCL will reduce its coincidence logic accordingly from 2oo4 to 2oo3 to initiate the reactor trip and/or ECCS/NSSSS functions</p> <p><u>IRIG</u></p> <p>This function reduces the operational burden for analyzing cyber security log file transfers from the Safety Displays and MTP to the non-safety DCS. The implementation of this function is similar to the Palo Verde and Waterford 3 Core Protection Calculator System that have been reviewed and approved by the NRC (ML033030364 and ML21131A243 respectively). [</p> <p style="text-align: right;">] <sup>a,c</sup> This function has</p>



Position Number	Position Description	Disposition
	<p>another, or could involve functions not directly related to the safety functions, and should not be executed within the safety system. Receipt of information from outside the division, and the performance of functions not directly related to the safety function, if used, should be justified. It should be demonstrated that the added system/software complexity associated with the performance of functions not directly related to the safety function and with the receipt of information in support of those functions does not significantly increase the likelihood of software specification or coding errors, including errors that would affect more than one division. The applicant should justify the definition of “significantly” used in the demonstration.”</p>	<p>been continuously running at the Palo Verde PPS since 2004 without impact on the safety function.</p> <p><u>CIM</u></p> <p>The Y-port facilitates actuating component feedbacks independent of the AC160 portions of the PPS that are susceptible to a CCF. This provides the diverse display indications for these actuating components to support the DPS and SRM/SECY-93-087 Position 4. The Y-port also facilitates LGS operations to control individual safety components from the DPS/RRCS.</p>
4	<p>The communication process itself should be carried out by a communications processor separate from the processor that executes the safety function, so that communications errors and malfunctions will not interfere with the execution of the safety function. The communication and function processors should operate asynchronously, sharing information only by means of dual-ported memory or some other shared memory resource that is dedicated exclusively to this exchange of information. The function processor, the communications processor, and the shared memory, along with all supporting circuits and software, are all considered to be safety-related, and must be designed, qualified, fabricated, etc., in accordance with 10 C.F.R. Part 50, Appendix A and B. Access to the shared memory should be controlled in such a manner that the</p>	<p><u>HSL</u></p> <p>The topical report disposition directly applies to the PPS application without modification.</p> <p><u>IRIG</u></p> <p>The MTP in this case is the communication processor and the AC160 controller is the function processor. Any communication delays or errors would only impact the MTP and not the AC160 controller.<sup>175</sup> The MTP and AC160 operate asynchronously.<sup>176</sup></p>



Position Number	Position Description	Disposition
	<p>function processor has priority access to the shared memory to complete the safety function in a deterministic manner. For example, if the communication processor is accessing the shared memory at a time when the function processor needs to access it, the function processor should gain access within a timeframe that does not impact the loop cycle time assumed in the plant safety analyses. If the shared memory cannot support unrestricted simultaneous access by both processors, then the access controls should be configured such that the function processor always has precedence. The safety function circuits and program logic should ensure that the safety function will be performed within the timeframe established in the safety analysis, and will be completed successfully without data from the shared memory in the event that the function processor is unable to gain access to the shared memory.</p>	<p><u>CIM</u></p> <p>The CIM technical report disposition directly applies to the PPS application without modification.</p>
5	<p>The cycle time for the safety function processor should be determined in consideration of the longest possible completion time for each access to the shared memory. This longest-possible completion time should include the response time of the memory itself and of the circuits associated with it, and should also include the longest possible delay in access to the memory by the function processor assuming worst-case conditions for the transfer of access from the communications processor to the function processor. Failure of the system to meet the limiting cycle time should be detected and alarmed.</p>	<p><u>HSL</u></p> <p>The topical report disposition directly applies to the PPS application with clarification. As described Section 3.2.12.2, the PM646A CPU load is monitored for 70% maximum CPU load. Should the CPU load go above 70% the condition will be annunciated.<sup>177</sup></p> <p><u>IRIG</u></p> <p>Because the IRIG data is not used to perform the safety function, it does not need to be considered in any response time calculation.</p>



Position Number	Position Description	Disposition
		<u>CIM</u>  The CIM technical report disposition directly applies to the PPS application without modification.
6	The safety function processor should perform no communication handshaking and should not accept interrupts from outside its own safety division.	<u>HSL</u>  The topical report disposition directly applies to the PPS application without modification.  <u>IRIG</u>  The MTP is the communication processor in this arrangement whereas the AC160 is the function processor. The MTP performs the handshaking for this communication. <sup>178</sup>  <u>CIM</u>  The CIM technical report disposition directly applies to the PPS application without modification.
7	Only predefined data sets should be used by the receiving system. Unrecognized messages and data should be identified and dispositioned by the receiving system in accordance with the pre-specified design requirements. Data from unrecognized messages must not be used within the safety logic executed by the safety function processor. Message format and protocol should be pre-determined. Every message should have the same message field structure and sequence, including message identification,	<u>HSL</u>  The topical report disposition directly applies to the PPS application without modification.  <u>IRIG</u>  The IRIG protocol is a fixed protocol to allow updating of the MTP [ ] <sup>a,c</sup> As described in Position 1, unrecognized messages and data



Position Number	Position Description	Disposition
	status information, data bits, etc. in the same locations in every message. Every datum should be included in every transmit cycle, whether it has changed since the previous transmission or not, to ensure deterministic system behavior.	<p>have no impact on the safety function. The MTP will generate and display an error message if unrecognized messages or data is identified.<sup>179</sup> The message requirements in this ISG-04 position are not necessarily met, however, the data is not used in the safety function of the PPS nor can it impact the execution time of the safety function.</p> <p><u>CIM</u></p> <p>The CIM technical report disposition directly applies to the PPS application without modification.</p>
8	Data exchanged between redundant safety divisions or between safety and nonsafety divisions should be processed in a manner that does not adversely affect the safety function of the sending divisions, the receiving divisions, or any other independent divisions.	<p><u>HSL</u></p> <p>The topical report disposition directly applies to the PPS application without modification. The response to ISG-04 position 1 explains how the PPS safety function is not dependent on the data coming from other divisions to perform its safety function.</p> <p><u>IRIG</u></p> <p>The communication is not cross channel. Each MTP has its own communication channel for the IRIG signal. Because this function only updates [ ]<sup>a,c</sup> the MTP in the PPS division, it cannot impact the execution of the safety function as described in Position 2.</p> <p><u>CIM</u></p> <p>The CIM technical report disposition directly applies to the PPS application without modification.</p>



Position Number	Position Description	Disposition
9	Incoming message data should be stored in fixed predetermined locations in the shared memory and in the memory associated with the function processor. These memory locations should not be used for any other purpose. The memory locations should be allocated such that input data and output data are segregated from each other in separate memory devices or in separate pre-specified physical areas within a memory device.	<p><u>HSL</u></p> <p>The topical report disposition directly applies to the PPS application without modification.</p> <p><u>IRIG</u></p> <p>The IRIG-B input is not used for any safety functions in the PPS and therefore it is not necessary for the MTP to have pre-allocated shared memory because the data is not shared with the safety function processor (i.e., AC160 controllers).</p> <p><u>CIM</u></p> <p>The CIM technical report disposition directly applies to the PPS application without modification.</p>
10	Safety division software should be protected from alteration while the safety division is in operation. On-line changes to safety system software should be prevented by hardwired interlocks or by physical disconnection of maintenance and monitoring equipment. A workstation (e.g., engineer or programmer station) may alter addressable constants, setpoints, parameters, and other settings associated with a safety function only by way of the dual-processor/ shared-memory scheme described in this guidance, or when the associated channel is inoperable. Such a workstation should be physically restricted from making changes in more than one division at a time. The restriction should be by means of physical	<p><u>PM646A</u></p> <p>The topical report disposition directly applies to the PPS application without modification for the MTP loading AC160 software.</p> <p><u>IRIG</u></p> <p>This communication function does not involve programming or reconfiguring. As a result, this position does not apply.</p>



Position Number	Position Description	Disposition
	<p>cable disconnect, or by means of keylock switch that either physically opens the data transmission circuit or interrupts the connection by means of hardwired logic. “Hardwired logic” as used here refers to circuitry that physically interrupts the flow of information, such as an electronic AND gate circuit (that does not use software or firmware) with one input controlled by the hardware switch and the other connected to the information source: the information appears at the output of the gate only when the switch is in a position that applies a “TRUE” or “1” at the input to which it is connected. Provisions that rely on software to effect the disconnection are not acceptable. It is noted that software may be used in the safety system or in the workstation to accommodate the effects of the open circuit or for status logging or other purposes.</p>	<p><u>CIM</u></p> <p>The CIM technical report disposition directly applies to the PPS application without modification.</p>
11	<p>Provisions for interdivisional communication should explicitly preclude the ability to send software instructions to a safety function processor unless all safety functions associated with that processor are either bypassed or otherwise not in service. The progress of a safety function processor through its instruction sequence should not be affected by any message from outside its division. For example, a received message should not be able to direct the processor to execute a subroutine or branch to a new instruction sequence.</p>	<p><u>HSL</u></p> <p>The topical report disposition directly applies for the PPS application. Only data (BPL trip signals and ITP-to-ITP values) are transmitted cross channels to each PPS.</p> <p><u>IRIG</u></p> <p>The IRIG communication channel is not interdivisional although it is between a safety and non-safety system. Its only function is to update the [ ]<sup>a,c</sup> MTP. There are no programming instructions in the protocol.<sup>180</sup></p>



Position Number	Position Description	Disposition
		<u>CIM</u>  The CIM technical report disposition directly applies for the PPS application.
12	Communication faults should not adversely affect the performance of required safety functions in any way. Faults, including communication faults, originating in nonsafety equipment, do not constitute “single failures” as described in the single failure criterion of 10 C.F.R. Part 50, Appendix A. Examples of credible communication faults include, but are not limited to, the following: [twelve types of failures are then described in this position].	<u>HSL</u>  The topical report disposition directly applies to the PPS application without modification.  <u>IRIG</u>  As described in the response for Position 2 the communication faults from this communication channel cannot impact the AC160 safety function.  <u>CIM</u>  The CIM technical report disposition directly applies for the PPS application.
13	Vital communications, such as the sharing of channel trip decisions for the purpose of voting, should include provisions for ensuring that received messages are correct and are correctly understood. Such communications should employ error-detecting or error-correcting coding along with means for dealing with corrupt, invalid, untimely or otherwise questionable data. The effectiveness	<u>HSL</u>  The topical report disposition directly applies to the PPS application without modification.  <u>IRIG</u>



Position Number	Position Description	Disposition
	of error detection/correction should be demonstrated in the design and proof testing of the associated codes, but once demonstrated is not subject to periodic testing. Error-correcting methods, if used, should be shown to always reconstruct the original message exactly or to designate the message as unrecoverable. None of this activity should affect the operation of the safety-function processor.	<p>This communication channel is not considered vital communications. The data is not used to perform a safety function.</p> <p><u>CIM</u></p> <p>The CIM technical report disposition directly applies for the PPS application.</p>
14	Vital communications should be point-to-point by means of a dedicated medium (copper or optical cable). In this context, "point-to-point" means that the message is passed directly from the sending node to the receiving node without the involvement of equipment outside the division of the sending or receiving node. Implementation of other communication strategies should provide the same reliability and should be justified.	<p><u>HSL</u></p> <p>The topical report disposition directly applies for the PPS application.</p> <p><u>IRIG</u></p> <p>This communication channel is not considered vital communications. The data is not used to perform a safety function.</p> <p><u>CIM</u></p> <p>The CIM technical report disposition directly applies for the PPS application.</p>
15	Communication for safety functions should communicate a fixed set of data (called the "state") at regular intervals, whether data in the set has changed or not.	<p><u>HSL</u></p> <p>The topical report disposition directly applies to the PPS application without modification.</p> <p><u>IRIG</u></p>



Position Number	Position Description	Disposition
		<p>The data is not used to perform a safety function.</p> <p><u>CIM</u></p> <p>The CIM technical report disposition directly applies for the PPS application.</p>
16	<p>Network connectivity, liveness, and real-time properties essential to the safety application should be verified in the protocol. Liveness, in particular, is taken to mean that no connection to any network outside the division can cause an RPS/ESFAS communication protocol to stall, either deadlock or livelock. (Note: This is also required by the independence criteria of: (1) 10 CFR. Part 50, Appendix A, General Design Criteria (“GDC”) 24, which states, “interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.”; and (2) IEEE 603-1991 IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.) (Source: NUREG/CR-6082, 3.4.3).</p>	<p><u>HSL</u></p> <p>The topical report disposition directly applies to the PPS application without modification.</p> <p><u>IRIG</u></p> <p>The data is not essential for performing a safety function. See the response to Position 2 in regards to it not interfering with the PPS safety function.</p> <p><u>CIM</u></p> <p>The CIM technical report disposition directly applies for the PPS application.</p>
17	<p>Pursuant to 10 C.F.R. § 50.49, the medium used in a vital communications channel should be qualified for the anticipated normal and post-accident environments. For example, some optical fibers and components may be subject to gradual degradation as a result of prolonged exposure to radiation or to heat. In addition, new digital systems may need susceptibility testing for EMI/RFI and</p>	<p><u>HSL</u></p> <p>The topical report disposition directly applies for the PPS application. The LGS PPS EQ Summary Report (Reference 36) demonstrates that the Common Q qualification bounds the site requirements of LGS.</p>



Position Number	Position Description	Disposition
	power surges, if the environments are significant to the equipment being qualified.	<u>IRIG</u>  This communication channel does not provide a safety function and therefore it is qualified to ensure it does not adversely affect the safety function of the PPS (see the LGS PPS EQ Summary Report, Reference 36).  <u>CIM</u>  The CIM technical report disposition directly applies for the PPS application. The LGS PPS EQ Summary Report (Reference 36) demonstrates that the CIM qualification bounds the site requirements of LGS.
18	Provisions for communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complication.	<u>HSL</u>  The topical report disposition directly applies for the PPS application. The FMEA for the LGS PPS is Reference 40. The failure of the HSL communication is included. The FMEA concludes that the PPS meets the single failure criterion.  <u>IRIG</u>  The response to Position 2 provides the analysis for hazards associated with this communication channel.  <u>CIM</u>



Position Number	Position Description	Disposition
		The CIM technical report disposition directly applies for the PPS application. The FMEA for the LGS PPS is Reference 40. The failure of the CIM communication is included.
19	If data rates exceed the capacity of a communications link or the ability of nodes to handle traffic, the system will suffer congestion. All links and nodes should have sufficient capacity to support all functions. The applicant should identify the true data rate, including overhead, to ensure that communication bandwidth is sufficient to ensure proper performance of all safety functions. Communications throughput thresholds and safety system sensitivity to communications throughput issues should be confirmed by testing.	<p><u>HSL</u></p> <p>The topical report disposition directly applies for the PPS application. The PPS timing analysis is described in Reference 56. This analysis includes the analyzed HSL delays in order to demonstrate the PPS meets the response time requirements of LGS.</p> <p><u>IRIG</u></p> <p>The IRIG data link does not need to be a real time data link. Its sole purpose is to update the MTP [            ]<sup>a,c</sup></p> <p><u>CIM</u></p> <p>The CIM technical report disposition directly applies for the PPS application.</p>
20	The safety system response time calculations should assume a data error rate that is greater than or equal to the design basis error rate and is supported by the error rate observed in design and qualification testing.	<p><u>HSL</u></p> <p>The topical report disposition directly applies to the PPS application with clarification.</p> <p><u>IRIG</u></p>



Position Number	Position Description	Disposition
		<p>The IRIG data link does not need to be a real time data link. Its sole purpose is to update the MTP [ ]<sup>a,c</sup></p> <p><u>CIM</u></p> <p>The CIM technical report disposition directly applies for the PPS application. The PPS timing analysis is described in Reference 56. This analysis includes the CIM.</p>



### 3.2.22 Failure Modes and Effects Analysis<sup>181</sup>

The failure modes and effects analysis (FMEA) is a qualitative evaluation which identifies various failure modes which contribute to a system's unreliability. The FMEA identifies significant single failures and their effects or consequences on the system's ability to perform its functions. The PPS FMEA is documented in Reference 40.

The PPS is designed so that any single failure in any PPS channel will not prevent proper protective action of the other PPS channels, or inhibit operation of the PPS at the system level. The failure modes and effects analysis for this system shows that no single failure will defeat more than one of the four redundant PPS channels. The FMEA assumes that one of the four PPS channels is bypassed, resulting in a two out of three PPS coincidence logic, that is consistent with the plant Technical Specification markups.

The FMEA addresses all credible PPS interfaces (e.g. communications failures, stalls, etc.), but not all possible causes of the failure condition. At the hardware interface level, the FMEA bounds all cases by considering the worst-case effects at the PPS module (e.g., AC160 PM 646A processor module).

The PPS possess several redundancy features within a PPS division to enhance reliability. Significant among these are PM646A processor modules redundant in each PPS BPL channel (see Figure 3.2.22-1), redundant LCL processor modules (as described in Section 3.5.1.1), redundant ILP processor modules (as described in Section 3.5.1.1), and CIM 2oo2 coincidence (as described in Section 3.5.1.1).

Figure 3.2.22-1 depicts PPS BPLs designated as Channel A. There are four channels of BPLs in the PPS, A through D). As shown in the figure two PM646A processor modules read the sensor inputs and compare these inputs to setpoints. When a measured value exceeds a setpoint, the associated protection function signal is set to trip/actuate. The BPL sends the trip/actuation statuses for each PPS function periodically over the HSL to the LCLs in all four divisions. Section 3.5.1.1 describes the LCL, ILP and CIM processing downstream of the trip/actuation signals.





**Figure 3.2.22-1 PPS BPL Channel (Typical)**

### **3.2.22.1 Analog Input Module Failure Modes**

Analog input failures are complicated by the overlaying of failure modes attributable to analog input module error condition and the individual analog input channel errors. The PPS monitors both the individual analog input module channel errors as well as the overall analog input module error notification.

The redundant BPL PM646A Processor Modules read the same analog inputs to the PPS. Each analog input module is monitored for individual channel failures and module failures. If the sensor input exceeds the range limit of the analog input channel in either direction (i.e., high or low) by greater than 10% of range, the channel error terminal is set.

The module error terminal is set if one or more channel errors is set, as well as for gross module failures, such as loss of voltage or failure of module communications with the PM646A. If a module error exists without one or more module channel errors, the entire module is considered faulty, and all analog inputs will flagged as failed. The PPS response to the failed analog input signal is documented in the PPS FMEA (Reference 40).

### **3.2.22.2 Watchdog Timer<sup>182</sup>**

The FMEA credits the AC160 window watchdog timer WWDT that is described in the Common Q Topical Report (Reference 4), Section 5.2.1.3. [

]<sup>a,c</sup> This hardware watchdog timer circuit monitors two aspects of the software functionality. It first monitors the accuracy



of the periodicity of the PM646A task scheduler (see Reference 3, Section 4.1.1.6). It secondly monitors complete failure of the task scheduler execution. When the WWDT circuit times out, a relay is actuated on the front panel of the PM646A. The LCL RPS AC160 PM646A WDT relay output is wired to the RPS Termination Unit to generate a reactor trip signal from that LCL PM on a WWDT timeout (see Figure 3.2-2).

### 3.2.23 Common Cause Failure (CCF)

The existing (legacy) RPS, NSSSS, and ECCS functions are implemented using analog technology, so the change to an integrated PPS using the Common Q platform represents an analog-to-digital upgrade. As a result, a Defense-in-Depth and Diversity (D3) CCF analysis is performed. The LGS Digital Modernization D3 CCF Coping Analysis, WNA-AR-01074-GLIM (Reference 11) performs the following three analyses:

1. CCF Coping Analysis that evaluates, for each LGS UFSAR Chapter 15 event, the plant coping ability with the assumption that the Common Q portion of the PPS is not available due to a CCF. This analysis defines the Diverse Protection System (DPS) functions needed to meet with coping acceptance criteria from NRC NUREG-0800, Chapter 7, Branch Technical Position (BTP) 7-19.
2. An analysis defining the set of displays and controls located in the main control room for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls are independent and diverse from the PPS Common Q system.
3. CCF Spurious Actuation Analysis that evaluates the potential for a PPS (as well as RRCS) system level spurious actuation [

] <sup>a,c</sup>

The analysis and safety case in Reference 11 demonstrates the CIM is not vulnerable to a CCF.

These analyses identify required functionality of the DPS. The analysis document also compares the diversity attributes between the Common Q digital platform and the Emerson Ovation platform that will implement the DPS/RRCS functions. Section 9.7 summarizes the required DPS functions as a result of the D3 CCF analysis (Reference 11).

### 3.2.24 Compliance to Applicable IEEE Std 603-1991 and IEEE Std 7-4.3.2-2003 Clauses

The licensing basis for LGS is IEEE Std. 279 and this modification will not change the LGS licensing basis. This licensing technical report, and this section in particular, demonstrates how the system satisfies the applicable clauses in IEEE Std 603-1991 and IEEE Std 7-4.3.2-2003 for the new system architecture as identified in ISG-06 (Reference 1), Section D.2.2.1 (plus the addition of IEEE Std 603 Clause 5.11).

#### 3.2.24.1 IEEE Std 603-1991

##### 3.2.24.1.1 IEEE Std 603-1991 Clause 5.1

IEEE Std 603-1991, Clause 5.1, Single-Failure Criterion states (in part):



*The safety systems shall perform all safety functions required for a design basis event in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures; (2) all failures caused by the single failure; and (3) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions. The single-failure criterion applies to the safety systems whether control is by automatic or manual means. IEEE Std 379-1988 [5] provides guidance on the application of the single-failure criterion.[B21].*

The PPS is a four channel/four division architecture. Providing four channels of BPL processing meets the single failure criterion. Although there are four actuating division, due to the LGS plant equipment arrangement, not all actuations are four-way redundant. The PPS actuating division arrangement is the same arrangement as in the LGS design basis.<sup>183</sup> In some cases the current design basis does not require a system to meet the single failure criterion. For instance, the HPCI system, by itself, is not required to meet the single failure criterion. The single failure criterion is met by the operability of ADS when a single PPS channel or division failure occurs.

Each redundant PPS channel/division is electrically independent and isolated from adjacent channels/divisions.

The LGS FMEA (Reference 40) identifies single failures and their effects or consequences in the system's ability to perform its functions and shows that no single failure will defeat more than one of the four redundant PPS channels/divisions.

#### **3.2.24.1.2 IEEE Std 603-1991 Clause 5.7**

IEEE Std 603-1991, Clause 5.7, Capability for Test and Calibration states:

*Capability for testing and calibration of safety system equipment shall be provided while retaining the capability of the safety systems to accomplish their safety functions. The capability for testing and calibration of safety system equipment shall be provided during power operation and shall duplicate, as closely as practicable, performance of the safety function. Testing of Class 1E systems shall be in accordance with the requirements of IEEE Std 338-1987 [3]. Exceptions to testing and calibration during power operation are allowed where this capability cannot be provided without adversely affecting the safety or operability of the generating station. In this case:*

- (1) appropriate justification shall be provided (for example, demonstration that no practical design exists),*
- (2) acceptable reliability of equipment operation shall be otherwise demonstrated, and*
- (3) the capability shall be provided while the generating station is shut down.*

The PPS is a four-channel, four-division safety system. One channel can be bypassed and the PPS still maintains the PPS safety function by relying on the other three PPS channels. Section 3.2.18 also describes the capability for test injection signals to be applied to the PPS. The LAR technical specification markups address the required minimum operable divisions based on protection function.

Appendix A and the DMP LAR propose the elimination of manual surveillance requirements for the PPS, however the PPS via the MTP maintains the capability to test portions of the system.



### 3.2.24.1.3 IEEE Std 603-1991 Clause 5.8.1

IEEE Std 603-1991, Clause 5.8.1, Displays for Manually Controlled Actions states:

*The display instrumentation provided for manually controlled actions for which no automatic control is provided and that are required for the safety systems to accomplish their safety functions shall be part of the safety systems and shall meet the requirements of IEEE Std 497-1981 [9]. The design shall minimize the possibility of ambiguous indications that could be confusing to the operator.*

The PPS does not include any system level manual actuations that are not also an automatic controlled action. The PPS also performs individual safety component control with component feedback to the safety-related SD. The PPS SD soft control for system level manual actuations that are a backup to the PPS automatic actuations and safety-related component control undergo an HFE evaluation.

### 3.2.24.1.4 IEEE Std 603-1991 Clause 5.8.2

IEEE Std 603-1991, Clause 5.8.2, System Status Indication states:

*Display instrumentation shall provide accurate, complete, and timely information pertinent to safety system status. This information shall include indication and identification of protective actions of the sense and command features and execute features. The design shall minimize the possibility of ambiguous indications that could be confusing to the operator. The display instrumentation provided for safety system status indication need not be part of the safety systems.*

The PPS provides both trip and system alarm status indication on the SD. The PPS also sends this status information over the AOI to the DCS.<sup>184</sup> These indications provide accurate and timely status of the PPS and its execute features and component actuation feedback. For the PPS, the CIM and the HARP are considered part of the safety system IEEE Std 603 execute features. There are other display screens for the operator through the SD that provide more detailed supporting information on the PPS channel. This is described in Section 3.2.8. A HFE Evaluation of the MCR including the SDs will be conducted for the DMP.

### 3.2.24.1.5 IEEE Std 603-1991 Clause 5.8.3

IEEE Std 603-1991, Clause 5.8.3, Indication of Bypasses, states:

*If the protective actions of some part of a safety system have been bypassed or deliberately rendered inoperative for any purpose other than an operating bypass, continued indication of this fact for each affected safety group shall be provided in the control room.*

*5.8.3.1 This display instrumentation need not be part of the safety systems.*

*5.8.3.2 This indication shall be automatically actuated if the bypass or inoperative condition (a) is expected to occur more frequently than once a year, and (b) is expected to occur when the affected system is required to be operable.*



*5.8.3.3 The capability shall exist in the control room to manually activate this display indication.*

As stated in Clause 5.8.2, all bypass status information is displayed on the SD and sent over the AOI data link to the DCS. The SD and MTP provide the operator with the capability to perform maintenance and operating bypasses.<sup>185</sup> The MTP provides the capability of performing maintenance bypass functions. The BPL sends a corresponding set of bypass statuses for each protection function it processes. The LCL reads the trip channel bypass status along with the BPL trip/actuation status data to appropriately apply the bypass when performing coincidence logic.<sup>186</sup>

In some cases, the PPS will automatically bypass a function, however the PPS will automatically remove all operating bypasses, both automatic and manual, when the condition for the bypass is no longer present.<sup>187</sup> An example of an automatic bypass is when the Reactor Mode Switch is in the SHUTDOWN position, the BPL in each channel automatically bypasses the Shutdown Mode SCRAM signal for ten seconds in accordance with the LGS design basis.<sup>188</sup>

The emergency operating procedures (EOPs) calls for overriding interlocks to allow operation of specific equipment under administrative control, for example, by overriding the low RPV water level (Level 1) automatic isolation of the MSIVs to allow the MSIVs to be manually open to establish the use of the main condenser as a heat sink if specific conditions are met. PPS provides the capability at the SDs to override specific interlocks under administrative control.

**3.2.24.1.6 IEEE Std 603-1991 Clause 5.8.4**

IEEE Std 603-1991, Clause 5.8.4, Location, states:

*Information displays shall be located accessible to the operator. Information displays provided for manually controlled protective actions shall be visible from the location of the controls used to effect the actions.*

The information described in IEEE Std 603-1991, Clause 5.8, is located on the SD in the control room.

**3.2.24.1.7 IEEE Std 603-1991 Clause 5.11**

IEEE Std 603, Clause 5.11, Identification states:

*In order to provide assurance that the requirements given in this standard can be applied during the design, construction, maintenance, and operation of the plant, the following requirements shall be met:*

- (1) Safety system equipment shall be distinctly identified for each redundant portion of a safety system in accordance with the requirements of IEEE Std 384-1981 [61] and IEEE Std 420-1982 [7].*
- (2) Components or modules mounted in equipment or assemblies that are clearly identified as being in a single redundant portion of a safety system do not themselves require identification,*
- (3) Identification of safety system equipment shall be distinguishable from any identifying markings placed on equipment for other purposes (for example, identification of fire protection equipment, phase identification of power cables).*



- (4) *Identification of safety system equipment and its divisional assignment shall not require frequent use of reference material.*
- (5) *The associated documentation shall be distinctly identified in accordance with the requirements of IEEE Std 494-1974 (R1990) [8].*

The same LGS plant procedures for distinctly identifying redundant portions of the RPS/NSSSS/ECCS, identifying these equipment, and identifying equipment assigned specifically to a RPS/NSSSS/ECCS channel, are not changed as a result of the new PPS. Westinghouse PPS design documentation are marked with the words “Nuclear Safety Related” on the first page.

### **3.2.24.2 IEEE Std 7-4.3.2**

#### **3.2.24.2.1 IEEE Std 7-4.3.2 Clause 5.5.2**

IEEE Std 7-4.3.2, Clause 5.5.2, Design for Test and Calibration states:

*Test and calibration functions shall not adversely affect the ability of the computer to perform its safety function. Appropriate bypass of one redundant channel is not considered an adverse effect in this context. It shall be verified that the test and calibration functions do not affect computer functions that are not included in a calibration change (e.g., setpoint change).*

*V&V, configuration management, and QA shall be required for test and calibration functions on separate computers (e.g., test and calibration computer) that provide the sole verification of test and calibration data. V&V, configuration management, and QA shall be required when the test and calibration function is inherent to the computer that is part of the safety system.*

*V & V, configuration management, and QA are not required when the test and calibration function is resident on a separate computer and does not provide the sole verification of test and calibration data for the computer that is part of the safety system.*

Section 3.2.12 describes the test and calibration functions of the PPS. These functions are subject to the Common Q SPM V&V process that was reviewed and approved by the NRC to demonstrate that these functions do not adversely affect the safety function.

#### **3.2.24.2.2 IEEE Std 7-4.3.2 Clause 5.5.3**

IEEE Std 7-4.3.2, Clause 5.5.3, Fault Detection and Self-Diagnostics states:

*Computer systems can experience partial failures that can degrade the capabilities of the computer system, but may not be immediately detectable by the system. Self-diagnostics are one means that can be used to assist in detecting these failures. Fault detection and self-diagnostics requirements are addressed in this subclause.*

*The reliability requirements of the safety system shall be used to establish the need for self-diagnostics. Self-diagnostics are not required for systems in which failures can be detected by alternate means in a*



*timely manner. If self-diagnostics are incorporated into the system requirements, these functions shall be subject to the same V&V processes as the safety system functions.*

*If reliability requirements warrant self-diagnostics, then computer programs shall incorporate functions to detect and report computer system faults and failures in a timely manner. Conversely, self-diagnostic functions shall not adversely affect the ability of the computer system to perform its safety function, or cause spurious actuations of the safety function. A typical set of self-diagnostic functions includes the following:*

- *Memory functionality and integrity tests (e.g., PROM checksum and RAM tests)*
- *Computer system instruction set (e.g., calculation tests)*
- *Computer peripheral hardware tests (e.g., watchdog timers and keyboards)*
- *Computer architecture support hardware (e.g., address lines and shared memory interfaces)*
- *Communication link diagnostics (e.g., CRC checks)*

*Infrequent communication link failures that do not result in a system failure or a lack of system functionality do not require reporting.*

*When self-diagnostics are applied, the following self-diagnostic features shall be incorporated into the system design:*

- a) *Self-diagnostics during computer system startup*
- b) *Periodic self-diagnostics while the computer system is operating*
- c) *Self-diagnostic test failure reporting*

The self-diagnostic programs in the AC160 controller are part of the safety platform that was commercially dedicated and reviewed/approved by the NRC as documented in the Common Q Platform topical report (Reference 4). The NRC approved the Westinghouse topical report WCAP-18461-P-A, “Common Q Platform and Component Interface Module System Elimination of Technical Specification Surveillance Requirements” (Reference 54). This topical report provides a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) for the AC160 controller, documenting the coverage of internal self-diagnostics for each AC160 module. Appendix A describes:

- Describes the differences between the WCAP architecture that is represented and the PPS architecture
- Describes the coverage of the FMEDA to the PPS FMEA
- Addresses the Licensee Required Actions
- Addresses the NRC Safety Evaluation Report (SER) Application Specific Action Items (ASAI)
- Summarizes the LGS technical specification manual surveillance requirements that can be eliminated because of the AC160 self-diagnostic coverage.

There are also self-diagnostic capabilities in the PPS application programs described in Appendix A. The PPS AC160 application programs follow the software quality assurance requirements in the Common Q SPM (Reference 6).



Technical specification manual surveillance requirements are changing to credit system self-diagnostics. This is described in Appendix A.

### 3.3 PPS - NEW SYSTEM FUNCTIONS (D.2.3 AND D.2.3.1)

Although the design basis functions remain the same, there are cases where PPS is modifying the logic for the design basis functions:

- UFSAR Chapters 7.6.1.3.3.5, HPCI System Leak Detection System - Instrumentation and Controls, and 7.6.1.3.3.3, RCIC Leak Detection System - Instrumentation and Controls, use HPCI and RCIC steam line pressure to monitor pipe break (item c) respectively. This design basis is changing because breaks are monitored by HPCI and RCIC area temperatures and not steam line pressure. Low steam pressure to HPCI and RCIC will be monitored by reactor pressure.
- There are new functions in the PPS to perform modulating RPV level and pressure control for HPCI and RCIC. For both, upon receipt of an automatic or manual system initiation, the PPS will automatically align to the injection mode. While operating in the injection mode, it is possible to switch operation into the Automatic Level Control mode where the operator can select the RPV water level setpoint. The automatic level controller for HPCI or RCIC interfaces with the flow controller which in term will modulate turbine speed to control RPV water level. HPCI or RCIC can be tested in the full flow test mode, where flow is directed through the test return valve to the CST or to the suppression pool depending upon the suction source. While operating in the full flow test mode, the operator can select the Pressure Control Mode and enter a desired RPV pressure setpoint. The automatic pressure controller for HPCI or RCIC interfaces with the flow controller which in term will modulate turbine speed to control reactor pressure. The automatic level and pressure control functions are non-safety related functions to ease the burden on the operator.
- PPS will perform the control functions of SLCS to include manual startup of the SLCS pumps, monitoring of squib valve electrical circuit continuity, firing of squib valves, tripping of the pumps upon SLCS tank level low, and control of injection valves in its flow path. The automatic initiation of SLCS will be performed by the non-safety RRCS.
- The emergency operating procedures (EOPs) calls for overriding interlocks to allow operation of specific equipment under administrative control, for example, by overriding the low RPV water level (Level 1) automatic isolation of the MSIVs to allow the MSIVs to be manually open to establish the use of the main condenser as a heat sink if specific conditions are met. PPS provides the capability at the SDs to override specific interlocks under administrative control.
- Main Steam Leak Detection - The automatic isolation function for Turbine Enclosure (TE) - Main Steam Line (MSL) Tunnel Temperature - High is eliminated. This elimination requires NRC approval to delete Function 1.g, "Turbine Enclosure - Main Steam Line Tunnel Temperature - High," from current Technical Specification (TS) instrumentation tables, exclude it from proposed TS instrumentation tables, and add a new proposed TS for the TE MSL tunnel temperature. A detailed discussion and justification for the elimination of the TE MSL Tunnel Temperature - High automatic isolation function is included in the LAR.

The ambient temperature of the monitored TE MSL tunnel area can approach the isolation setpoint for reasons other than actual main steam leaks in the area, such as hot weather, reduced efficiency of the TE chillers, or instrument drift. If both TE MSL Tunnel Temperature - High trip



systems were to initiate an isolation signal, a full Group 1 isolation and reactor trip would result. Group 1 isolation closes the MSIVs, resulting in a loss of heat sink, as well as rendering the main feedwater system unavailable for scram recovery.

The new TS establishes a maximum temperature for the TE MSL Tunnel and requires verification that the TE MSL tunnel temperature on a frequency controlled by the Surveillance Frequency Control Program (SFCP). The initial frequency will be 24 hours. If the TE MSL tunnel maximum temperature exceeds the maximum, the Actions require immediate action to verify that no MSL leak exists, and periodic verification every 12 hours thereafter. If it cannot be verified that there is no MSL leakage or if the periodic verification is not performed, a plant shutdown is required.

The elimination of the TE MSL Tunnel Temperature - High automatic isolation function is similar to an NRC approved license amendment for Edwin I. Hatch Nuclear Plant, Unit Nos. 1 and 2 (ADAMS Accession No. ML21286A595).

Chapter 15.0 of the LGS Updated Final Safety Analysis Report (UFSAR) presents analytical evaluations of the nuclear steam supply system (NSSS) response to postulated disturbances in process variables and to postulated malfunctions or failures of equipment. The assumptions for PPS performance, response time, and accuracy in Chapter 15.0 will continue to be met with the new system (see Section 3.2 for a description of the architecture).

The design functions of the RPS, NSSSS, and ECCS are tabulated in Table 3.3-1. These safety analysis design functions are not changing as a result of the PPS project. The following information is included:

- FSAR Events (AOOs/PAs relevant to the plant equipment discussed in the LAR)
- Credited Trip/Actuation Signals
- Variable(s) and ranges
- Nominal (100% RTP) Analytical Limit
- Number of Channels
- Actuation Logic
- Automated Protection Function (all are reactor trip functions)
- Interlock / Permissive / Override and conditions for these functions
- Response Time Assumed in FSAR Event Analysis

The arrows in the Actuation Logic column indicate a rising or falling bistable function.



Table 3.3-1 LGS Safety Function Summary Table

Case No. (Chapter 15 Section No.)	FSAR Event (AOO/PA)	Credited Trip/Actuation Signals	Variable(s)	Range	Nominal (100% RTP)	Analytical Limit	Number of Channels	Actuation Logic	Automated Protection Function	Interlock / Permissive / Override	Condition for Interlock/ Permissive Override	Function	Response Time Assumed in FSAR Event Analysis
1 (15.1.1)	Loss of Feedwater Heating	No trip. Reactor Thermal Power- High Setpoint provides primary protection if required	APRM trip status	Trip / No Trip	No Trip	N/A	4	2oo4 ↑	Reactor Trip	N/A	N/A	N/A	>120 s
2 (15.1.2)	Feedwater Controller Failure- Maximum Demand	Turbine Stop Valve-Closure  (Level 8 trip performed by non- safety trip devices located in the DFWLCS Cabinet that operate independently of the DFWLCS)	Main turbine trip status	Trip / No trip	No Trip	N/A	4	2oo4 ↓	Reactor Trip,  EOC-RPT	Reactor power (equivalent first- stage pressure)	> 29.5%	Automatically enable respective trip logic channel	8.4 s
3A (15.1.3)	Pressure Regulator Failure-Open	Turbine Stop Valve-Closure  (Level 8 trip performed by non- safety trip devices located in the DFWCS Cabinet that operate independently of the DFWLCS)	Main turbine trip status	Trip / No trip	No Trip	N/A	4	2oo4 ↓	Reactor Trip,  EOC-RPT	Reactor power (equivalent first- stage pressure)	> 29.5%	Automatically enable respective trip logic channel	4.7 s
3B (15.1.3)	Pressure Regulator Failure-Open	Main Steam Line Pressure – Low	Main steam line pressure	0-1200 psig	980 psig	805 psig	4	2oo4 ↓	Isolation of MSIVs	Reactor Mode Switch position	Not in RUN Mode	Bypass MSIV isolation	46.8 s
3C (15.1.3)	Pressure Regulator Failure-Open	Reactor Vessel Water Level-Low, Level 2	Wide Range reactor water level	-150 to +60 inches	35 inches	-70 inches	4	2oo4↓	Initiation of RCIC.  Initiation of HPCI	N/A	N/A	N/A	52 s



Case No. (Chapter 15 Section No.)	FSAR Event (AOO/PA)	Credited Trip/Actuation Signals	Variable(s)	Range	Nominal (100% RTP)	Analytical Limit	Number of Channels	Actuation Logic	Automated Protection Function	Interlock / Permissive / Override	Condition for Interlock/ Permissive Override	Function	Response Time Assumed in FSAR Event Analysis
4 (15.1.4)	Inadvertent Main Steam Relief Valve Opening	Transient event requires no protection system or safeguard systems operation.											
5 (15.1.6)	Inadvertent RHR Shutdown Cooling Operation	APRM Neutron Flux-Upscale (Setdown)	APRM trip status	Trip / No trip	No Trip	N/A	4	2oo4 ↑  Note: APRM Neutron Flux- Upscale (Setdown) is not a direct input to PPS. The PPS interfaces to the final APRM 2oo4 Voter outputs.	Reactor trip	Reactor Mode Switch Position	Not in RUN Mode	Enables APRM trip setpoint for low power operation	>10 s
6 (15.2.1)	Pressure Regulator Failure- Closed	Transient event requires no protection system or safeguard systems operation.											
7A (15.2.2)	Generator Load Rejection	Turbine Control Valve Fast Closure, Trip Oil Pressure- Low	Generator trip status	Trip / No trip	No Trip	N/A	4	2oo4 ↓	Reactor trip	Reactor power (equivalent first- stage pressure)	> 29.5%	Automatically enable respective trip logic channel	0.07 s
7B (15.2.2)	Generator Load Rejection	Turbine Control Valve Fast Closure, Trip Oil Pressure- Low	Generator trip status	Trip / No trip	No trip	N/A	4	2oo4 ↓	EOC-RPT	Reactor power (equivalent first- stage pressure)	> 29.5%	Automatically enable respective trip logic channel	0.175 s
8 (15.2.3)	Turbine Trip	Turbine Stop Valve- Closure	Main turbine trip status	Trip / No trip	No trip	N/A	4	2oo4 ↓	Reactor trip, EOC-RPT	Turbine first-stage pressure	>29.5% reactor power	Enables reactor trip	0.01 s
9A (15.2.4)	MSIV Closures (all valves)	MSIV Closure	MSIV Open/Close status	Open/Close	Open	N/A	4	2oo4 ↓	Reactor trip	Reactor Mode Switch position	Shutdown, Refuel, or Startup	Bypass reactor trip	0.3 s



Case No. (Chapter 15 Section No.)	FSAR Event (AOO/PA)	Credited Trip/Actuation Signals	Variable(s)	Range	Nominal (100% RTP)	Analytical Limit	Number of Channels	Actuation Logic	Automated Protection Function	Interlock / Permissive / Override	Condition for Interlock/ Permissive Override	Function	Response Time Assumed in FSAR Event Analysis
9B (15.2.4)	MSIV Closures  (all valves)	Reactor Vessel Water Level-Low, Level 2	Wide Range reactor water level	-150 to +60 inches	35 inches	-70 inches	4	2oo4↓	Initiation of RCIC and HPCI systems	N/A	N/A	N/A	26 s
9C (15.2.4)	MSIV Closure (1 valve)	APRM Neutron Flux- Upscale	APRM Trip status	Trip / No trip	No Trip	N/A	4	2oo4 ↑  Note: APRM Neutron Flux- Upscale is not a direct input to PPS. The PPS interfaces to the final APRM 2oo4 Voter outputs.	Reactor trip	N/A	N/A	N/A	See Note 1
9D (15.2.4)	MSIV Closures (1 valve)	Reactor Vessel Steam Dome Pressure-High	Reactor vessel steam dome pressure	0 – 1500 psig	1044 psig	1111 psig	4	2oo4 ↑	Reactor trip	N/A	N/A	N/A	See Note 1
Note 1: The FSAR states that there are no quantitative analysis provided because this transient is bounded by Closure of All MSIVs. However, it states that a closure of one MSIV above 90% power may increase reactor pressure and flux enough to initiate a high neutron flux scram.													
10A (15.2.5)	Loss of Condenser Vacuum	Main Turbine Stop Valve-Closure	Main turbine trip status	Trip/No trip	No trip	N/A	4	2oo4 ↓	Reactor trip, EOC-RPT	N/A	N/A	N/A	0.01 s
10B (15.2.5)	Loss of Condenser Vacuum	Reactor Vessel Water Level-Low, Level 2	Wide Range reactor water level	-150 to +60 inches	35 inches	-70 inches	4	2oo4↓	Initiation of RCIC and HPCI systems	N/A	N/A	N/A	50.6 s
11 (15.2.6)	Loss of AC Power	Event results in generator load rejection. See Items 7A and 7B above.											
12A (15.2.7)	Loss of Feedwater Flow	Reactor Vessel Water Level-Low, Level 3	Narrow Range reactor water level	0-60 inches	35 inches	2.83 inches	4	2oo4 ↓	Reactor trip	N/A	N/A	N/A	~ 6 s



Case No. (Chapter 15 Section No.)	FSAR Event (AOO/PA)	Credited Trip/Actuation Signals	Variable(s)	Range	Nominal (100% RTP)	Analytical Limit	Number of Channels	Actuation Logic	Automated Protection Function	Interlock / Permissive / Override	Condition for Interlock/ Permissive Override	Function	Response Time Assumed in FSAR Event Analysis
12B (15.2.7)	Loss of Feedwater Flow	Reactor Vessel Water Level-Low, Level 2	Wide Range reactor water level	-150 to +60 inches	35 inches	-70 inches	4	2oo4↓	RCIC and HPCI initiation  Containment Isolation initiation	N/A	N/A	N/A	~ 19 s
13 (15.2.9)	Failure of RHR Shutdown Cooling	Qualitative analysis described in UFSAR Section 15.2.9. Manual operations are described to restore shutdown cooling by various means. No protection actuation is taken credit for in the analysis.											
14 (15.2.10)	Loss of Stator Cooling	Reactor Vessel Steam Dome Pressure-High	Reactor vessel steam dome pressure	0-1500 psig	1044 psig	1111 psig	4	2oo4 ↑	Reactor trip	N/A	N/A	N/A	~ 138 s
15 (15.3.1)	Recirculation Pump Trip (2 pumps)	Turbine Stop Valve-Closure	Main turbine trip status	Trip/No trip	No trip	N/A	4	2oo4 ↓	Reactor trip, EOC-RPT	N/A	N/A	N/A	5.2 s
		Reactor Vessel Water Level-Low, Level 2	Wide Range reactor water level	-150 to +60 inches	35 inches	-70 inches	4	2oo4↓	RCIC and HPCI initiation,  Containment Isolation initiation	N/A	N/A	N/A	~ 43.5 s
16 (15.3.2)	Recirculation Flow Control Failure- Decreasing Flow	Results of analyses are bounded by analysis of trip of two recirculation pumps in 15.3.1.											
17 (15.3.3)	Recirculation Pump Seizure	Transient event analyzed requires no protection system or safeguard systems operation. Different nuclear boiler system operational parameters might result in reactor water level swell causing a high level turbine trip, reactor trip, recirculation pump trip, and HPCI/RCIC initiation, but bounded by analysis of two recirculation pump trip in 15.3.1.											
18 (15.3.4)	Recirculation Pump Shaft Break	Transient event analyzed requires no protection system or safeguard systems operation.											



Case No. (Chapter 15 Section No.)	FSAR Event (AOO/PA)	Credited Trip/Actuation Signals	Variable(s)	Range	Nominal (100% RTP)	Analytical Limit	Number of Channels	Actuation Logic	Automated Protection Function	Interlock / Permissive / Override	Condition for Interlock/ Permissive Override	Function	Response Time Assumed in FSAR Event Analysis
19 (15.4.1)	Rod Withdrawal Error-Low Power	Transient event analyzed requires no protection system or safeguard systems operation.											
20 (15.4.2)	Rod Withdrawal Error-At Power	Transient event analyzed requires no protection system or safeguard systems operation.											
21 (15.4.3)	Control Rod Maloperation	This transient is covered by the evaluations cited in 15.4.1 and 15.4.2.											
22 (15.4.4)	Abnormal Startup of Idle Recirculation Pump	APRM Neutron Flux-Upscale	APRM trip status	Trip/No trip	No trip	N/A	4	2004 ↑  Note: APRM Neutron Flux- Upscale is not a direct input to PPS. The PPS interfaces to the final APRM 2oo4 Voter outputs.	Reactor trip	N/A	N/A	N/A	10.4 s
23 (15.4.5)	Recirculation Flow Control Failure with Increasing Flow	APRM Neutron Flux-Upscale	APRM trip status	Trip/No trip	No trip	N/A	4	2004 ↑  Note: APRM Neutron Flux- Upscale is not a direct input to PPS. The PPS interfaces to the final APRM 2oo4 Voter outputs.	Reactor trip	N/A	N/A	N/A	1.7 s
24 (15.4.7)	Misplaced Bundle Accident	Event analyzed requires no protection system or safeguard systems operation.											



Case No. (Chapter 15 Section No.)	FSAR Event (AOO/PA)	Credited Trip/Actuation Signals	Variable(s)	Range	Nominal (100% RTP)	Analytical Limit	Number of Channels	Actuation Logic	Automated Protection Function	Interlock / Permissive / Override	Condition for Interlock/ Permissive Override	Function	Response Time Assumed in FSAR Event Analysis
25 (15.4.9)	Control Rod- Drop Accident	APRM Neutron Flux-Upscale	APRM trip status	Trip/No trip	No trip	N/A	4	2oo4 ↑  Note: APRM Neutron Flux- Upscale is not a direct input to PPS. The PPS interfaces to the final APRM 2oo4 Voter outputs.	Reactor trip	N/A	N/A	N/A	See Note 2
Note 2: The FSAR analysis for the control rod drop accident refers to GE’s generic license application document GESTAR II. The sequence of events is: time 0 = rod drop, reactor goes on a positive period and initial power burst is terminated by the Doppler reactivity feedback in ≤ 1 second, APRM 120% high flux scrams reactor; time is not given, and Scram terminates accident at ≤ 5 seconds. All control rods are fully inserted in approximately 3 seconds or less. Thus, the time at which APRM would have exceeded the Upscale trip setpoint would be approximately 2 seconds.													
26 (15.5.1)	Inadvertent HPCI Startup	Event analyzed requires no protection system or safeguard systems operation.											
27 (15.6.1)	Inadvertent Main Steam Relief Valve Opening	Event analyzed requires no protection system or safeguard systems operation. See 15.1.4.											
28 (15.6.2)	Instrument Line Pipe Break	Event analyzed requires no protection system or safeguard systems operation.											
29A (15.6.4)	Steam System Piping Break Outside Primary Containment	Main Steam Line Flow-High	Main steam line flow (ΔP)	0-150 psid	72 psid	< 123 psid	4	2oo4↑	MSIV closure	N/A	N/A	N/A	1.0 s
29B (15.6.4)	Steam System Piping Break Outside Primary Containment	MSIV Closure	MSIV positions	Open / Close	Open	N/A	4	2oo4 ↓	Reactor trip	N/A	N/A	N/A	<1.5 s



Case No. (Chapter 15 Section No.)	FSAR Event (AOO/PA)	Credited Trip/Actuation Signals	Variable(s)	Range	Nominal (100% RTP)	Analytical Limit	Number of Channels	Actuation Logic	Automated Protection Function	Interlock / Permissive / Override	Condition for Interlock/ Permissive Override	Function	Response Time Assumed in FSAR Event Analysis
29C (15.6.4)	Steam System Piping Break Outside Primary Containment	Reactor Vessel Water Level-Low, Level 2	Wide Range reactor water level	-150 to +60 inches	35 inches	-70 inches	4	2oo4↓  2oo4↓	RCIC and HPCI initiation,  Containment Isolation initiation.	N/A	N/A	N/A	~ 60 s
29D (15.6.4)	Steam System Piping Break Outside Primary Containment	Reactor Vessel Water Level-Low, Level 1	Wide Range reactor water level	-150 to +60 inches	35 inches	-161 inches	4	2oo4 ↓	ADS initiation (Note 3)	High drywell pressure bypass timer and  ADS timer	Timers “timed out”	Initiate ADS	~ 1780 s
Note (3): Div 1 actuates “A” solenoids of ADS valves. Div 3 actuates “B” solenoid valves of ADS valves. See UFSAR Figure 7.3-4 for divisional trip logic. Reactor water level and drywell pressure use 2oo4 logic.													
30A (15.6.5)	LOCA Inside Containment	Drywell Pressure-High	Drywell pressure	0 – 10 psig	0.3 psig	2.00 psig	4	2oo4 ↑  2oo4↑  2oo4↑  2oo4↓ water level, or 2oo4↑ drywell pressure and reactor pressure ↓ permissive	Reactor trip  HPCI initiation  Containment isolation (except for the MSIVs)  LPCI initiation	N/A	N/A	N/A	<1 s
30B (15.6.5)	LOCA Inside Containment	Reactor Vessel Level-Low Level 3	Narrow Range reactor water level	0-60 inches	35 inches	2.83 inches	4	2oo4 ↓	Reactor trip (second signal),	N/A	N/A	N/A	~1 s



Case No. (Chapter 15 Section No.)	FSAR Event (AOO/PA)	Credited Trip/Actuation Signals	Variable(s)	Range	Nominal (100% RTP)	Analytical Limit	Number of Channels	Actuation Logic	Automated Protection Function	Interlock / Permissive / Override	Condition for Interlock/ Permissive Override	Function	Response Time Assumed in FSAR Event Analysis
30C (15.6.5)	LOCA Inside Containment	Reactor Vessel Level-Low Level 2	Wide Range reactor water level	-150 to +60 inches	35 inches	-70 inches	4	2oo4↓	HPCI initiation (second signal)	N/A	N/A	N/A	~ 4 s
30D (15.6.5)	LOCA Inside Containment	Reactor Vessel Level-Low Level 1	Wide Range reactor water level	-150 to +60 inches	35 inches	-161 inches	4	2oo4↓  2oo4↓	MSIV closure  Main steam line drain isolation	N/A	N/A	N/A	~ 5 s
30E (15.6.5)	LOCA Inside Containment	Reactor Vessel Level-Low Level 1	Wide Range reactor water level	-150 to +60 inches	35 inches	-161 inches	4	2oo4↓ water level, or 2oo4↑ drywell pressure and reactor pressure ↓ permissive	CS initiation	Vessel to drywell ΔP	<289 psid (vessel to drywell)	CS injection valve ΔP permissive to open	~ 22 s
30F (15.6.5)	LOCA Inside Containment	Reactor Vessel Level-Low Level 1	Wide Range reactor water level	-150 to +60 inches	35 inches	-161 inches		2oo4↓ water level,  Or 2oo4↑ drywell pressure and reactor pressure ↓ permissive	LPCI initiation	Vessel to drywell ΔP	<295 psid (vessel to drywell)	LPCI injection valve ΔP permissive to open	~ 26 s
31A (15.6.6)	Feedwater Line Break Outside Primary Containment	Reactor Vessel Level-Low Level 3	Narrow Range reactor water level	0-60 inches	35 inches	2.83 inches	4	2oo4↓	Reactor trip	N/A	N/A	N/A	~1 s
31B (15.6.6)	Feedwater Line Break Outside Primary Containment	Reactor Vessel Level-Low Level 2	Wide Range reactor water level	-150 to +60 inches	35 inches	-70 inches	4	2oo4↓  2oo4↓	HPCI initiation  RCIC initiation	N/A	N/A	N/A	<0.5 s



Case No. (Chapter 15 Section No.)	FSAR Event (AOO/PA)	Credited Trip/Actuation Signals	Variable(s)	Range	Nominal (100% RTP)	Analytical Limit	Number of Channels	Actuation Logic	Automated Protection Function	Interlock / Permissive / Override	Condition for Interlock/ Permissive Override	Function	Response Time Assumed in FSAR Event Analysis
31C (15.6.6)	Feedwater Line Break Outside Primary Containment	Reactor Vessel Level-Low Level 1	Wide Range reactor water level	-150 to +60 inches	35 inches	-161 inches	4	2oo4↓   2oo4↓   2oo4↓ water level, Or 2oo4↑ drywell pressure and reactor pressure ↓ permissive   2oo4↓ water level, Or 2oo4↑ drywell pressure and reactor pressure ↓ permissive	MSIV closure   Main steam drain isolation   CS initiation*   LPCI initiation*   *System initiation but no injection due to reactor at high pressure	N/A	N/A	N/A	<0.5 s
32 (15.7.1)	Radioactive Gas Waste System Leak or Failure	Event analyzed requires no protection system or safeguard systems operation.											
33 (15.7.2)	Liquid Radioactive Waste System Failure	Event analyzed requires no protection system or safeguard systems operation.											



Case No. (Chapter 15 Section No.)	FSAR Event (AOO/PA)	Credited Trip/Actuation Signals	Variable(s)	Range	Nominal (100% RTP)	Analytical Limit	Number of Channels	Actuation Logic	Automated Protection Function	Interlock / Permissive / Override	Condition for Interlock/ Permissive Override	Function	Response Time Assumed in FSAR Event Analysis
34 (15.7.3)	Postulated Radioactive Releases due to Liquid Radwaste Tank Failure	Event analyzed requires no protection system or safeguard systems operation.											
35 (15.7.4)	Fuel Handling Accident	Event analyzed requires no protection system or safeguard systems operation.											
36A (15.8)	ATWS	Reactor Vessel Level-Low Level 2	Wide Range reactor water level	-150 to +60 inches	35 inches	-70 inches	4	2oo4↓ OR 2oo4 ↑ RPV Pressure High	RPT  ARI  RWCU Isolation (Note 4)  SLCS Initiation	N/A	N/A	N/A	N/A  N/A N/A 118 s
36B (15.8)	ATWS	Reactor Vessel Steam Dome Pressure-High	Reactor vessel steam dome pressure	0-1500 psig	1044 psig	1111 psig	4	2oo4↓ OR 2oo4 ↑ RPV Pressure High	RPT  ARI  RWCU Isolation (Note 4)  SLCS Initiation	N/A	N/A	N/A	N/A  N/A N/A 118 s
Note (4): RWCU isolation will only occur upon a valid SLCS initiation.													



### 3.3.1 IEEE Std 603-1991 Clause 4 Compliance

IEEE Std 603-1991 Clause 4 requires the plant design basis to be documented for the following criteria. For each criterion, the impact on the existing design basis for LGS is indicated as a result of replacing RPS/NSSSS/ECCS with the Common Q platform based PPS.

*Clause 4.1: The design basis events applicable to each mode of operation of the generating station along with the initial conditions and allowable limits of plant conditions for each such event.*

The LGS design basis events are unchanged as a result of the PPS upgrade.

*Clause 4.2: The safety functions and corresponding protective actions of the execute features for each design basis event.*

For the PPS the execute features include the CIM and the HARP. The PPS safety functions and corresponding protective actions of the execute features are functionally unchanged as a result of the RPS, ECCS and NSSSS replacement, except as noted in Section 3.3.

*Clause 4.3: The permissive conditions for each operating bypass capability that is to be provided.*

The permissive conditions for each operating bypass capability of the RPS, ECCS, and NSSS are unchanged, except as noted in Section 3.3, and is initiated from the PPS.

*Clause 4.4: The variables or combinations of variables, or both, that are to be monitored to manually or automatically, or both, control each protective action; the analytical limit associated with each variable, the ranges (normal, abnormal, and accident conditions); and the rates of change of these variables to be accommodated until proper completion of the protective action is ensured.*

The variables or combination of variables monitored by the PPS for each control protection action (except as noted in Sections 3.3 and 3.5.1), the analytical limit associated with each variable, the ranges and rates of change of these variables are unchanged as a result of the PPS upgrade. This is summarized in Table 3.3.-1.

*Clause 4.5: The following minimum criteria for each action identified in 4.2 whose operation may be controlled by manual means initially or subsequent to initiation.*

The PPS upgrade does not change the minimum criteria for each protective function whose operation may be controlled by manual means initially or subsequent to initiation. Except for UFSAR DBE 15.2.9, “Failure of RHR Shutdown Cooling” in Table 3.3-1, all actions are automatic.

*Clause 4.6: For those variables in 4.4 that have a spatial dependence (that is, where the variable varies as a function of position in a particular region), the minimum number and locations of sensors required for protective purposes.*

The variables used to initiate the PPS protection functions are summarized in Table 3.3-1. These are unchanged as a result of the PPS upgrade, except as noted in Sections 3.3 and 3.5.1.



Clause 4.7: *The range of transient and steady-state conditions of both motive and control power and the environment (for example, voltage, frequency, radiation, temperature, humidity, pressure, and vibration) during normal, abnormal, and accident circumstances throughout which the safety system shall perform.*

Both the PPS input instrumentation (e.g., temperature and pressure sensors) and plant actuators (e.g., scram solenoids) are unchanged as a result of the PPS upgrade. The AER in which the PPS cabinets are located is in a mild environment.<sup>189</sup> The EQ Summary Report (Reference 36) summarizes how the equipment qualification of the Common Q platform bounds the LGS site requirements for seismic, EMC, and environmental conditions. The same LGS bus power will be used to power the PPS equipment. The compatibility of the equipment to equivalent power sources is summarized in the LGS PPS EQ Summary Report (Reference 36). The site acceptance test for the PPS will demonstrate the compatibility of the PPS equipment to the LGS Class 1E Power Supply System.

Clause 4.8: *The conditions having the potential for functional degradation of safety system performance and for which provisions shall be incorporated to retain the capability for performing the safety functions (for example, missiles, pipe breaks, fires, loss of ventilation, spurious operation of fire suppression systems, operator error, failure in non-safety-related systems).*

The LGS EQ Summary Report (Reference 36) demonstrates the capability of the PPS to continue operating at higher temperatures as a result of abnormal of HVAC operation in the AER.<sup>190</sup> Once the PPS reaches its qualified temperature limit, a high temperature alarm is generated.<sup>191</sup>

Clause 4.9: *The methods to be used to determine that the reliability of the safety system design is appropriate for each safety system design and any qualitative or quantitative reliability goals that may be imposed on the system design.*

The PPS Reliability Analysis (Reference 42) provides a calculation of the availability for the Plant Protection System (PPS) for LGS. The Reliability Block Diagram (RBD) analysis is performed using the method described in Section 8 of WNA-IG-00064-GEN, “Reliability and Availability Analysis Methods” (Reference 43). [

]<sup>a,c</sup> This method of analysis meets the intent of IEEE Std 352-2016.

The LGS PPS reliability calculation (Reference 42) documents that the Common Q PPS meets the LGS reliability requirements for the following subsystems within PPS:



PPS Reliability Requirements/Calculation		
System	Failures Per Demand Requirements <sup>192</sup>	Failures Per Demand Calculated
RPS	3E-06	[ ] <sup>a,c</sup>
ECCS	3E-04	[ ] <sup>a,c</sup>
NSSSS	3E-04	[ ] <sup>a,c</sup>

Clause 4.10: *The critical points in time or the plant conditions, after the onset of a design basis event, including:*

Clause 4.10.1: *The point in time or plant conditions for which the protective actions of the safety system shall be initiated.*

Clause 4.10.2: *The point in time or plant conditions that define the proper completion of the safety function.*

Clause 4.10.3: *The points in time or the plant conditions that require automatic control of protective actions.*

Clause 4.10.3: *The point in time or the plant conditions that allow returning a safety system to normal.*

The LGS design basis events as defined in Chapter 15 for LGS are not changed as a result of this PPS project. The response time budget for the PPS is defined in the PPS System Requirements Specification (Reference 2), Section 7.1. The response time analysis (Reference 56) for the Common Q LGS PPS demonstrates that the PPS calculated response times meet these requirements.

Clause 4.11: *The equipment protective provisions that prevent the safety systems from accomplishing their safety functions.*

The PPS protective provision in case the safety system fails to accomplish its safety function is to fail to a known state. In the case of RPS functions, the failed state is to initiate a reactor trip. [

]<sup>a,c</sup>

For NSSSS functions, the failed state is to initiate the isolation function. For ECCS it is to fail as-is to avoid a spurious actuation.



Clause 4.12: *Any other special design basis that may be imposed on the system design (example: diversity, interlocks, regulatory agency criteria).*

Any regulatory agency criteria and interlocks in the design basis will be carried over to the new PPS. Due to the integration of HPCI and RCIC functions within the PPS, certain design basis statements in the UFSAR will need to be updated. For instance, UFSAR, Chapter 7.2.11.1 currently states, “*The reset control for the HPCI/RCIC isolation logics do not strictly meet the intent of Bulletin 80-06. If the isolation logic is reset with the valve control switches in the open position, the isolation valves will open, but we believe the design is acceptable. There are two completely independent isolation logics for the HPCI and RCIC. Each of these logics consists of two logic channels, one for the inboard valves and one for outboard valves.*” For the PPS there are now four independent logic channels performing both HPCI and RCIC logic, with a Diverse Protection System in the unlikely event the PPS fails due to a CCF.

### 3.3.2 IEEE Std 603-1991 Applicable Clauses for New System Functions

This section demonstrates compliance to the applicable clauses in IEEE Std 603-1991 for new system functions as identified in ISG-06 (Reference 1), Section D.2.3.1.

#### 3.3.2.1 IEEE Std 603-1991 Clause 5.2 and 7.3

IEEE Std 603-1991, Clause 5.2, Completion of Protective Action states:

*The safety systems shall be designed so that, once initiated automatically or manually, the intended sequence of protective actions of the execute features shall continue until completion. Deliberate operator action shall be required to return the safety systems to normal. This requirement shall not preclude the use of equipment protective devices identified in 4.11 of the design basis or the provision for deliberate operator interventions. Seal-in of individual channels is not required.*

The PPS System Requirements Specification (Reference 2), Requirement PPS-SyRS-372 requires the PPS to ensure the protection actions, once started at the system level or lower, continue to completion. When the LCL sends a system level actuation signal to the ILP and the ILP subsequently sends the actuating component signal to the CIM, [

]<sup>a,c</sup>

IEEE Std 603-1991, Clause 7.3, Completion of Protective Action states:

*The design of the execute features shall be such that once initiated, the protective actions of the execute features shall go to completion. This requirement shall not preclude the use of equipment protective devices identified in 4.11 of the design basis or the provision for deliberate operator interventions. When the sense and command features reset, the execute features shall not automatically return to normal; they shall require separate, deliberate operator action to be returned to normal. After the initial protective action has gone to completion, the execute features may require manual control or automatic control (that is, cycling) of specific equipment to maintain completion of the safety function.*

For the PPS, Constellation considers the CIM and the HARP as part of the execute features described in IEEE Std 603-1991. [

]<sup>a,c</sup>



[<sup>a,c</sup> The PPS requires the operator to manually reset the SCRAM,<sup>195</sup> NSSSS<sup>196</sup>, and ECCS outputs<sup>197</sup>.

### 3.3.2.2 IEEE Std 603-1991 Clause 5.5

IEEE Std 603-1991, Clause 5.5, System Integrity states:

*The safety systems shall be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis.*

The same existing RPS, ECCS, and NSSSS logic is employed in the PPS, with the exception of more robust coincidence logic in certain circumstances and changes in logic described in Section 3.3. The existing logic was licensed to meet the full range of applicable conditions in the LGS design basis for the safety functions to be accomplished. The PPS equipment undergoes an equipment qualification program to ensure the PPS equipment will function properly in all applicable conditions enumerated in the design basis.<sup>198</sup>

### 3.3.2.3 IEEE Std 603-1991 Clauses 5.7, 6.5, 6.5.1 and 6.5.2

IEEE Std 603-1991 Clause 5.7 is addressed in Section 3.2.24.1.2.

IEEE Std 603-1991 Clause 6.5.1 states:

*Means shall be provided for checking, with a high degree of confidence, the operational availability of each sense and command feature input sensor required for a safety function during reactor operation. This may be accomplished in various ways; for example:*

- (1) by perturbing the monitored variable,*
- (2) within the constraints of 6.6, by introducing and varying, as appropriate, a substitute input to the sensor of the same nature as the measured variable, or*
- (3) by cross-checking between channels that bear a known relationship to each other and that have readouts available.*

The DMP PPS project is using the existing sensors and terminating the sensor cabling to the PPS termination units (see Section 3.5.3). The existing technical specifications incorporate Channel Functional Test within the definition of Channel Calibration. To unwind this relationship, the LAR technical specification markups will create a new term specifically for the PPS: Sensor Channel Calibration. This new definition will require an adjustment, as necessary, of the sensor output such that it responds with the necessary range and accuracy to known values of the parameter which the channel monitors.<sup>199</sup> The PPS will be performing automatic channel comparisons of the same measured values.<sup>200</sup>

IEEE Std 603-1991 Clause 6.5.2 states: *One of the following means shall be provided for assuring the operational availability of each sense and command feature required during the post-accident period:*

- (1) Checking the operational availability of sensors by use of the methods described in 6.5.1.*



- (2) *Specifying equipment that is stable and retains its calibration during the post-accident time period.*

The PPS equipment undergoes an equipment qualification program to validate that the equipment can survive design basis events and continue to function after the design basis event. The equipment qualification summary report (Reference 36) summarizes the equipment qualification tests and analyses performed and describes how these tests and analyses bound the LGS design basis requirements.

#### **3.3.2.4 IEEE Std 603-1991 Clause 5.8**

This clause is addressed in Sections 3.2.24.1.3 through 3.2.24.1.6.

#### **3.3.2.5 IEEE Std 603-1991 Clause 5.9**

IEEE Std 603-1991 Clause 5.9, Control of Access states: *The design shall permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof.*

Control of access is protected by a number of defense in depth measures. The PPS MTP requires two unique key switches in order to allow certain configuration changes to the system. One is the function enable (FE) key switch for changing addressable constants and enabling system test features, and an SLE key switch to allow changes to the PPS AC160 controller software (see Section 3.2.21 for SLE compliance to DI&C-ISG-04).

To perform functions in the MTP, the maintenance technician must first obtain a key to unlock the PPS Maintenance and Test Cabinet that houses the MTP and ITP.<sup>201</sup> The PPS cabinet door open/close status is monitored by the PPS and sent to the DCS over the AOI.<sup>202</sup> Certain service and test functions require the PPS channel to be in bypass prior to these functions being performed (e.g., Section 3.2.12.3).

The access controls that are utilized are provided in more detail as follows:

1. Access to the PPS cabinet is administratively controlled by door key locks to protect against unauthorized access.<sup>203</sup>
2. An FE key will be required for any addressable constant or system state changes (e.g., test).<sup>204</sup>
3. A visual alert on the SD appears when the MTP FE key switch is in the enable position.<sup>205</sup>
4. An SLE key will be required for any software updates to the AC160.<sup>206</sup> This key switch in combination with manually connecting and disconnecting the programming cable to the processor is a physical disconnect of the serial port connection between the MTP (or engineering workstation) and a processor module.<sup>207</sup> Switching the SLE switch to the ENABLE position [ ]<sup>a,c</sup> in the MTP that stores the AC160 software tool to load AC160 Controller software. The MTP is no longer functional when the MTP is rebooted after the SLE key switch is in the Enable position. The AC160 programming tool is used on the MTP. All interfaces to the MTP (e.g., AOI datalink, AF100, etc.) will time out and the PPS send out an alert.<sup>208</sup>



5. CRC checks are implemented on both the AC160 controllers and on the SD and MTP for both the non-volatile program and data storage areas and memory.<sup>209</sup>
6. During operation, a CRC monitoring process actively checks both the AC160 controllers and on the SD and MTP non-volatile program and data storage areas and produces PPS channel alerts when deviations are detected. These alerts are displayed on the PPS MTP and SD and sent to the DCS via the AOI datalink (see Section 3.2.12.2).<sup>210</sup>

The SD in the control room is not configured to be able to download software to the AC160. An SLE switch is required in order for that capability to exist and there is no SLE switch for the SD.<sup>211</sup> For the LGS PPS, changing the SD software itself will require attaching an external keyboard to the SD. During normal operation, there is no keyboard and therefore there is no mechanism for inadvertent loading of SD software. This design mitigates the vulnerability of unintended software changes being made to the safety system from the SD.

### 3.3.2.6 IEEE Std 603-1991 Clause 5.10

IEEE Std 603-1991 Clause 5.10, Repair states: *The safety systems shall be designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment.*

Section 3.2.12 describes the System Status display on both the SD and MTP. This display provides hardware operability status down to the individual channel on an AC160 I/O module. This facilitates timely recognition, location, and replacement of malfunctioning equipment. Typically, failed modules are swapped out with a spare to facilitate timely repair of the system. The PPS hardware does not need periodic adjustment.<sup>212</sup>

### 3.3.2.7 IEEE Std 603-1991 Clause 5.13

IEEE Std 603-1991, Clause 5.13, Multi-Unit Stations states, “*The sharing of structures, systems, and components between units at multi-unit generating stations is permissible provided that the ability to simultaneously perform required safety functions in all units is not impaired. Guidance on the sharing of electrical power systems between units is contained in IEEE Std 308-1980 [1]. Guidance on the application of the single failure criterion to shared systems is contained in IEEE Std 379-1988 [5]*”

The PPS itself is not a shared System, Structure or Component (SSC) between units. The LGS design basis includes the sharing between Units 1 and 2, the secondary containment isolated ventilation Zone III. The secondary containment is divided into three isolated ventilation zones. Zones I and II consist of the reactor enclosures which surround the primary containments of Units 1 and 2, respectively. Zone III consists of the common refueling area above the reactor enclosures.

Each of the ventilation zones is provided with independent HVAC systems designed to operate during normal plant operation and during shutdown. Zone III has a separate ventilation system, with both units providing redundant ventilation infrastructure. The ability to procedurally combine either of the reactor enclosure secondary containment zones to the common refueling area secondary containment zone exists in the LGS design basis and is a function of the PPS. PPS will automatically isolate the appropriate ventilation zones of the secondary containment upon the following conditions:



1. High radiation in the refueling area exhaust ducts
2. High radiation in the reactor enclosure exhaust ducts
3. Low differential pressure in the referenced zone
4. LOCA signal (Low reactor water level or high drywell pressure)
5. Manual initiation signal from the main control room.

When the zones are combined, the isolation signals for either of the zones will isolate both of the combined zones as required.

The control of this shared resource between units, as described, already exists in the LGS design basis and the function described for the PPS is the same function that is performed by the existing safety system.

### 3.3.2.8 IEEE Std 603-1991 Clauses 6.6 and 7.4

IEEE Std 603-1991 Clause 6.6, Operating Bypasses states: *Whenever the applicable permissive conditions are not met, a safety system shall automatically prevent the activation of an operating bypass or initiate the appropriate safety function(s). If plant conditions change so that an activated operating bypass is no longer permissible, the safety system shall automatically accomplish one of the following actions:*

- (1) *Remove the appropriate active operating bypass(es).*
- (2) *Restore plant conditions so that permissive conditions once again exist.*
- (3) *Initiate the appropriate safety function(s).*

The PPS provides permissives for manual operating bypasses when plant conditions are appropriate and will remove these permissives when the plant conditions are no longer appropriate.<sup>213</sup> The PPS also initiates automatic bypasses consistent with the current design basis (see Section 3.2.24.1.5). The emergency operating procedures (EOPs) or Severe Accident Guidelines (SAG) call for bypassing or defeating of interlocks to allow operation of specific equipment under administrative control, for example, by passing or defeating the low RPV water level (Level 1) automatic isolation of the MSIVs to allow the MSIVs to be manually open to establish the use of the main condenser as a heat sink if specific conditions are met. PPS provides the capability at the SDs to bypass or defeat specific interlocks under administrative control. The use of these logic bypasses or overrides does not conflict with the design and licensing basis, but does not meet the criteria of this clause. UFSAR Section 15.0.6 provides the licensing basis vs. the Emergency Procedure Guidelines.

IEEE Std 603-1991 Clause 7.4, Operating Bypass states: *Whenever the applicable permissive conditions are not met, a safety system shall automatically prevent the activation of an operating bypass or initiate the appropriate safety function(s). If plant conditions change so that an activated operating bypass is no longer permissible, the safety system shall automatically accomplish one of the following actions:*

- (1) *Remove the appropriate active operating bypass(es).*
- (2) *Restore plant conditions so that permissive conditions once again exist.*
- (3) *Initiate the appropriate safety functions).*



For the PPS, Constellation considers the CIM and HARP part of the IEEE Std 603 Execute Features. Operating bypasses originate at the PPS sense and command portion of the architecture (i.e., BPL and LCL) and their effects flow down to the CIM and HARP.

### 3.3.2.9 IEEE Std 603-1991 Clauses 6.7 and 7.5

IEEE Std 603-1991 Clause 6.7, Maintenance Bypass states: *Capability of a safety system to accomplish its safety function shall be retained while sense and command features equipment is in maintenance bypass. During such operation, the sense and command features shall continue to meet the requirements of 5.1 and 6.3.*

*EXCEPTION One-out-of-two portions of the sense and command features are not required to meet 5.1 and 6.3 when one portion is rendered inoperable, provided that acceptable reliability of equipment operation is otherwise demonstrated (that is, that the period allowed for removal from service for maintenance bypass is sufficiently short to have no significantly detrimental effect on overall sense and command features availability).*

The PPS (excluding the CIM and HARP) is a four-channel sense and command system. In the case of four channel inputs for a protective function, the Technical Specifications will define the minimum operable channels as three because the IEEE Std 603-1991 Clause 5.1, Single Failure Criterion, can still be met in that PPS configuration (that is, one channel in bypass and three channels operable). Should the number of operable channels be less than the minimum operable channels, the Limiting Condition for Operation (LCO) is not met, and the Actions are entered.

The actuating divisions interfacing existing LGS equipment is defined in the System Requirements Specification (Reference 2). The proposed PPS Technical Specifications will require four operable divisions to satisfy the LCO.

IEEE Std 603-1991 Clause 7.5, Maintenance Bypass states: *The capability of a safety system to accomplish its safety function shall be retained while execute features equipment is in maintenance bypass. Portions of the execute features with a degree of redundancy of one shall be designed such that when a portion is placed in maintenance bypass (that is, reducing temporarily its degree of redundancy to zero)', the remaining portions provide acceptable reliability.*

For the PPS, Constellation considers the CIM and HARP as IEEE Std 603 Execute Features. Since the CIM and the relay in the HARP have a one-for-one correspondence with the actuating component, the same LGS operational procedures for identifying an inoperable actuating component for maintenance would apply to the CIM and HARP relay that actuate that component. In other words, an inoperable CIM or HARP relay is identical to an inoperable actuating component and the same LGS operational procedures would apply. The level of redundancy of the CIM and HARP directly mirror the level of redundancy of the existing actuating components in the plant.



### 3.3.2.10 IEEE Std 603-1991 Clause 6.8

IEEE Std 603-1991 Clause 6.8.1, Setpoints states: *The allowance for uncertainties between the process analytical limit documented in Section 4.4 and the device setpoint shall be determined using a documented methodology. Refer to ISA S67.040-1987 [18].*

The PPS is only changing out the logic portions of the existing RPS, ECCS and NSSSS. The existing analog sensors and actuators will remain and be external interfaces to the PPS. The only area in which accuracy of the PPS would be of consideration is the accuracy of the analog input card and in particular the analog to digital conversion function.

LGS PPS will be using the AI688 analog input module. It is an NRC-approved AC160 analog input module since 2013 (Reference 3, Section 11).

The Westinghouse PPS accuracy calculation (Reference 60) is provided to Constellation to determine if the existing RPS, NSSSS, and ECCS setpoints are appropriate or need to be changed. If the PPS setpoints need to be changed, as a result of the accuracy calculation, then Constellation's NRC approved setpoint methodology, as defined in UFSAR section 7.1.2.5.25, is used to create new values for RPS, NSSSS, and ECCS process setpoints to ensure LGS operation stays within its analytical limits.

IEEE Std 603-1991 Clause 6.8.2, Setpoints states: *Where it is necessary to provide multiple setpoints for adequate protection for a particular mode of operation or set of operating conditions, the design shall provide positive means of ensuring that the more restrictive setpoint is used when required. The devices used to prevent improper use of less restrictive setpoints shall be part of the sense and command features.*

See the response to Clause 6.8.1. There is only one setpoint per protection function in the PPS.<sup>214</sup> Any mode dependency is handled by operating bypasses for specification safety functions.<sup>215</sup>

### 3.3.2.11 IEEE Std 603-1991 Clause 5.3

IEEE Std 603-1991 Clause 5.3 Quality states: *Components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Safety system equipment shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program (ANSI/ASME NQA1-1989 [16]).*

Westinghouse is a 10 CFR 50 Appendix B (Appendix B) vendor that provides nuclear safety-related products and services. The PPS components are commercially dedicated in accordance with the Westinghouse Appendix B Quality Assurance procedures. The configuration control of these components, the manufacturing of the PPS, its inspection, and testing are governed by the procedures in the Westinghouse Appendix B Quality Assurance procedures.

IEEE Std 7-4.3.2-2003, Clause 5.4.2 Qualification of existing commercial computers, states: *NOTE-See Annex C for more information about commercial grade item dedication.*

*The qualification process shall be accomplished by evaluating the hardware and software design using the criteria of this standard. Acceptance shall be based upon evidence that the digital system or*



*component, including hardware, software, firmware, and interfaces, can perform its required functions. The acceptance and its basis shall be documented and maintained with the qualification documentation.*

*In those cases in which traditional qualification processes cannot be applied, an alternative approach to verify a component is acceptable for use in a safety-related application is commercial grade dedication. The objective of commercial grade dedication is to verify that the item being dedicated is equivalent in quality to equipment developed under a 10 CFR 50 Appendix B program [B 16].*

*The dedication process for the computer shall entail identification of the physical, performance, and development process requirements necessary to provide adequate confidence that the proposed digital system or component can achieve the safety function. The dedication process shall apply to the computer hardware, software, and firmware that are required to accomplish the safety function. The dedication process for software and firmware shall, whenever possible, include an evaluation of the design process. There may be some instances in which a design process cannot be evaluated as part of the dedication process. For example, the organization performing the evaluation may not have access to the design process information for a microprocessor chip to be used in the safety system. In this case, it would not be possible to perform an evaluation to support the dedication. Because the dedication process involves all aspects of life cycle processes and manufacturing quality, commercial grade item dedication should be limited to items that are relatively simple in function relative to their intended use.*

*Commercial grade item dedication involves preliminary phase and detailed phase activities. These phase activities are described in 5.4.2.1 through 5.4.2.2.*

This clause and subclauses 5.4.2.1 and 5.4.2.2 are criteria for commercial grade dedication. In RG 1.152, Revision 3, the NRC stated, in regards to endorsing the standard's Annex C, "Dedication of Existing Commercial Computers, *Electric Power Research Institute Topical Report (TR)-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," issued October 1996 (Ref. 10) contains adequate guidance [for commercial grade dedication], which the NRC has endorsed.* Since these clauses (5.4.2, 5.4.2.1 and 5.4.2.2) are considered "general guidance" for commercial grade dedication in RG 1.152, Revision 3, and the statement above regarding EPRI TR 106439 has being adequate NRC-endorsed guidance for commercial grade dedication, addressing these clauses is bounded by compliance to EPRI TR-106439. The commercial grade dedication of the Common Q Platform is described in the Common Q Topical Report (Reference 4), Section 10. The commercial dedication process was reviewed and approved by the NRC using EPRI TR-106439 criteria.

### **3.3.3 System Requirements Documentation (D.2.3.3 and D.2.3.3.1)**

Section D.2.3.3.1 of ISG-06 (Reference 1) defines the expected content for the system requirements specification. Table 3.3-2 cross references the list of ISG-06 expected content to the PPS System Requirements Specification (Reference 2) or the LGS System Design Specification (Reference 21). Revision 0 of this Licensing Technical Report describes the plant change for the license amendment. References 2 and 21 are design documents that incorporate these changes into requirements. These design documents currently have open items that will be closed in Revision 1. The subsequent revisions of those documents will provide the additional requirements encompassing the plant changes described in this document for the license amendment.



**Table 3.3-2 ISG-06 System Requirements Document Content**

ISG-06 System Requirements Document Content	<p>Limerick Generating Station Plant Protection System Digital Modernization Project System Requirement Specification, WNA-DS-04899-GLIM (Reference 2)</p> <p>OR</p> <p>System Design Specification for the Limerick Generating Station Plant Protection System Digital Modernization Project, WNA-DS-04900-GLIM (Reference 21).</p>
<i>1.a. defining system requirements for the I&amp;C functions in the modification's scope and the modification's effects on associated systems and equipment within the plant's safety analysis</i>	<p>Reference 2 establishes the PPS Functional Requirements. These functional requirements define the PPS effects on the associated system and equipment it interfaces to within the LGS safety analysis.</p> <p>Reference 21 establishes the PPS System Requirements. These system requirements define the PPS effects on the associated systems and equipment it interfaces to within the LGS safety analysis.</p>
<i>1.b. defining the plant layout for the modification scope</i>	<p>The plant layout of the modification is divided between the AER and the MCR. The AER Equipment includes the PPS cabinets and MCR equipment includes the SDs (see Reference 21 PPS-SyDS-2140 and Section 3.8.2 respectively).</p>
<i>1.c. defining the operational context for the modification scope and changes resulting from the modification</i>	<p>Reference 2 and 21, Sections 1.2 define the modification scope. The modification scope is the integration of the RPS, PCRVICS, and ECCS logic functions to a PPS. The operational context for the modification scope is contained in the Functional Requirements section of Reference 2 (Section 5). The source requirements for the modification for the PPS is Reference 5.</p>
<i>1.d. structuring the overall I&amp;C architecture and assigning I&amp;C functions to the modification scope</i>	<p>Reference 21 Section 2 defines the PPS architecture and Section 3 describes the allocation of functions to the PPS architecture.</p>



ISG-06 System Requirements Document Content	<p>Limerick Generating Station Plant Protection System Digital Modernization Project System Requirement Specification, WNA-DS-04899-GLIM (Reference 2)</p> <p>OR</p> <p>System Design Specification for the Limerick Generating Station Plant Protection System Digital Modernization Project, WNA-DS-04900-GLIM (Reference 21).</p>
<i>1.e. identifying the design criteria for the modification scope, including ensuring that features providing defense-in-depth in the existing system are not compromised and minimizing the potential for common-cause failure (CCF)</i>	The design criteria are the Functional Requirements defined in Section 5 of Reference 2. The modification represents the integration of the existing RPS, PCRVICS, and ECCS logic functions into a PPS. A D3 Analysis (Reference 11) analyzes the PPS architecture for vulnerabilities to a CCF and defines required diverse protection functions in case the PPS suffers a CCF. See the discussion on CCF in Section 3.2.23.
<i>1.f. describing how the modification fits within the overall architecture of the plant's I&amp;C systems and any changes to the architecture</i>	The modification is the integration of the RPS, PCRVICS, and the ECCS logic circuits to a digital PPS. As stated in 1.b, Reference 21 defines the equipment that will be in the AER and the MCR. The PPS interfaces with existing sensors and actuating equipment.
<i>1.g. defining system interfaces and the reasons for the interfaces (see Section D.2.5.1 of this ISG)</i>	Section 6 in Reference 2 and Section 4 in Reference 21 define the system interfaces. For each interface requirement, a rationale for the requirement is provided.

The Reference 2 system requirements specification is the basis for the development of Reference 21 (system design specification). Reference 21 is considered the hardware requirements for the hardware detailed design. Reference 2 system requirements, the PPS Functional Logic Diagrams (see References 47 - 50), as well as Reference 21 system design specification are the input requirements for the software design. The hardware design process requirements are defined by the Westinghouse 10 CFR 50 Appendix B Quality Assurance procedures. The Westinghouse NRC-approved Appendix B quality assurance program is in accordance with NRC Regulatory Guide 1.28, Revision 4, with clarifications, alternatives, and exceptions defined in Appendix A of the NRC-approved QA manual.



The provisions for PPS equipment quality are defined in the Digital Modernization Project Quality Plan Reference 44.

Reference 2 (PPS System Requirements Specification) defines the functional requirements (Section 5) and performance requirements in Section 7.

Section 7.2 (PPS System Design Specification) Reference 21 defines the accuracy requirements for the input signals based on the total uncertainties attributable to:

- 1) loading effects
- 2) reference voltage supply regulation
- 3) electrical noise
- 4) linearity
- 5) A/D converter power supply sensitivity
- 6) quantization

The PPS interlock requirements are defined in the following sections of the PPS system requirements specification (Reference 2): 5.3.1.3 (HPCI), 5.3.3.3 (Core Spray), 5.3.4.3 (RHR/LPCI), and 5.3.5.3 (RCIC).

The Reference 2 System Requirements Specification defines the requirements for boundary interfaces with other systems in Section 6, and independence requirements via requirements PPS-SyRS-317 and PPS-SyRS-405. In Reference 21 System Design Specification, the following independence requirements are defined: PPS-SyDS-390, PPS-SyDS-1921, Section 10.6.1, PPS-SyDS-1934, and Section 10.7.

The PPS will replace existing logic cabinets for RPS, PCRVICS, and ECCS with new logic cabinets. Fitting the new PPS cabinets in the existing RPS, PCRVICS and ECCS logic cabinet area in the AER, and the control board are the physical constraints in the plant. There is also the constraint in regards to the control board in the main control room where the Common Q Flat Panel Display System will be installed for the PPS safety displays. The design of the PPS equipment will take into account fitting within the existing AER and control board space constraints.

The PPS System Requirements Specification (Reference 2) defines the operator and maintenance technician interface requirements in Sections 4.1.2 and 5.4. The PPS system design specification (Reference 21) defines the operator and maintenance technician interface requirements in Sections 3.7, 3.8, and 4.3.

The requirements for equipment qualification to environmental conditions is specified in Section 9 of Reference 2 and Section 10 in Reference 21.

The Reference 2 System Requirements Specification defines the service/test functions that will be deployed for the PPS in Sections 5.4.2 and 8. The Reference 21 system design specification defines the service/test functions that will be deployed for the PPS in Sections 3.8.1 and 6.



This LTR references Revision 0 of the PPS System Requirements Specification (Reference 2) and the PPS System Design Specification (Reference 21). These are preliminary revisions that will require a subsequent Revision 1 for each.



### 3.4 PPS - FUNCTION ALLOCATION (D.2.4 AND D.2.4.1)

In most cases, the BPL in each channel reads the sensor inputs and compares the measured value against a setpoint and sends this trip/actuation signal to the LCL (see the PPS architecture Level 1 description in Section 3.2). There are exceptions to this as described below for reactor trip functions with response times  $\leq 124$  ms. This is described in Section 3.4.1.

The LCL in each division receives both the trip/actuation signals and bypass statuses for each trip/actuation signal for all PPS functions from the four channels of BPL (see the PPS architecture Level 2 description in Section 3.2 and the LCL description in Section 3.5.1.1).

The ILPs and CIMs in each division perform the ECCS and NSSSS actuation functions. The ILPs receive the system level actuation signals from the LCL and perform a fanout of component actuation signals to the CIMs that interface with the safety-related actuating components via the HARP (see the PPS architecture Level 3 description in Section 3.2 and the ILP and CIM descriptions in Section 3.5.1.1). The ILP receives inputs directly to perform asset protection of actuating components (see Section 3.2.4).

The divisional allocation shown in Table 3.1.3-1 is unchanged in the new PPS architecture.

The allocation of service/test functions is described in Section 3.2.12. Some of these functions are operator or technician initiated calibrations and tests. Other functions are reported status from the self-diagnostic functions within the AC160 controllers. These are described in Section 6 of the PPS System Design Specification (Reference 21).

#### 3.4.1 PPS Response Times

The PPS allocated response times are defined in Section 7 of the PPS System Requirements Specification (Reference 2). The PPS Response Time Analysis (Reference 56) substantiates that the architecture and software will meet these response time requirements.

To provide an example of the methodology for calculating the maximum response time for the PPS, three types of RPS trip functions are presented.

##### RPS Trip Functions with $\leq 50$ ms Response Time

The following reactor trip functions require the PPS to respond in  $\leq 50$  ms:

- APRM 2-Out-Of-4 Voter
- Main Steam Line Isolation Valve - Closure
- Turbine Stop Valve - Closure
- Turbine Control Valve Fast Closure, Trip Oil Pressure - Low

Each of these trip functions are initiated by a contact input (one for each Channel). [

] <sup>a,c</sup>



[

] <sup>a,c</sup>



a,c

**Figure 3.4-1 RPS Trip Functions  $\leq 50$  ms Response Time**



RPS Trip Functions for Reactor Vessel Pressure and Reactor Vessel Water Level

The PPS response requirements for these two RPS trip functions are:

- Reactor Vessel Pressure – High ( $\leq 160$  ms)
- Reactor Vessel Water Level – Low, Level 3 ( $\leq 166$  ms)

Each of these trip functions are initiated by a 4-20ma signal processed by the BPL in each Channel. [

] <sup>a,c</sup>



a,c

**Figure 3.4-2 RPS Trip Functions Reactor Vessel Pressure and Reactor Vessel Water Level**



RPS Trip Functions with > 166 ms Response Time

The remaining trip functions (with the exception of IRM Neutron Flux, see Section 3.2.3.1) are initiated by a 4-20ma signal processed by the BPL in each Channel, which then sends the trip signal to each LCL in all four divisions over the HSL. [

functions. [ ]<sup>a,c</sup> Figure 3.4-3 is the timing diagram for these trip

] <sup>a,c</sup>



**Figure 3.4-3 RPS Trip Functions with > 124 ms Response Time**



The same methodology is used in Reference 56 for the ECCS and NSSSS functions involving the ILP, CIM, and HARP.

### **3.5 PPS -SYSTEM INTERFACES (D.2.5)**

This section describes each of the PPS external interfaces and the PPS cross division communication. The PPS human-system interfaces are discussed in Sections 3.2.7 and 3.2.8 to address DI&C-ISG-06 D.2.5.1 items 1.b and 1.c.

#### **3.5.1 Transmitter Consolidation**

The LGS has multiple identical transmitters on reactor vessel instrumentation legs to provide input to logic channels across the existing trip unit and relay logic systems for the nuclear safety systems (RPS, ECCS, and NSSSS). The instrumentation includes reactor vessel pressure, reactor vessel water level, and drywell pressure.

In the existing design, the RPS, ECCS, NSSSS, and RRCS have duplicate channel-specific transmitters for the same range of a measured variable to support each system independently. The Digital Modernization Project (DMP) will consolidate these duplicated, similarly ranged, sets of transmitters, and use one set of similarly ranged transmitters in the PPS and RRCS. This is in lieu of duplicating similarly ranged transmitters for each function (i.e., RPS, ECCS, NSSSS). Figure 3.5-1 is a markup of a portion of the Nuclear Boiler Vessel Instrumentation Piping & Instrumentation Diagram (P&ID) that shows a portion of these transmitters and those transmitters that will be abandoned in place (by red boxes) for the PPS implementation.

An example of the consolidation of transmitters is shown in Table 3.5.1-1 for reactor vessel water level 2. As shown in this table, LT-1(2)N081A(BCD) will be used for multiple PPS functions (i.e., NSSSS, RHR, ADS, RCIC, HPCI, and RRCS). There will be two sets for water level: narrow range and wide range. Note that RRCS will share the same transmitters in a manner to meet the independence and diversity requirements of 10 CFR 50.62, as described in Section 9.3.1. The other Reactor Vessel Water Level 2 signals will be abandoned in place.

A similar example is Reactor Vessel Pressure. One set of channelized transmitters will support multiple functions as shown In Table 3.5.1-2.



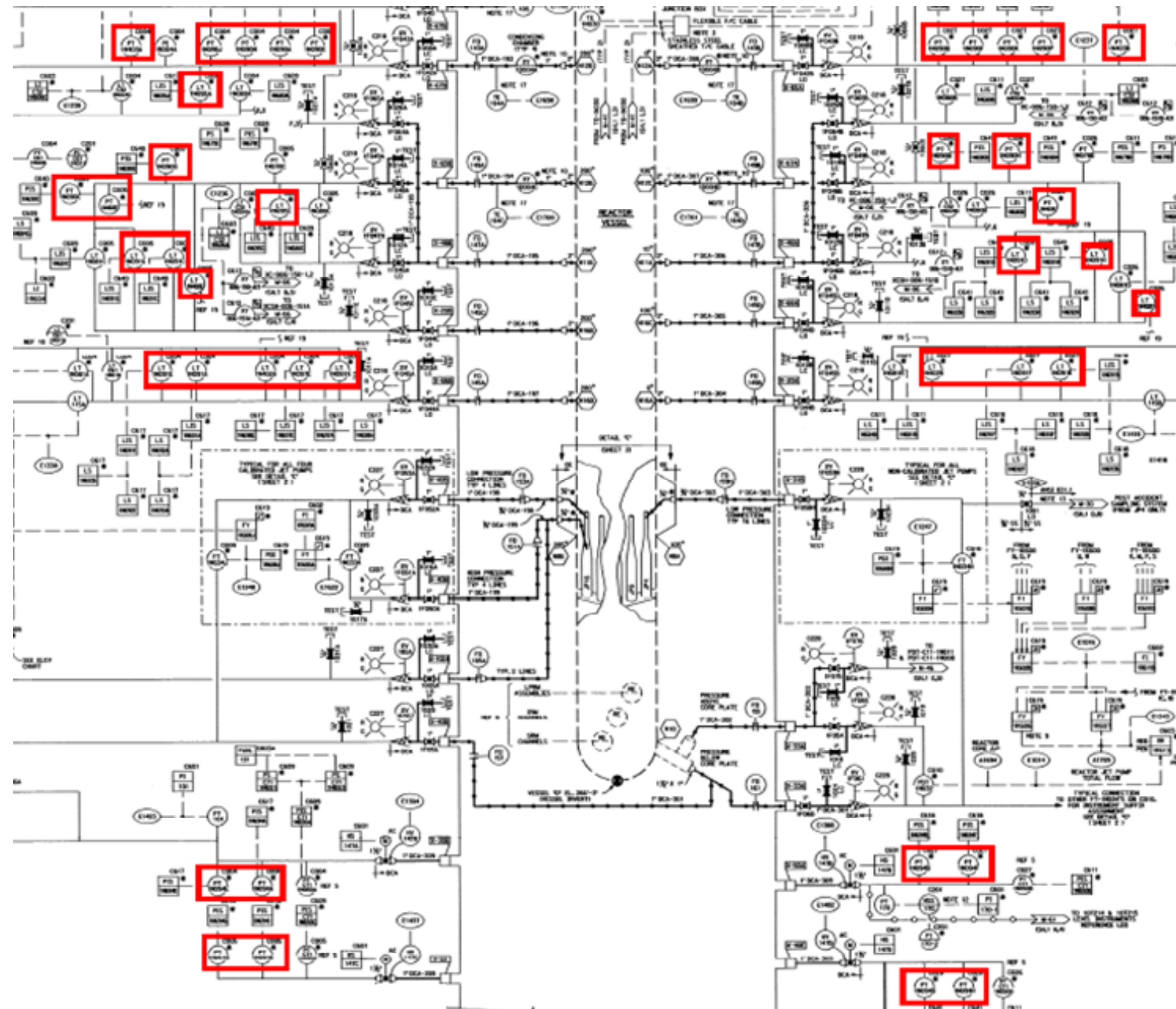


Figure 3.5-1 Nuclear Boiler Vessel Instrumentation P&amp;ID



Table 3.5.1-1 Example of Transmitter Consolidation for Reactor Vessel Water Level 2

Existing Reactor Pressure Vessel Level Instrumentation for Reactor Water Level 2							Proposed RWL 2
Instrument	Function	Range	Variable Leg Nozzle	Nozzle Height	Reference Leg Nozzle	Nozzle Height	Function
LT-1(2)N081A	NS4	WR	N16D	366"	N12D	599"	NS4/CS/RHR/ADS/RCIC/HPCI/RRCS
LT-1(2)N081B	NS4	WR	N16A	366"	N12A	599"	NS4/CS/RHR/ADS/RCIC/HPCI/RRCS
LT-1(2)N081C	NS4	WR	N16B	366"	N12B	599"	NS4/CS/RHR/ADS/RCIC/HPCI/RRCS
LT-1(2)N081D	NS4	WR	N16C	366"	N12C	599"	NS4/CS/RHR/ADS/RCIC/HPCI/RRCS
LT-1(2)N091A	CS(A)/RHR(A)/ADS(A), RCIC	WR	N16D	366"	N12D	599"	To be removed from service
LT-1(2)N091B	CS(B)/RHR(B), HPCI	WR	N16A	366"	N12A	599"	To be removed from service
LT-1(2)N091F	CS(B)/RHR(B), HPCI	WR	N16A	366"	N12A	599"	To be removed from service
LT-1(2)N091C	CS(C)/RHR(C)/ADS(C)	WR	N16B	366"	N12B	599"	To be removed from service
LT-1(2)N091G	CS(C)/RHR(C)/ADS(C)	WR	N16B	366"	N12B	599"	To be removed from service
LT-1(2)N091D	CS(D)/RHR(D), HPCI	WR	N16C	366"	N12C	599"	To be removed from service
LT-1(2)N091H	CS(D)/RHR(D), HPCI	WR	N16C	366"	N12C	599"	To be removed from service
LT-1(2)N091E	CS(A)/RHR(A)/ADS(A), RCIC	WR	N16D	366"	N12D	599"	To be removed from service
LT-1(2)N097A	RCIC	WR	N16D	366"	N12D	599"	To be removed from service
LT-1(2)N097E	RCIC	WR	N16D	366"	N12D	599"	To be removed from service
LT-1(2)N402A	RRCS	WR	N16D	366"	N12D	599"	To be removed from service
LT-1(2)N402B	RRCS	WR	N16A	366"	N12A	599"	To be removed from service
LT-1(2)N402E	RRCS	WR	N16B	366"	N12B	599"	To be removed from service
LT-1(2)N402F	RRCS	WR	N16C	366"	N12C	599"	To be removed from service
LT-1(2)15A	Wide Range Indication	WR	N16D	366"	N12D	599"	Wide Range Indication
LT-1(2)15B	Wide Range Indication	WR	N16A	366"	N12A	599"	Wide Range Indication

Table 3.5.1-2 Example of Transmitter Consolidation for Reactor Vessel Pressure

Transmitter	Function
PT-1N078A	RPS/NS4, CS(A)/RHR(A)
PT-1N078B	RPS/NS4, CS(B)/RHR(B)
PT-1N078C	RPS/NS4, CS(C)/RHR(C)
PT-1N078D	RPS/NS4, CS(D)/RHR(D)
PT-103A	Wide Range Indication
PT-103B	Wide Range Indication

Transmitter consolidation does not involve the existing RG 1.97 variables.



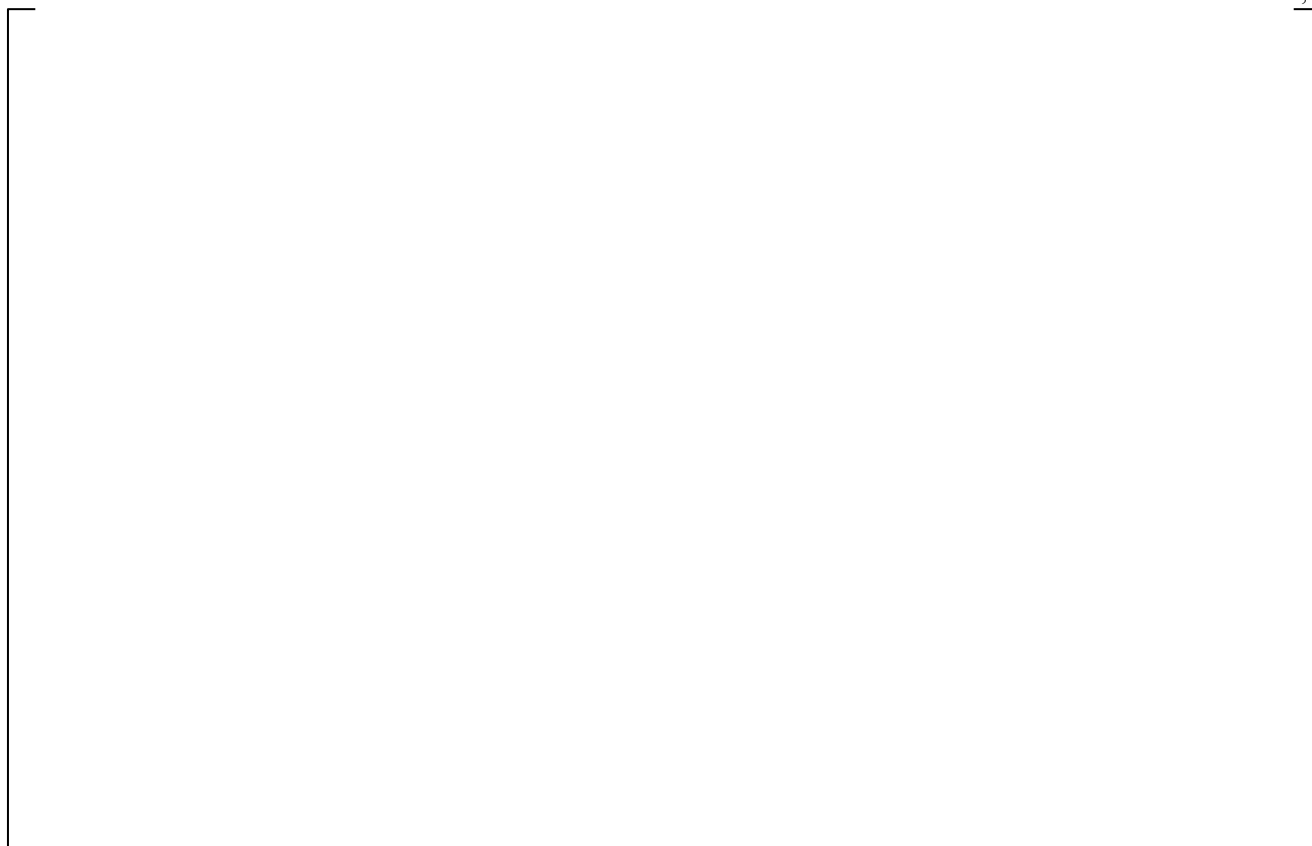
### 3.5.1.1 Safety Case for Transmitter Consolidation

Transmitter consolidation in combination with the new design architecture of the PPS provides a different approach to achieving reliability and independence that is comparable to the original reliability and independence characteristics of the existing RPS/ECCS/NSSSS design that had dedicated transmitters for each system. The PPS architecture provides for four independent bistable channels with four divisions of coincidence voting. In addition, the PPS architecture provides redundancy within each division. This improved resilience and channel sensor independence from single points of vulnerability provide the reliability and independence required by 10 CFR 50.55 a(h) and the General Design Criteria (GDCs) in 10 CFR 50 Appendix A.

Starting with the BPL channels, each BPL AC160 controller has two processor modules performing the bistable logic redundantly and providing all the trip/actuation signals to all LCLs in the four divisions using redundant HSLs (as shown by lines with FOM boxes). There are exceptions to this process as described in Section 3.4.1

The LCL segmentation in the four divisions of coincidence voting is depicted in Figure 3.5.1.1-1 and Figure 3.5.1.1-2. Figure 3.5.1.1-1 shows the dedicated processor modules performing the coincidence voting for RPS only. In most cases, PM646A-3 and PM646A-4 receive the RPS trip actuation signals from the BPL HSL either directly (as shown for PM646A-4) or indirectly (as shown in PM646A-1). In other words, the BPL HSL link represented by the cyan line goes into the PM646A-1 processor and then this data is shared with the PM646A-3 using the global memory feature of the AC160 controller as described in the Common Q Topical Report (Reference 4). PM646A-3 and PM646A-4 only perform RPS trip 2004 coincidence logic redundantly and sends out the trip signal to the RPS Trip Unit (see Figure 3.5.1.1-1). There are exceptions to this process as described in Section 3.4.1.





**Figure 3.5.1.1-1 LCL Segmentation for Reactor Trip (One Division)**

Figure 3.5.1.1-2 shows the dedicated processor modules performing the coincidence voting for ECCS and NSSSS only. [

]a,c





a,c

**Figure 3.5.1.1-2 LCL Segmentation for ECCS and NSSSS Actuation (One Division)**

Figure 3.5.1.1-3 depicts the configuration of the ILP for ECCS/NSSSS execution. As described in Section 3.2.4, the ILPs receive the division protection function actuation signals from the LCL via redundant HSLs. The ILPs compute the component fanout for the actuating function and this is performed by redundant processor modules. The component actuation signals are then transmitted to the CIMs via redundant HSLs to the CIM SRNC that handles the HSL communication. [

] <sup>a,c</sup>





**Figure 3.5.1.1-3 ILP Configuration (One Division)**



In summary, although the RPS, ECCS and NSSSS no longer have dedicated transmitters, the PPS architecture has significant redundancy to provide the same level of reliability and independence:

- The PPS architecture has four channels of BPLs to read four channels of transmitters and compare the measured values to protection function setpoints
  - Each BPL channel reads its channel's transmitters redundantly and generates trip/actuation signals redundantly, and sends these redundant signals to each of the four division LCLs
  - The LCL in each division performs the coincidence logic redundantly using separate sets of redundant processors for RPS coincidence and ECCS/NSSSS coincidence
  - The LCL in each division sends redundant hardwired RPS trip signals to the RPS TU and redundant ECCS/NSSSS actuation signals to the ILPs via HSLs
  - The ILPs in each division compute the ECCS/NSSSS component fanout using redundant processors and send the commands to the CIM SRNC using redundant HSLs
  - [
- ] <sup>a,c</sup>
- All HSL communication is unidirectional with no handshaking and internal diagnostic checks on the data (see Common Q Topical Report (Reference 4), Sections 4.5 and 5.4.1.3

The existing independent transmitters produce a certain “system” or “safety” level of reliability. The new design architecture of the PPS provides a different perspective in which independence is replaced with redundancy. This architecture, including using the same transmitters among multiple protection functions, meets the single failure criterion for all protection functions.

### 3.5.2 Cross Division Communication

Cross divisional communication in the PPS occurs via HSL or by Hardwired I/O.

There are two HSL schemes for cross division communication in the PPS architecture. The first is the BPL channel in each division reads its channel's sensors redundantly and generates trip/actuation signals redundantly and sends these redundant signals to each of the four division LCLs via HSL.

The second scheme is the cross division communication between ITPs in each division. The ITPs share sensor data from all four channels via HSL to perform channel checks on the process inputs used by the BPLs and to share redundant division information for safety display indication.

The HSL is described in the Common Q Topical Report (Reference 4) and was reviewed and approved by the NRC for cross channel communication pending closure of any relevant Plant Specific Action Items (PSAIs).

Section 3.2.21 demonstrates how communication hazards are controlled via HSL communication in compliance to DI&C-ISG-04. These cross division communication paths have no external path (e.g., human contact point) to jeopardize the secure operating environment of the PPS.

The following functions utilize Hardwired I/O for cross divisional communications:



- RPS fast trip signals (with response time less than or equal to 50 ms, see Section 3.4.1) are terminated at the LCLs and shared with the other LCLs
- RPS fast trip signals (with response time less than or equal to 160/166 ms, see Section 3.4.1) are sent from each BPL (via Digital Outputs) to each LCL (via Digital Inputs)
- Select valve statuses that are fed back to the ILPs are shared with ILPs in different divisions when the valve status provides an interlock.

### 3.5.3 Shared Sensor Interface

DPS and RRCS share sensors with the PPS in a configuration that maintains diversity and independence between the PPS and DPS/RRCS. Figure 3.5.3-1 is a typical shared sensor configuration for both the DPS and RRCS. This figure shows the 1E and non-1E boundary. At the Analog Input Termination Unit (AI TU) the 1E field signal is terminated. The TU has a second termination for the Ovation remote I/O Analog Input Module (AI). The remote AI module interfaces with the Remote Node Interface (RNI) to transmit AI signals to the DPS/RRCS. The Ovation remote AI and RNI are non-safety equipment. They are considered an associated circuit within the PPS cabinet. The remote AI and RNI configuration will undergo equipment qualification to demonstrate that the Ovation AI and RNI configuration cannot adversely affect the PPS safety function. The RNI transmits the analog input signals to the DPS/RRCS via fiber optic media to provide electrical isolation.<sup>216</sup>





**Figure 3.5.3-1 Typical configuration for Shared Sensor Data**

For contact shared inputs the field signal will be terminated at the PPS cabinet and then wired to the DPS/RRCS with a 1E isolator at the PPS cabinet to protect the PPS from electrical faults from the non-safety DPS/RRCS.

### **3.5.4 Sequence of Events**

The DCS receives Sequence of Events (SOE) data from the PPS using the Ovation SOE modules. Figure 3.5.4-1 depicts the configuration for this interface. These SOE modules are a hardwired connection from PPS Digital Output module channels. The SOE module interfaces with the Ovation RNI to transmit time



stamped data to the DCS. The Ovation SOE and RNI modules are non-safety equipment. They are considered an associated circuit within the PPS cabinet. The SOE/RNI configuration will undergo equipment qualification to demonstrate that the configuration cannot adversely affect the PPS safety function. Figure 3.5.4-1 shows the 1E and non-1E boundary for this configuration. The RNI transmits the SOE data to the DCS via fiber optic media to provide electrical isolation.<sup>217</sup>

a,c

**Figure 3.5.4-1 PPS Interface for SOE data**



### 3.5.5 MTP DCS Interface (AOI)

Each division's MTP provides a unidirectional fiber optically isolated Ethernet data link to the DCS to provide both electrical and functional isolation.<sup>218</sup> This interface is referred to as the Advant to Ovation Interface (AOI). Figure 3.5.5-1 shows the configuration of this interface. As depicted in Figure 3.5.5-1, the PPS division (i.e., MTP) cannot receive any transmission due to the nature of the Ethernet protocol used and the absence of a receive channel connection, thus the secure operational environment of the PPS channel is preserved.



**Figure 3.5.5-1 AOI Interface**

### 3.5.6 PPS Interface for Reactor Scram

Each PPS division has an RPS Reactor Scram Matrix that is described in Section 3.2.3. These Reactor Scram Matrices interface with a configuration of the HARP as shown in Figure 3.5.6-1. The Scram HARP is an interposing relay panel that interfaces to field devices powered by AC or DC voltage that draw more current than is rated for the Common Q equipment. The combination of the Reactor Scram Matrix and the HARP in each division is referred to as the RPS Termination Unit (RPS TU). Each RPS Scram Matrix interfaces with a set of normally energized solid-state relays located in the RPS TU. These relays (which interface with the Scram Pilot Solenoid Valves, the Backup Scram Solenoid Valves, and the SDV Vent and Drain Pilot Solenoid Valves) are de-energized when a scram signal comes from the respective RPS Scram Matrix. The solid-state relays in the Division 1 and 3 RPS TUs are hardwired



together to create a functional OR, so that either pair of relays de-energizing will generate a scram output from the PPS to the scram pilot solenoid valves (along with the associated aforementioned valves). Similarly, the solid-state relays in the Division 2 and 4 RPS TUs are hardwired together to create a functional OR, so that either pair of relays de-energizing will generate a scram output from the PPS to the scram pilot solenoid valves (along with the associated aforementioned valves). This is described in more detail on Figure 3.5.6-1.<sup>219</sup>

As shown in Figure 3.5.6-1, the HARP portion of the RPS TU in each division includes the MCR manual scram pushbutton input signal that will actuate the solid-state relay output relays.

The RPS TU is designed to have a maximum time delay of 12ms from the time it receives a trip command from the LCL Digital Outputs to the time the command is issued to the reactor Scram Solenoids.<sup>220</sup>



a,c



**Figure 3.5.6-1 HARP Interfaces for Reactor Scram**



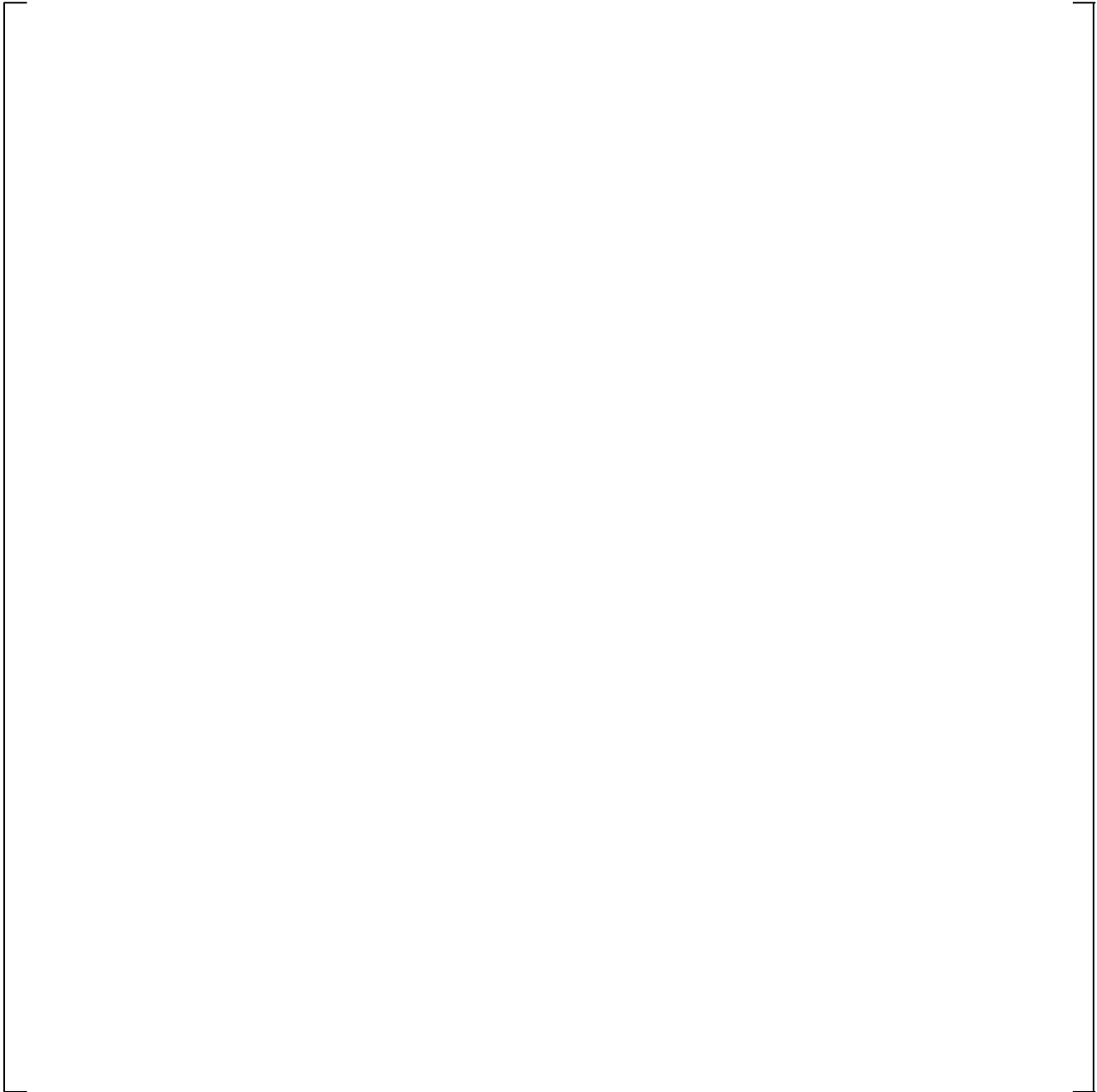
### 3.5.7 CIM Y-Port for DCS Control of Safety Related Components

Similar to the approach used for the AP1000 Protection and Safety Monitoring System (PMS), the PPS accommodates the control of safety-related components by the non-safety DCS using the CIM's Y-port.<sup>221</sup> The CIM Y-port also provides actuating component feedback. Figure 3.5.7-1 shows the configuration of this interface. There are three ports, plus the local control switch in the CIM, that can control a single safety related component. [

]<sup>a,c</sup> The X-port is the source for the PPS actuating signal for the component and the Z-port is the source for the DPS actuating signal. The Y-port is bidirectional communication with the DCS. Tables 3.2.5-1, 3.2.5-2, and 3.2.21-1 explain how the Y-port meets DI&C-ISG-04. Each Y-port signal interface with the DCS is via the Ovation Remote Node Interface (RNI) and fiber optic cable. The Ovation RNI is considered an RG 1.75 associated circuit in the PPS and undergoes equipment qualification to ensure the RNI does not adversely impact the safety function of the PPS. The fiber optic cable provides electrical isolation between the DCS and the PPS.<sup>222</sup>



a,c

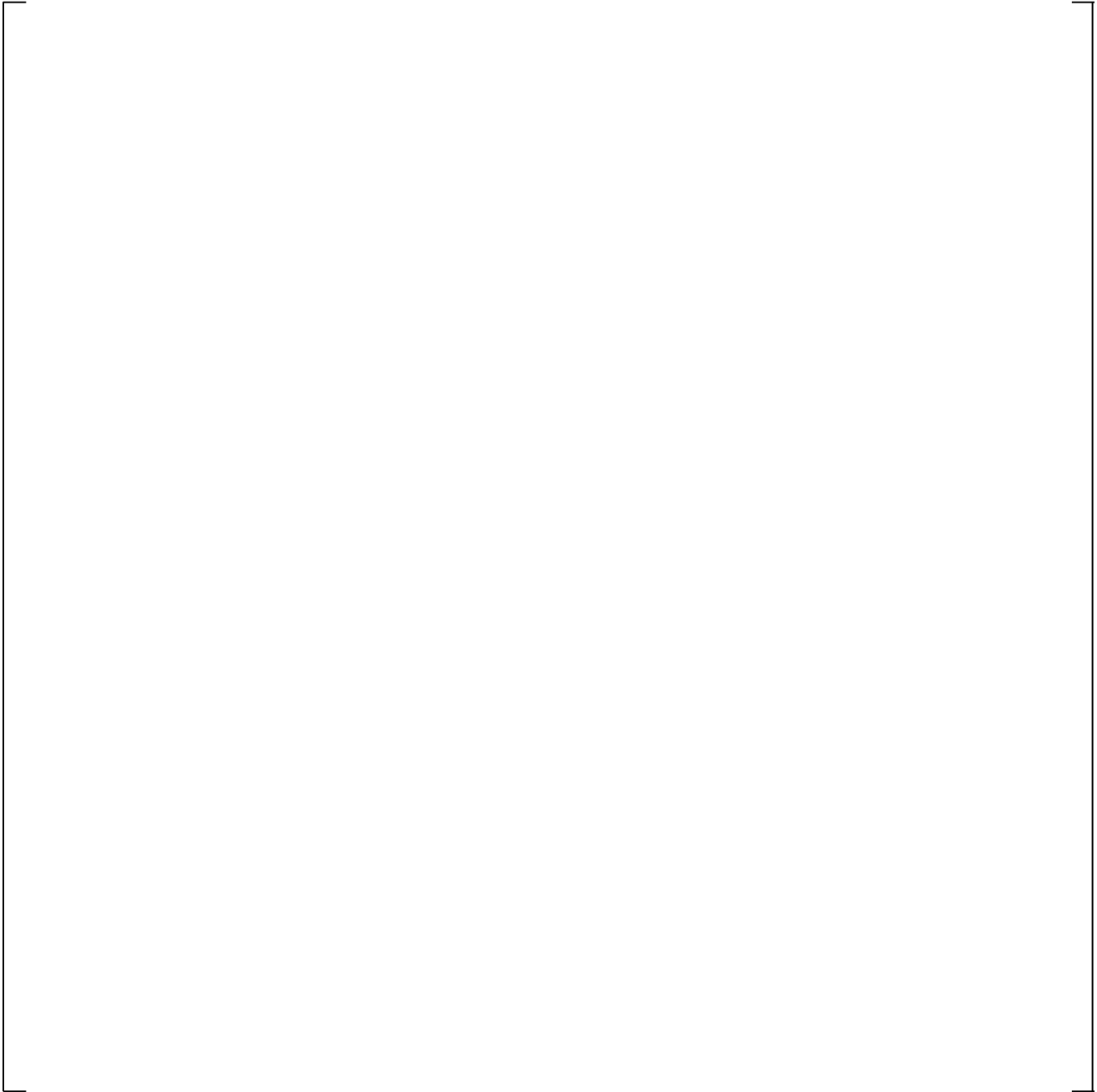


**Figure 3.5.7-1 CIM Y-Port Configuration**

### **3.5.8 CIM Z-Port DPS/RRCS Interface for Diverse Component Actuation**

The Z-port is hardwired to the DPS/RRCS for a diverse means to perform component actuation for certain protection functions in case the PPS fails to do so due to a CCF. Figure 3.5.8-1 shows the configuration for this interface. There is a 1E isolator between the Z-port and the DPS/RRCS to provide electrical isolation.





**Figure 3.5.8-1 Z-Port Interface**

### **3.5.9 CIM Interface to Actuating Components**

The PPS interfaces with various types of actuating components including MOVs, Solenoid Operating Valves (SOVs), pumps, and squib devices. The HARP is a high amperage interposing relay panel between the CIM and the actuation components that draw high current.



### 3.5.9.1 High Amperage Relay Panel (HARP)

In order to control field devices powered by AC or DC voltage that draw more current than is rated for the Common Q and CIM equipment, an interposing relay panel is provided. The HARP receives command signals from Common Q system and facilitates control of and feedback from the field actuating components. The main uses of the HARP are in controlling components through the CIM as well as the actuation of SCRAM pilot solenoid valves (see Section 3.5.6).

The HARP has the ability to control AC and DC loads up to 10A and is used when field loads exceed the switching capability of the CIM or AC160 digital outputs. There are two standard HARP configurations:

1. The HARP-SCRAM provides for a voting matrix as well as actuation of six banks of AC SCRAM solenoids and one bank of DC backup SCRAM solenoids (see Section 3.5.6).
2. The HARP-CIM provides for actuation of up to 24 CIM controlled field components, while also gathering required feedbacks that are field wetted and providing dry contacts back to the CIM or system digital inputs for use in the safety system.

The HARP uses coil-to-contact solid state relays, providing highly repeatable time response due to the absence of moving parts. The coil side of the relay is powered by the PPS cabinet power supply system. The contact side of the relay is powered by plant power. Two figures are provided to show the HARP solid state components and how they interface to the CIM and ILP (ILC in the diagram). Figure 3.5.9.1-1 is a typical HARP interface diagram showing the interplay between the CIM, HARP, ILP (ILC in the diagram), and an AC powered MOV.<sup>223</sup> Figure 3.5.9.1-2 is a typical HARP interface diagram showing the same relationships with the CIM, HARP, ILP, and a DC powered MOV.<sup>224</sup>



**Figure 3.5.9.1-1 Typical HARP Interface to AC Powered MOV**





**Figure 3.5.9.1-2 Typical HARP Interface to DC Powered MOV**



### 3.5.10 RRCS Direct Control of Safety-Related Components

Although the RRCS logic functions are reclassified as non-safety related (see Section 9.1), the components the RRCS needs to actuate are safety-related. Figure 3.5.10-1 shows a typical interface configuration between these components and the RRCS. A 1E isolator in the Maintenance and Test Cabinet (MTC - houses the MTP and ITP equipment) provides the electrical isolation between the non-safety RRCS and the safety related component.

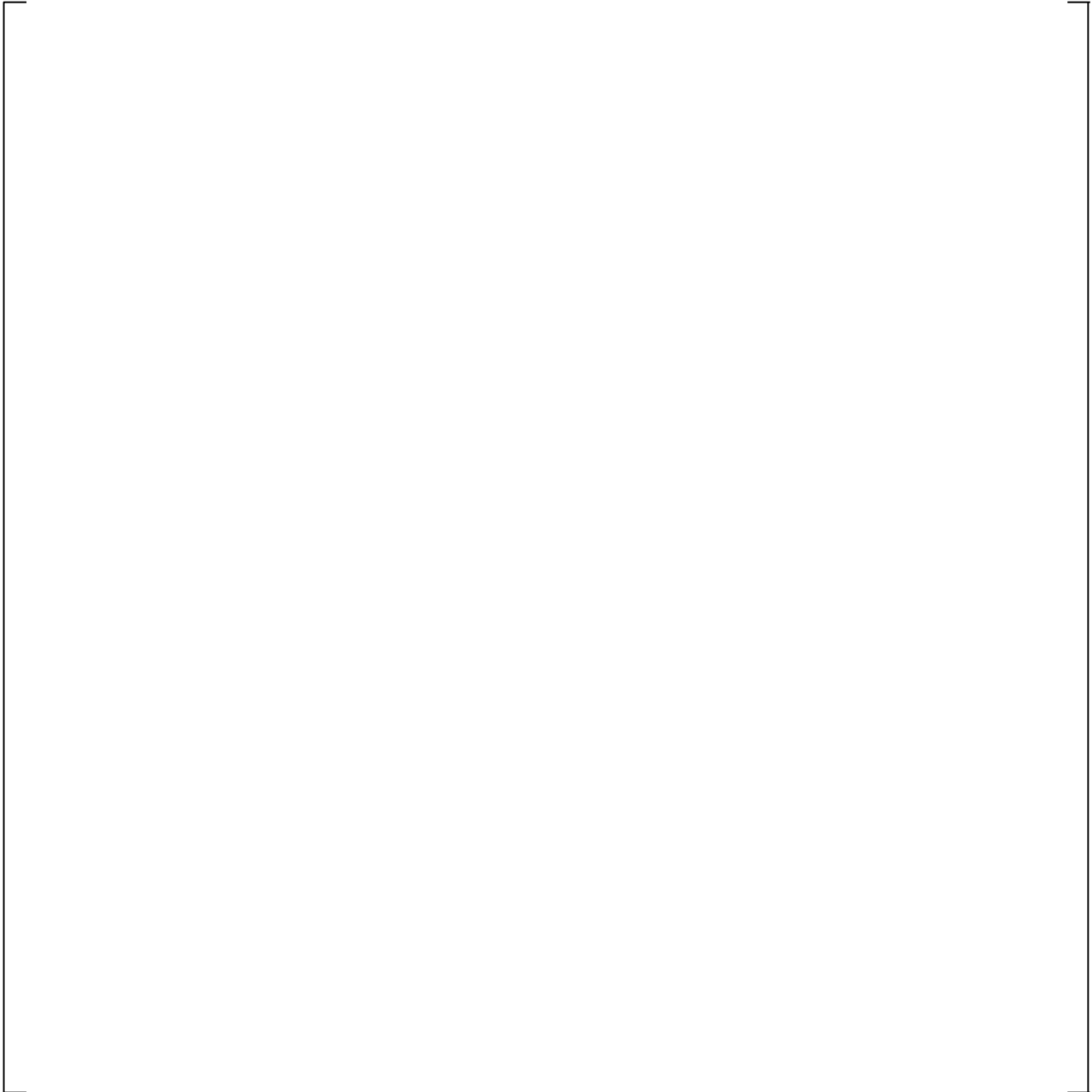
a,c

**Figure 3.5.10-1 RRCS Safety-Related Component Interface**

### 3.5.11 MTP IRIG-B Communication Interface

The MTP includes an IRIG-B interface to synchronize the RTC in the MTP and SDs with the DCS. Figure 3.5.11-1 shows the configuration of this interface. Compliance to DI&C-ISG-04 for this communication interface is documented in Table 3.2.21-1. The IRIG-B interface configuration in the MTP will undergo equipment qualification to ensure the interface does not adversely affect the PPS safety function. The fiber connection to the DCS provides 1E electrical isolation.





**Figure 3.5.11-1 MTP IRIG-B Interface**

### **3.5.12 Support and Auxiliary System Interfaces**

Section 3.5 identifies all the external PPS interfaces and there is no direct interface between the PPS and the plant HVAC. Section 3.2.10 discusses the PPS Heat Load Calculation that will be produced to ensure the HVAC requirements in the MCR and AER are still adequate.

Each division of the PPS is powered from one of the Class 1E Power System channels described in LGS UFSAR Chapter 8. The PPS complies with IEEE 603-1991 Clause 8.1 because it is using the existing LGS Class 1E Power System that meets its licensing basis for an electrical power source. IEEE 603-



1991, Clause 8.2 does not apply because the PPS only uses electrical power. The PPS is compliant to IEEE 603-1991 Clause 8.3 via the maintenance bypass capability described in Section 3.3.2.9.

### 3.5.13 Safety to Non-Safety Isolation Requirements

There are two forms of electrical isolation in the PPS when interfacing with external systems: fiber optic cable and 1E isolation devices. Data communications to non-safety systems use fiber optic cable to provide electrical isolation. The 1E isolation devices shown in the figures in Section 3.5 provide 1E electrical isolation that meets the minimum breakdown voltage of at least  $600V_{RMS}$ .<sup>225</sup>

### 3.5.14 IEEE Std 603 and IEEE Std 7-4.3.2 Relevant Clauses

The following clauses to IEEE Std 603-1991 and IEEE Std 7-4.3.2 are relevant to the discussion of system interfaces as identified in DI&C-ISG-06 (Reference 1), Section D.2.5.

#### 3.5.14.1 IEEE Std 603 Clause 5.6.1

Clause 5.6.1, states: ***Independence Between Redundant Portions of a Safety System.*** *Redundant portions of a safety system provided for a safety function shall be independent of and physically separated from each other to the degree necessary to retain the capability to accomplish safety function during and following any design basis event requiring, that' safety function.*

The level of independence between the redundant portions of the PPS is described in Sections 3.2 and 3.5.2. Each BPL channel transmits its trip and actuation signals to all four divisions using fiber optically isolated and unidirectional data links (HSL). The Common Q Topical Report (Reference 4) describes the HSL. The LCL in each division performs coincidence logic on these received signals. The LCL is not dependent on these signals to perform its safety function. If one channel is lost, the LCL will either assume the trip signal is tripped/actuated, or if the function is bypassed, then the coincidence voting will reduce to 2oo3.

The ITP also shares data between the divisions using the same HSL technology, but only performs diagnostic tasks and not plant protection functions.

#### 3.5.14.2 IEEE Std 603 Clause 5.6.2

Clause 5.6.2 states: ***Independence Between Safety Systems and Effects of Design Basis Event.*** *Safety system equipment required to mitigate the consequences of a specific design basis event shall be independent of, and physically separated from, the effects of the design basis event to the degree necessary to retain the capability to meet the requirements of this standard. Equipment qualification in accordance with 5.4 is one method that can be used to meet this requirement.*

The PPS equipment is qualified to withstand design basis events including seismic and loss of HVAC. This is documented in the equipment qualification summary report for LGS PPS (Reference 36).



### 3.5.14.3 IEEE Std 603 Clause 5.6.3

Clause 5.6.3 states: ***Independence Between Safety Systems and Other Systems.*** *The safety system design shall be such that credible failures in and consequential actions by other systems, as documented in 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard.*

As discussed for IEEE Std 603-1991, Clause 4.8 in Section 3.3.1, the LGS EQ Summary Report (Reference 36) demonstrates the capability of the PPS to continue operating at higher temperatures as a result of loss of control room HVAC. Once the PPS reaches its qualified temperature limit, a high temperature alarm is generated.<sup>226</sup> All interfaces to non-safety equipment are described in Section 3.5

#### 3.5.14.3.1 IEEE Std 603 Clause 5.6.3.1

Clause 5.6.3.1 states: ***Interconnected Equipment Classification:*** *(1) Equipment that is used for both safety and nonsafety functions shall be classified as part of the safety systems, Isolation devices used to effect a safety system boundary shall be classified as part of the safety system.*

*(2) Isolation:* *No credible failure on the non-safety side of an isolation device shall prevent any portion of a safety system from meeting its minimum performance requirements during and following any design basis event requiring that safety function. A failure in an isolation device shall be evaluated in the same manner as a failure of other equipment in a safety system.*

The PPS has non-safety functions (e.g., ITP functions). The software for these non-safety functions are developed to the software quality assurance requirements as safety related software using the NRC-approved Common Q Software Program Manual (Reference 6). Where there are interfaces to external systems either qualified isolators are used for hardwired interfaces (e.g., see Section 3.5.8) or fiber optic cable for data communication interfaces (e.g., see Section 3.5.6). In all cases the data communication meets the criteria of DI&C-ISG-04 (see Table 3.2.21-1).

The PPS cabinets also contain Ovation equipment including analog input modules, remote node interfaces, and SOE modules. These are described in Section 3.5. This equipment is classified as RG 1.75 associated circuits and are qualified to demonstrate that this equipment will not adversely impact the PPS safety equipment.

#### 3.5.14.3.2 IEEE Std 603 Clause 5.6.3.2

Clause 5.6.3.2 states: ***Equipment in Proximity***

*(1) Separation:* *Equipment in other systems that is in physical proximity to safety system equipment, but that is neither an associated circuit nor another Class 1E circuit, shall be physically separated from the safety system equipment to the degree necessary to retain the safety systems' capability to accomplish their safety functions in the event of the failure of non-safety equipment. Physical separation may be achieved by physical barriers or acceptable separation distance. The separation of Class 1E equipment shall be in accordance with the requirements of IEEE Std 384-1981*



(2) **Barriers:** Physical barriers used to effect a safety system boundary shall meet the requirements of 5.3, 5.4 and 5.5 for the applicable conditions specified in 4.7 and 4.8 of the design basis.

The non-safety interfaces are described in this Section 3.5. In all cases when non-safety equipment resides in the PPS, the non-safety equipment is classified as a RG 1.75 associated circuit. No physical barriers are used to isolate non-safety equipment within a PPS cabinet.

#### 3.5.14.3.3 IEEE Std 603 Clause 5.6.3.3

Clause 5.6.3.3 states: **Effects of a Single Random Failure.** *Where a single random failure in a nonsafety system can (1) result in a design basis event, and (2) also prevent proper action of a portion of the safety system designed to protect against that event, the remaining portions of the safety system shall be capable of providing the safety function even when degraded by any separate single failure. See IEEE Std 379-1988 [51] for the application of this requirement.*

The non-safety DCS was recently upgraded to an Ovation DCS. For that modification, Westinghouse produced an FMEA (Reference 53) confirming that any random single failure in the DCS would not place LGS in a condition not analyzed in the LGS Safety Analysis. The DPS/RRCS will be added to the new Ovation based DCS. The PPS interfaces described in this Section 3.5 ensure that a DCS single random failure cannot adversely affect the PPS from performing its safety function. In addition, other than the RRCS and DPS, the DCS does not share any sensors with the PPS.<sup>227</sup>

#### 3.5.14.4 IEEE Std Clause 5.6.4

Clause 5.6.4 states: **Detailed Criteria.** *IEEE Std 384-1981 [6] provides detailed criteria for the independence of Class 1E equipment and circuits [B3].*

The PPS interfaces as discussed in Section 3.5 meet the independence criteria of IEEE Std 384-1991. The interfaces discussed in Section 3.5 demonstrate the electrical isolation and functional independence of the PPS to the non-safety interfaces.

#### 3.5.14.5 IEEE Std 7-4.3.2 Clause 5.6

Clause 5.6 states: *In addition to the requirements of IEEE Std 603-1998, data communication between safety channels or between safety and nonsafety systems shall not inhibit the performance of the safety function.*

*IEEE Std 603-1998 requires that safety functions be separated from nonsafety functions such that the nonsafety functions cannot prevent the safety system from performing its intended functions. In digital systems, safety and nonsafety software may reside on the same computer and use the same computer resources.*

*Either of the following approaches is acceptable to address the previous issues:*

- a) *Barrier requirements shall be identified to provide adequate confidence that the nonsafety functions cannot interfere with performance of the safety functions of the software or firmware.*



*The barriers shall be designed in accordance with the requirements of this standard. The nonsafety software is not required to meet these requirements.*

- b) *If barriers between the safety software and nonsafety software are not implemented, the nonsafety software functions shall be developed in accordance with the requirements of this standard.*

*Guidance for establishing communication independence is provided in Annex E.*

The interfaces described in this Section 3.5 demonstrate that all data communications meets this requirement by utilizing fiber optically isolated data links or 1E isolation devices. The data communication hazards to the PPS safety function are addressed by meeting the DI&C-ISG-04 criteria in Section 3.2.21 and Table 3.2.21-1.

As discussed in Section 3.5.14.3.1, there are non-safety functions in the PPS, however they are developed using the same software quality assurance process as the PPS safety functions as defined by the Common Q Software Program Manual (Reference 6).

### **3.5.14.6 IEEE Std 603 Clause 5.12**

IEEE Std 603-1991 Clause 5.12 defines criteria for Auxiliary Features. The following sections describe compliance to the underlining subclauses 5.12.1 and 5.12.2.

#### **3.5.14.6.1 IEEE Std 603 Clause 5.12.1**

Clause 5.12.1 states: *Auxiliary supporting features shall meet all requirements of this standard.*

PPS auxiliary support features include cabinet locks and door limit switches to detect cabinet doors are opened. They are described in Section 8.2.1. The PPS also monitors cabinet temperature.<sup>228</sup>

#### **3.5.14.6.2 IEEE Std 603 Clause 5.12.2**

Clause 5.12.2 states: *Other auxiliary features that (1) perform a function that is not required for the safety systems to accomplish their safety functions, and (2) are part of the safety systems by association (that is, not isolated from the safety system) shall be designed to meet those criteria necessary to ensure that these components, equipment, and systems do not degrade the safety systems below an acceptable level. Examples of these other auxiliary features shown in Fig 3 and an illustration of the application of this criteria is contained in Appendix A.*

- Built in test equipment and circuitry: for the PPS this would be the built-in diagnostics of the system; see Sections 0 and 3.2.24.2.2. There are also built-in diagnostics in the CIM that are listed in Reference 11 and described in the CIM Technical Report, Section 2.5 (Reference 8). These diagnostics were developed using the same safety-related software development process as the CIM safety functions.
- Bypass and Reset Circuitry: The MTP and SDs are the human system interface to the PPS for maintenance and operational bypasses. These functions were developed in accordance with the NRC-approved SPM.
- Electric Protective Relaying: The PPS utilizes 1E isolation devices as described in Section 3.5.13.



All of the hardware associated with these features are qualified to IEEE Std 603-1991 criteria in accordance with the Common Q Topical Report (Reference 4). All of the software associated with these features are developed using the Common Q Software Program Manual (Reference 6) that was reviewed and approved by the NRC to the criteria in both IEEE Std 603-1991 and IEEE Std 7-4.3.2-2003.

The CIM logic for these features was developed and reviewed by the NRC as part of the AP1000 ITAAC process (ITAAC number 2.5.02.14). The results of the NRC inspection are summarized in the Southern Nuclear “Notification on the Completion of ITAAC 2.5.02.14,” (Reference 29), and the NRC Closure Form for ITAAC 2.5.02.14 (Reference 30).

#### **3.5.14.7 IEEE Std 603 Clause 5.14**

Clause 5.14 states: ***Human Factors Considerations.*** *Human factors shall be considered at the initial stages and throughout the design process to assure that the functions allocated in whole or in part to the human operator(s) and maintainer(s) can be successfully accomplished to meet the safety system design goals, in accordance with IEEE Std 1023-1988 [12].*

Idaho National Laboratory (INL) is working with Constellation in a public/private partnership for the human factors evaluation of the Digital Modernization Project that includes the PPS, RRCS and DPS. The INL Human Factors Engineering Program Plan for Constellation Safety Related I&C Upgrades (Reference 52) describes the HFE evaluation work that will be conducted for the project.

#### **3.5.14.8 IEEE Std 603 Clauses 8.1 - 8.3**

These clauses are addressed in Section 3.5.12.



### **3.6 PPS - FUNDAMENTAL DESIGN PRINCIPLES IN THE NEW ARCHITECTURE (D.2.6)**

This section discusses how the PPS meets the four fundamental design principles: Redundancy, Independence, Deterministic Behavior, and Defense-in-Depth and Diversity, and the attribute Simplicity of Design.

#### **3.6.1 Redundancy (D.2.6.2.1)**

The PPS sensor channels are four-way redundant and there are four divisions for coincidence voting. The divisions that actuate equipment mirror the LGS plant equipment arrangements. For instance, for reactor trip, PPS Division 1 and Division 2 interface to the reactor scram pilot solenoid valves “A” and “B” respectively (see Figure 3.1.1-1 for existing scram pilot solenoid valve arrangement). Refer to Section 3.3 for a further description.

The PPS architecture has the following redundancies within a division:

- Diverse and redundant PPS cabinet power supplies
- Each HSL datalink is redundant
- AF100 bus is redundant
- Redundant BPL processing
- Redundant LCL processing
- Redundant ILP processing
- Redundant SRNC datalinks from the ILP to the CIM

Reference 40 is the Failure Modes and Effects Analysis (FMEA) for the LGS PPS that uses the redundancy of the system to meet IEEE Std 603-1991 single failure criterion. The FMEA is a bounding analysis. It postulates higher level failures that cover lower level failures that would have the same impact on the system.

The EQ Summary Report (Reference 36), documents the qualification of the PPS equipment to mitigate against LGS design basis events.

##### **3.6.1.1 Relevant IEEE Std 7-4.3.2 Clauses**

This section documents compliance to IEEE Std 7-4.3.2-2003 clauses deemed relevant by DI&C-ISG-06, Section D.2.6.2.1.2 (Reference 1).

###### **3.6.1.1.1 IEEE Std 7-4.3.2 Clause 5.1**

Clause 5.1 states: *No requirements beyond IEEE Std 603-1998 are necessary (see also Annex B).*

IEEE Std 603-1991, Clause 5.1 is addressed in Section 3.2.24.1.1.

###### **3.6.1.1.2 IEEE Std 7-4.3.2 Clause 5.15**



Clause 5.15 states: **Reliability** NOTE-See Annex F for more information about the reliability criterion.

*In addition to the requirements of IEEE Std 603-1998, when reliability goals are identified, the proof of meeting the goals shall include the software. The method for determining reliability may include combinations of analysis, field experience, or testing. Software error recording and trending may be used in combination with analysis, field experience, or testing.*

The reliability goals, and how they are met, for the PPS is discussed in Section 3.3.1 – Clause 4.9.

The PPS reliability analysis substantiates that the PPS will meet the established reliability goals (see Section 3.6.1.3). The PPS software hazards analyzes (Reference 55) the software for potential faults and mitigation or elimination of those faults. The LGS PPS will be developed and undergo extensive testing in accordance with the Common Q Software Program Manual (Reference 6) which was reviewed and approved by the NRC.

#### **3.6.1.1.3 IEEE Std 7-4.3.2 Clause 6.7**

IEEE Std 7-4.3.2-2003 does not have additional criteria for IEEE Std 603-1991 Clause 6. IEEE Std 603-1991 Clause 6.7 is addressed in Section 3.3.2.9.

#### **3.6.1.1.4 IEEE Std 7-4.3.2 Clause 7.5**

IEEE Std 7-4.3.2-2003 does not have additional criteria for IEEE Std 603-1991 Clause 7. IEEE Std 603-1991 Clause 7.5 is addressed in Section 3.3.2.9.

#### **3.6.1.2 IEEE Std 379 Criteria**

IEEE Std 603-1991 cites IEEE Std 379-1988 for guidance on the application of the single failure criterion. NRC Regulatory Guide 1.53 endorsed IEEE Std 379-2000. The following paragraphs address compliance to IEEE Std 379-2000.

Clause 5.1 addresses independence and redundancy. The FMEA for the LGS PPS (Reference 40) is summarized in Section 3.2.22 to demonstrate that no single failure of the PPS will interfere with the proper operation of its safety functions.

Clause 5.2 addresses non-detectable failures. The PPS provides four channels of BPL processing of inputs and generation of protective action signals to four divisions of PPS. There are four divisions that perform coincidence logic on the four channels of trip/actuation signals. The divisions that actuate equipment mirror the LGS plant equipment arrangements. The four BPL channels and four coincidence logic divisions will meet the criteria that the PPS can still perform its safety function with both a detectable single failure and an identified non-detectable failure in the BPLs and LCLs. The licensing criteria for the actuating divisions is defined by the current LGS licensing basis.

Clause 5.3 addresses Cascaded failures. Cascaded failures resulting from a single failure is considered a single failure. Due to the independence of the PPS divisions, cascaded single failures would be localized



to a single PPS division. As a result there are still three other PPS divisions that can generate protective action signals.

Clause 5.4 addresses Design basis events. The LGS design basis events that could impact the PPS are covered by the equipment qualification program for seismic and environmental hazards. The LGS PPS equipment qualification summary report (Reference 36) demonstrates that the PPS will withstand the design basis events that could impact the PPS.

Clause 5.5 addresses Common-cause failures. CCFs that originate from the plant design basis is addressed in Clause 5.4. CCFs that originate from the PPS is addressed in Section 3.2.23.

Clause 5.6 addresses Shared systems. See Section 3.3.2.7 that addresses the shared systems requirement in IEEE 603.

Clause 6 addresses Design analysis for single failure. The LGS PPS FMEA (Reference 40) as summarized in Section 3.2.22 is the analysis that determines that the PPS meets the single failure criterion.

### 3.6.1.3 GDC 21

GDC 21 Protection System Reliability and Testability states: *The protection system shall be designed for high functional reliability and in service testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection system shall be sufficient to assure that (1) no single failure results in loss of the protection function and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. The protection system shall be designed to permit periodic testing of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred.*

The LGS PPS is designed for high functional reliability by using a high quality software design process in accordance with the NRC-approved Common Q Software Program Manual (Reference 6). The LGS reliability analysis (Reference 42) demonstrates that the LGS PPS is designed for high reliability. The LGS PPS provides for in-service testability as described in Section 3.2.12.

The LGS PPS redundancy and independence is described in Sections 3.5.1.1 and 3.2.13, as well as the beginning of this section (3.6.1) such that it meets the single failure criterion even when one PPS channel is out of service. The service/test functions described in Section 3.2.12 support testing even when the reactor is in operation.

### 3.6.1.4 GDC 24

GDC 24 Separation of Protection and Control Systems states: *The protection system shall be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and*



*independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.*

Except for RRCS/DPS, the PPS does not share sensors or components with the LGS non-safety plant control systems such as the Digital Electro-Hydraulic Control (DEHC) system and Digital Feedwater Level Control System (DFWLCS), which have their own sensors. The configuration of the shared sensors between the PPS and the DPS/RRCS is described in Section 3.5.3. The PPS maintains functional and electrical isolation from any non-safety system including non-safety control systems in the plant, as described in Section 3.5.

### **3.6.2 Independence (D.2.6.2.2)**

The PPS provides for four functionally independent and electrically isolated BPL channels that calculate and initiate protective actuation signals. PPS provides four functionally independent and electrically isolated divisions to perform coincidence and protection system actuation. For electrical independence see Section 3.2.13. For data communications functional and electrical independence see Section 3.2.21. Section 3.5 describes the unidirectional communications between divisions of the PPS and the external interfaces between the PPS and non-safety systems which meets the IEEE Std 384 criteria for independence of Class 1E equipment and circuits.

#### **3.6.2.1 Relevant IEEE Std 7-4.3.2 Clauses**

This section documents compliance to IEEE Std 7-4.3.2-2003 clauses deemed relevant by DI&C-ISG-06, Section D.2.6.2.2.2 (Reference 1).

##### **3.6.2.1.1 IEEE Std 7-4.3.2 Clause 5.6**

Clause 5.6 is addressed in Section 3.5.14.5

##### **3.6.2.1.2 IEEE Std 7-4.3.2 Clause 5.11**

Clause 5.11 states: *To provide assurance that the required computer system hardware and software are installed in the appropriate system configuration, the following identification requirements specific to software systems shall be met:*

- a) Firmware and software identification shall be used to assure the correct software is installed in the correct hardware component.*
- b) Means shall be included in the software such that the identification may be retrieved from the firmware using software maintenance tools.*
- c) Physical identification requirements of the digital computer system hardware shall be in accordance with the identification requirements in IEEE Std 603-1998.*

Each application loaded into a PM646A processor module has a calculated cyclic redundancy check (CRC) value. To verify that the qualified software is installed and not modified, a comparison is made between the calculated CRC and the CRC documented in the release document for the application. If they are the same then the technician knows that the correct software is installed. This is described in the



Common Q Topical Report (Reference 4) Section 5.4.1.1. Because each AC160 controller has a different configuration, if the application software was installed in the wrong PM646A, errors would occur announcing the mismatch on the controller configuration with the application (i.e., the expected I/O configuration would not match the application database).<sup>229</sup>

The operator or maintenance technician can call up the CRC/System Load Display (Section 3.2.12.2) to view the software CRC identification for each PM646A.

### 3.6.2.1.3 IEEE Std 7-4.3.2 Clause 6.3

IEEE 7-4.3.2 states that there are no additional requirements beyond IEEE Std 603 Clause 6. IEEE Std 603 Clause 6.3 Interaction Between the Sense and Command Features and Other Systems has two subclauses 6.3.1 and 6.3.2.

IEEE Std 603-1991 Clause 6.3.1 states: *Where a single credible event, including all direct and consequential results of that event, can cause a non-safety system action that results in a condition requiring protective action and can concurrently prevent the protective action in those sense and command feature channels designated to provide principal protection against the condition, one of the following requirements shall be met:*

- (1) *Alternate channels not subject to failure resulting from the same single event shall be provided to limit the consequences of this event to a value specified by the design basis. Alternate channels shall be selected from the following:*
  - (a) *Channels that sense a set of variables different from the principal channels.*
  - (b) *Channels that use equipment different from that of the principal channels to sense the same variable.*
  - (c) *Channels that sense a set of variables different from those of the principal channels using equipment different from that of the principal channels. Both the principal and alternate channels shall be part of the sense and command features.*
- (2) *Equipment not subject to failure caused by the same single credible event shall be provided to detect the event and limit the consequences to a value specified by the design bases. Such equipment is considered a part of the safety system.)*

*See Fig 5 for a decision chart for applying the requirements of this section.*

There is no interconnectivity or shared resources between the PPS and the non-safety control systems that are identified as event initiators in Chapter 15 of the LGS FSAR.<sup>230</sup> However, there will be digital RRCS and DPS added to the DCS as part of the modification. But these systems perform protective functions and not control functions. The D3 analysis (Reference 11) analyzes the potential spurious actuation of these systems to confirm that plant can cope within its design basis when these unlikely events occur.

IEEE Std 603-1991, Clause 6.3.2 states: *Provisions shall be included so that the requirements in 6.3.1 can be met in conjunction with the requirements of 6.7 if a channel is in maintenance bypass. These provisions include reducing the required coincidence, defeating the non-safety system signals taken from the redundant channels, or initiating a protective action from the bypassed channel.*



Compliance to Clause 6.3.1 is maintained even when one channel of PPS is in maintenance bypass (See Section 3.5.1.1 for a description of the PPS redundancy characteristics).

### **3.6.2.2 RG 1.75**

See Section 3.5 for a description of PPS external interfaces that deploy non-safety equipment in the PPS cabinet. In all such cases the non-safety equipment is considered a RG 1.75 associated circuit and is qualified to not adversely impact the PPS safety functions.

### **3.6.2.3 Applicable 10 CFR 50 Appendix A General Design Criteria**

The following sections address the GDCs listed in Reference 1, Section D.2.6.2.2.2 for the fundamental principle of Independence.

### **3.6.2.4 GDC 13 Instrumentation and Control**

GDC 13 states: *Instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges.*

The PPS variable ranges for normal operation, for anticipated operational occurrences (AOOs), and for accident conditions is established in the LGS design basis and is unchanged as a result of the PPS project. These are documented in the LGS PPS System Requirements Specification (Reference 2), Table A-13 for the RG 1.97 process inputs and in the Functional Logic Specification (Reference 70), Section 2.1 and Appendix A. The functional requirements for monitoring the RG 1.97 variables are in Section 5.7 of the PPS System Requirements Specification (Reference 2). The AC160 modules that interface to these variables are qualified both in the range required to interface to these variables, and to the environment in which the PPS equipment resides (see Section 4 and Reference 36).

The PPS Safety Displays are used to display the RG 1.97 variables. These displays are safety-related and are qualified to continue operating after a design basis event.

### **3.6.2.5 GDC 21 Protection System Reliability and Testability**

Compliance to GDC 21 is discussed in Section 3.6.1.3.

### **3.6.2.6 GDC 22 Protection System Independence**

GDC 22 states: *The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function.*



The PPS has four functionally and electrically independent channels and divisions to provide RPS, ECCS and NSSSS protective functions as applicable. The PPS equipment is qualified to the natural phenomena events in Chapter 15 of the LGS FSAR that impact the PPS (see Reference 36). The functional diversity of the existing RPS, ECCS, and NSSSS functions is defined by the various sensor types (e.g., pressure sensing vs. temperature sensing) for overlapping monitoring of plant conditions to ensure adequate protection from DBEs are activated. This functional diversity is carried over to the integrated PPS architecture. Diversity of component design is achieved by having a diverse PPS cabinet power supply design and a Diverse Protection System to protect against a PPS CCF.

### **3.6.2.7 GDC 23 Protection System Failure Modes**

GDC 23 states: *The protection system shall be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy (e.g., electric power; instrument air), or postulated adverse environments (e.g., extreme heat or cold, fire, pressure, steam, water, and radiation) are experienced.*

The fail-safe state for the PPS RPS functions is the reactor trip condition. The NSSSS actuations are designed to de-energize to activate. Should there be a loss of power to a division, the NSSSS functions will activate. ECCS functions are designed to fail as-is. This is to protect the plant from spurious actuation of ECCS functions on loss of power.<sup>231</sup>

### **3.6.2.8 GDC 24 Separation of Protection and Control Systems**

PPS compliance to GDC 24 is discussed in Section 3.6.1.4.

## **3.6.3 Deterministic Behavior (D.2.6.2.3)**

The fundamental element for deterministic behavior of the PPS is the AC160 PM646A controller and its cyclic execution of the application programs described in the Common Q Topical Report (Reference 4) Section 5.2.1.2.1. The cycle time of PPS application programs are established to meet the response time requirements for the Chapter 15 events and the PPS response time requirements in the LGS PPS System Requirements Specification (Reference 2), Section 7.1. As long as the PPS maintains a PM646A CPU load of 70% or less, the programs will execute deterministically (see Common Q Topical Report [Reference 4], Section 5.3.1.1). The PM646A window watchdog timer will halt the PM646A if the precision interval timer that controls the cyclic execution of the PPS applications is not refreshed in the prescribed periodic window (see Common Q Topical Report [Reference 4], Section 5.2.1.3.1).

The LGS PPS timing analysis calculates the worst possible response time for each event in Chapter 15 of the FSAR.<sup>232</sup>

### **3.6.3.1 Applicable IEEE Std 603 and IEEE Std 7-4.3.2 Clauses**

The following sections address applicable clauses to IEEE Std 603-1991 and IEEE Std 7-4.3.2-2003 as described in Section D.2.6.2.3.2 of Reference 1.

#### **3.6.3.1.1 IEEE Std 603 Clause 5.2**



There is no corresponding Clause 5.2 in IEEE Std 7-4.3.2, and Clause 5.2 in IEEE Std 603 is addressed in Section 3.3.2.1.

### 3.6.3.1.2 IEEE Std 603 Clause 5.5 and IEEE Std 7-4.3.2 Clauses 5.5.1 – 5.5.3

Clause 5.5 in IEEE Std 603 is addressed in Section 3.3.2.2.

IEEE Std 7-4.3.2 Clause 5.5.1 states: ***Design for computer integrity.*** *The computer shall be designed to perform its safety function when subjected to conditions, external or internal, that have significant potential for defeating the safety function. For example, input and output processing failures, precision or roundoff problems, improper recovery actions, electrical input voltage and frequency fluctuations, and maximum credible number of coincident signal changes.*

*If the system requirements identify a safety system preferred failure mode, failures of the computer shall not preclude the safety system from being placed in that mode. Performance of computer system restart operations shall not result in the safety system being inhibited from performing its function.*

The failures described in this clause have been analyzed in the PPS FMEA (Reference 40). Also, Section 3.2.12 discusses the PPS diagnostics. The FMEA demonstrates how the PPS will revert to its preferred failure mode.

IEEE Std 7-4.3.2 Clause 5.5.2 is addressed in Section 3.2.24.2.1.

IEEE Std 7-4.3.2 Clause 5.5.3 is addressed in Section 3.2.24.2.2.

### 3.6.3.1.3 IEEE Std 603 Clause 6.1

IEEE Std 603 states: ***Automatic Control.*** *Means shall be provided to automatically initiate and control all protective actions except as justified in 4.5. The safety system design shall be such that the operator is not required to take any action prior to the time and plant conditions specified in 4.5 following the onset of each design basis event. At the option of the safety system designer, means may be, provided to automatically initiate and control those protective actions of 4.5.*

The PPS provides automatic trip and actuation functions for events summarized in Section 3.3. The design functions listed in Table 3.3-1 are unchanged as a result of this license amendment. The PPS will generate these same protections functions as the existing RPS, ECCS and NSSSS for these credited events without required operator action.

### 3.6.3.1.4 IEEE Std 603 Clause 6.2 and 7.2

IEEE Std 603 Clause 6.2 is criteria for Manual Control.

**IEEE Std 603 Clause 6.2.1:** *Means shall be provided in the control room to implement manual initiation at the division level of the automatically initiated protective actions. The means provided shall minimize the number of discrete operator manipulations and shall depend on the operation of a minimum of equipment consistent with the constraints of 5.6.1.*



The PPS provides manual reactor scram pushbuttons located in the MCR. Each reactor scram pushbutton is hardwired directly to one of the RPS TUs, so that each division receives one of the four pushbutton inputs which bypass the software-based portion of the PPS. A reactor scram will occur if Division 1 OR 3 pushbutton is depressed simultaneously with the Division 2 OR 4 pushbutton.

Each division of the PPS provides soft control, through the SDs, for manual initiation of division level automatically initiated protective actions. To affect the manual initiation, a hardwired confirm switch adjacent to each SD is activated [ ]<sup>a,c</sup> This confirm switch is to protect against spurious actuation of the manual initiation. An HFE evaluation is conducted by INL as part of the control room modernization that includes this soft control manual operation. The evaluation will include assessing that the manner in which the operator uses the SD to perform these manual initiations to minimize the number of discrete operator manipulations. Having the confirm switch hardwired to the division LCL represents the operation of minimum equipment because it would require significantly more equipment (cabling) to hardwire the confirm switch at the ILP or CIM level of the architecture. It also simplifies the logic because the LCL simply needs to OR the automatic coincidence output with the manual initiation to affect the same result downstream in the PPS division architecture.

**IEEE Std 603 Clause 6.2.2:** *Means shall be provided in the control room to implement manual initiation and control of the protective actions identified in 4.5 that have not been selected for automatic control under 6.1. The displays provided for these actions shall meet the requirements of 5.8.1.*

Any such controls that are required by the current design basis are implemented similarly in the SDs (see Section 3.3.1). The SD is a safety-related display system as described in the Common Q Topical Report (Reference 4).<sup>233</sup> The software is developed in accordance with the Common Q Software Program Manual (Reference 6).

**IEEE Std 603 Clause 6.2.3:** *Means shall be provided to implement the manual actions necessary to maintain safe conditions after the protective actions are completed as specified in 4.10. The information provided to the operators, the actions required of these operators, and the quantity and location of associated displays and controls shall be appropriate for the time period within which the actions shall be accomplished and the number of available qualified operators. Such displays and controls shall be located in areas that are accessible, located in an environment suitable for the operator, and suitably arranged for operator surveillance and action.*

See Section 3.3.1 for the disposition of Clause 4.10. An HFE evaluation is conducted by INL as part of the control room modernization that includes this soft control manual operation. The evaluation will include assessing the information provided to the operators, the actions required of these operators, and the quantity and location of the SDs to meet Clause 4.10 if applicable. The SDs are located in the MCR.

**IEEE Std 603 Clause 7.2:** *If manual control of any actuated component in the execute features is provided, the additional design features in the execute features necessary to accomplish such manual control shall not defeat the requirements of 5.1 and 6.2. Capability shall be provided in the execute features to receive and act upon manual control signals from the sense and command features consistent with the design basis.*



For the PPS, Constellation considers the CIM and HARP part of the IEEE Std 603 Execute Features. PPS is designed for manual component control to be performed in the Control Room via the SDs in that PPS division. This meets the requirement for IEEE Std Clause 6.2.

The CIM has the capability to manually control a component. This CIM local manual control is on a component-by-component basis and is only used in cases of emergency when the component cannot be manually controlled from the Control Room via the PPS SDs (see IEEE Std Clause 6.2 compliance). Manually controlling the component via the CIM manual control switch does not invalidate the Single Failure Criterion of the PPS (IEEE Std Clause 5.1) because there are redundant divisions to perform the execute features. The CIM is designed to receive manual control signals from either the PPS (via the CIM X-Port) or the non-safety DCS (via the Y-Port). The CIM Z-Port is reserved for component actuation from the DPS.

#### **3.6.3.1.5 IEEE Std 603 Clause 7.1**

**IEEE Std 603 Clause 7.1: Automatic Control.** *Capability shall be incorporated in the execute features to receive and act upon automatic control signals from the sense and command features consistent with 4.4 of the design basis.*

For PPS, Constellation considers the CIM and HARP as IEEE Std 603 Execute Features. The ILP receives the protective actuation signal from the LCL and then fans out the signal into component actuation signals to the CIM, whose output goes to the HARP interface to the actuating components. The generated LCL protective actuation signal is based on the PPS sense and command function consistent with the plant design basis.

#### **3.6.3.2 Applicable 10 CFR 50 Appendix A General Design Criteria**

This section describes PPS compliance to the listed GDCs in Section D.2.6.2.3.2 in Reference 1.

##### **3.6.3.2.1 GDC 13 Instrumentation and Control**

GDC 13 is addressed in Section 3.6.2.4.

##### **3.6.3.2.2 GDC 21 Protection System Reliability and Testability**

GDC 21 is addressed in Section 3.6.1.3.

##### **3.6.3.2.3 GDC 23 Protection System Failure Modes**

GDC 23 is addressed in Section 3.6.2.7



#### 3.6.3.2.4 GDC 29 Protection Against Anticipated Operational Occurrences

GDC 29 states: *The protection and reactivity control systems shall be designed to assure an extremely high probability of accomplishing their safety functions in the event of anticipated operational occurrences.*

The AOOs in which the PPS is credited for mitigating is summarized in Section 3.3. The same variables and algorithms are used in the PPS as in the existing RPS/NSSSS/ECCS to monitor for the AOO and provide the protective action to mitigate the event, except as noted in Section 3.3.

#### 3.6.4 Defense-in-Depth and Diversity (D.2.6.2.4)

Although BTP 7-19 refers to NUREG-6303 (Reference 64) for describing echelons of defense that separate reactor trip from ESFAS, there is regulatory precedence for integrating these protection functions into one system as long as the requirements of 10 CFR 50 are met<sup>234</sup>. BTP 7-19 recognizes this possibility by stating:

*DI&C systems can integrate design functions that were previously located in separate and dedicated analog systems. For example, formerly discrete systems (e.g., the reactor trip system (RTS) and the engineered safety feature actuation system (ESFAS)) can be combined into a single DI&C protection system. Also, DI&C systems can share resources, such as communications, networks, controllers, power supplies, or multifunction display and control stations. The integrability of DI&C systems makes it more challenging to identify and evaluate potential consequences of a postulated CCF.*

Special considerations need to be taken into account for an integrated system like PPS. In particular the consequences of a PPS CCF need to be considered. Sections 3.2.23 explains the need for an additional Diverse Protection System to address the potential for a PPS CCF.

DI&C-ISG-06 (Reference 1) identifies GDC 13, 22 and 24 to be applicable to this fundamental design principle. These GDCs are addressed in Sections 3.6.2.4, 3.6.2.6, and 3.6.1.4 respectively.

#### 3.6.5 Simplicity of Design (D.2.6.2.5)

In its simplest form, the LGS PPS measures plant parameters, compare those parameters to boundary conditions, and if necessary, actuate a reactor trip, ECCS or NSSSS function. Although maintaining the analog protection systems was an option, Constellation chose to integrate the analog RPS, ECCS, and NSSSS into a PPS using a platform that has had many operating years in the nuclear industry. A digital PPS is more accurate because the logic is based on 1's and 0's and not voltage levels. There is less maintenance required in a digital system because there are less calibration adjustments to be made in a digital system and the self-diagnostics eliminate the need for numerous manual surveillances.

With any new technology, capabilities exist that may be nice to have, but the level of complexity outweighs the benefit. For example, the PPS technology allows for communicating all kinds of information between divisions that could be incorporated into the safety function. The PPS trip and actuation functions are simply replicated. Data sharing is only for coincidence voting.



The communication between divisions is point-to-point, unidirectional, and serial rather than a network topology. The PPS employs this simpler technology for communication between divisions to ensure independence between divisions.

So in summary, the PPS uses digital I&C technology in a conservative manner and still reap the benefits that digital technology can provide for a safety system.

#### 3.6.5.1 IEEE Std 603 Clause 6.4

DI&C-ISG-06, Reference 1, identifies IEEE Std 603-1991, Clause 6.4 as relevant to this fundamental design attribute.

Clause 6.4 states: ***Derivation of System Inputs.*** *To the extent feasible and practical, sense and command feature inputs shall be derived from signals that are direct measures of the desired variables as specified in the design basis.*

The design function of the PPS measures plant process parameters and generate trip and actuation signals are replicated from the existing RPS, ECCS and NSSSS. The relationship between the Chapter 15 event that credits the PPS protective functions and the process values used is summarized in Section 3.3. The process variables used to calculate the PPS protective functions are unchanged as a result of this license amendment.



## 4 PPS - HARDWARE EQUIPMENT QUALIFICATION (D.3)

The Common Q Platform Topical Report (Reference 4), Section 7, describes the equipment qualification methodology for the generic qualification of the Common Q Platform. The Common Q equipment is mounted in a test rack in the same manner as it will be mounted in an actual cabinet.

IEEE Std 603-1991, Clause 5.4 requires that *Safety system equipment shall be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it will be capable of meeting, on a continuing basis, the performance requirements as specified in the design basis. Qualification of Class 1E equipment shall be in accordance with the requirements of IEEE Std 323-1983 [2] and IEEE Std 627-1980 [11].*

As described in the Common Q Topical Report (Reference 4), Section 7, the generic qualification of Common Q platform was performed by type test and/or analysis. The Common Q platform generic qualification program was reviewed and approved by the NRC using the criteria of RG 1.100 Revision 3, 1.89 Revision 1, RG 1.180, Revision 1, RG 1.209, Revision 0, and EPRI TR-107330. As a result of the NRC review, plant-specific action items were documented. These are addressed for the LGS PPS in Section 6.2.2.

IEEE Std 7-4.3.2, 2003, Clause 5.4.1 **Computer system testing**, states: *Computer system qualification testing (see 3.1.36) shall be performed with the computer functioning with software and diagnostics that are representative of those used in actual operation. All portions of the computer necessary to accomplish safety functions, or those portions whose operation or failure could impair safety functions, shall be exercised during testing. This includes, as appropriate, exercising and monitoring the memory, the CPU, inputs and outputs, display functions, diagnostics, associated components, communication paths, and interfaces. Testing shall demonstrate that the performance requirements related to safety functions have been met.*

The LGS equipment qualification summary report (EQSR), EQ-EV-386-GLIM, “Comparison of Equipment Qualification Hardware Testing for Common Q Applications to Limerick Requirements,” (Reference 36) summarizes the equipment qualification performed to-date for the PPS equipment and demonstrates that the equipment qualification tests/analyses meet the LGS site requirements for the PPS. The previous qualification of Common Q equipment is summarized in WCAP-17415-P, Addendum to Summary Qualification Report of Hardware Testing for Common Q Applications” (Reference 66) and is referenced in the LGS EQSR for the Common Q equipment. WCAP-17415-P, Revision 1, was submitted to the NRC September 2019 (ML19261A067). The LGS EQSR lists the equipment analyzed in the report and identifies additional testing that will need to be conducted due to differences in the LGS configuration (e.g., different cabinet types).

The original, comprehensive equipment qualification for the Common Q platform used type test software running in the test specimen that performed the following:

[

] <sup>a,c</sup>



[

] <sup>a,c</sup>

The EQSR provides assurance that the DMP project-specific equipment qualification program will successfully demonstrate that the PPS architecture can meet the LGS site requirements.

Further equipment qualification testing is required after the detailed hardware design is complete. The EQSR representing this equipment qualification testing will be submitted subsequent to the initial LAR submittal.



## 5 PPS - I&C SYSTEM DEVELOPMENT PROCESSES (D.4)

Westinghouse will be using the NRC-approved Common Q Software Program Manual (SPM, Reference 6) as the framework for the design and development of the LGS PPS. This framework is a supplement to the Westinghouse 10 CFR 50 Appendix B Quality Assurance program to specifically address digital I&C safety system development. Attributes of the framework as outlined in DI&C-ISG-06, Revision 2 (Reference 1), D.4.1 are:

- a. Create the concepts on which the system design will be based. For the LGS PPS the following basic concepts inform the LGS PPS system design:
  1. The LGS PPS system design is based on the design described in the Plant Protection System Performance Specification (Reference 2).
  2. It uses a similar four division, three level PPS architecture as the AP1000 Protection and Safety Monitoring System (PMS) described in Reference 3.
  3. The LGS PPS system design addresses the functional requirements of the existing LGS PPS system as described in Section 2, Plant System Description (D.1) and Section 3.1, Existing System Architecture (D.2.1).
- b. Translate these concepts into system requirements. The base system requirements for the LGS PPS is the PPS System Requirements Specification (Reference 2). This document translates the concepts upon which the system design is based into system requirements.
- c. Allocate system requirements to system elements (e.g., software, hardware, and human-system interfaces). The base system requirements that are documented in PPS System Requirements Specification (Reference 2). The allocation of these requirements to system elements is documented in the PPS System Design Specification (Reference 21). These requirements are allocated to hardware, software, and other responsible groups in accordance with the requirements management plan.<sup>236</sup> The independent V&V team assess the allocation of functions for completeness and correctness per the NRC approved Common Q SPM (Reference 6)<sup>237</sup>.
- d. Implement the design into hardware and software functions. As stated in c. above, the requirements traceability matrix documents the implementation of the system requirements into hardware and software functions in accordance with the NRC-approved Common Q SPM (Reference 6).
- e. Integrate system elements such as software and hardware. Westinghouse uses its testing methodology as described in the NRC-approved Common Q SPM (Reference 6), Section 7, that documents successive levels of testing to integrate the system elements (both software and hardware).
- f. Test the unit functions and the completed system to confirm that system requirements have been implemented correctly. The NRC-approved Common Q SPM (Reference 6), Section 7, describes the successive levels of testing up to a System Validation Test, and a Factory Acceptance Test to validate manufacturing. The independent V&V team uses the RTM to trace testable requirements to test procedures and reports.
- g. Perform appropriate human factors engineering for the human-system interfaces throughout the development process. LGS will engage operations staff early in the project to familiarize them with the established display set so that operating procedures can be prepared in a timely manner to take advantage of the benefits of an improved human-system interface. Constellation has also engaged INL for the HFE evaluation of the MCR modification including the PPS human-system interfaces.



- h. Analyze hazards and incorporate requirements that eliminate or mitigate identified hazards throughout the development process. An LGS PPS FMEA is developed to eliminate or mitigate any hazards identified in that analysis. The LGS PPS documents include a software hazard analysis (SHA) in accordance with the Common Q SPM (Reference 6) to eliminate or mitigate any software hazards identified in the analysis (see Reference 55).
- i. Perform V&V activities on work products throughout the development process. The LGS PPS development will undergo independent verification and validation (V&V) in accordance with the NRC-approved Common Q SPM (Reference 6).

The software life cycle process is governed by the NRC-approved Common Q SPM (Reference 6). Section 1.4.1 in the Common Q SPM defines the software life cycle to be:

- Concept
- Requirements Analysis
- Design
- Implementation or Coding
- Test
- Installation and Checkout
- Operation and Maintenance
- Retirement

The LGS PPS project will be following this life cycle process. Any clarifications or exceptions (with justification) to the processes described in the NRC-approved Common Q SPM are documented in the LGS PPS Software Development Plan (Reference 25). There are other overarching processes such as Project Management, Verification and Validation (V&V), and Configuration Management. V&V and Configuration Management will be performed in accordance with the NRC-approved Common Q SPM (Reference 6). Project Management is discussed in Section 5.2.10.

## 5.1 COMMON Q SPM PLANT SPECIFIC ACTION ITEMS

The NRC documented seven Plant Specific Action Items (PSAIs) in the safety evaluation on the NRC-approved SPM (Reference 6). This section provides the dispositions for the seven PSAIs.

### 5.1.1 PSAI 1

*As noted in Sections 3.2.1 and 3.2.3, WEC may choose to use alternatives to the SPM defined processes when performing Initiation phase activities for individual projects. These alternatives are required to be documented in the Project Quality Plan (PQP). This PQP should be reviewed to determine if alternatives to the SPM are being used for development of project specific software. When such alternatives are being used, the PQP should be evaluated to determine if the justifications for the use of alternatives to the SPM processes are acceptable.*

The SPM states, “When the SPM refers to a PQP, it includes the Project Quality Plan and Project Plan (including the Software Development Plan) defined in the Westinghouse Quality Management System Procedures.” Any alternative processes to the SPM would be documented in the LGS PPS Software Development Plan (Reference 25) with justification. The Software Development Plan also includes



clarifications to particular items to make clear how certain aspects of the SPM are being fulfilled. The LGS PPS Software Development Plan (Reference 25) does not identify any alternatives to the Common Q SPM (Reference 6) for this project.

### 5.1.2 PSAI 2

*The Common Q SPM only includes the Software Life Cycle Process Planning Documentation as outlined in SRP BTP 7-14, Section B.2.1. As such, the plant-specific documentation outlined in SRP BTP 7-14, Sections B.2.2, "Software Life Cycle Process Implementation," and B.2.3, "Software Life Cycle Process Design Outputs," is to be evaluated separately for any application that references the Common Q SPM.*

The following table provides the cross reference between the documents listed in BTP 7-14 Sections B.2.2 and B.2.3 and the name of the Westinghouse LGS PPS corresponding document. If the document is complete, a document number will be cited, otherwise the document is produced later in the life cycle.

**Table 5.1.2-1 BTP 7-14 Documents**

<i>BTP 7-14 Document</i>	<i>Westinghouse Corresponding Document</i>
<i>B.2.2 Documents</i>	
Safety analyses	Software Hazards Analysis (Reference 55)
Verification and validation analysis and test reports	V&V Phase Summary Reports V&V Task Reports V&V Module Test Reports
Configuration management reports	Configuration Baseline Reports Configuration Management Release Reports
Testing Activities	Test Plan System verification test / FAT procedures and test reports
Requirements	PPS System Requirements Specification (Reference 2) PPS System Design Specification (Reference 21) PPS Software Requirements Specification
Design	Software Design Descriptions
Implementation	Software Release Records
Integration	V&V module and unit test reports (Unit tests may be part of the System Verification Test / FAT)



**Table 5.1.2-1 BTP 7-14 Documents**

<i>BTP 7-14 Document</i>	<i>Westinghouse Corresponding Document</i>
Validation	System Verification Test / FAT Reports
Installation	Technical Manual
Operations and maintenance	Technical Manual
<i>B.2.3 Documents</i>	
Software Requirements Specification	(See Requirements above).
Hardware and software architecture descriptions	Software Requirements Specification (for software architecture) System Design Specification (for hardware architecture)
Software design descriptions	(See Design above)
Code listings	Code resides on secure development environment and documented in Software Release Records.
Build documents	Various Westinghouse internal work instructions and PPS Technical Manual
Installation configuration tables	Installation configuration tables reside on secure development environment and documented in Software Release Records.
Operations manuals	PPS Technical Manual
Maintenance manuals	PPS Technical Manual
Training Manuals	Separate training materials as part of a LGS site training program.

### 5.1.3 PSAI 3

*The Common Q SPM only addresses the vendor software planning processes for a Common Q-based system. For all activities in which the applicant or licensee assumes responsibility within a given project (including vendor oversight) for quality assurance, additional evaluations, audits or inspections must be performed to ensure that these licensee responsibilities are fulfilled.*

Constellation has developed a vendor oversight plan that is summarized in the LAR to verify that Westinghouse is performing its activities in accordance with their quality assurance commitments. This verification is conducted by Constellation by way of evaluations, audits or inspections.



#### 5.1.4 PSAI 4

*Because the Common Q SPM does not address the criteria of BTP 7-14 Section B.3.1.8.4, "Software Operations Plan," an evaluation of compliance must be performed at the time of system development when the operational aspects of the system have been defined.*

Westinghouse will develop a technical manual that includes the elements of a Software Operations Plan. As part of Constellation's vendor oversight activities as documented in the LGS PPS vendor oversight plan, Constellation will verify that the elements of BTP 7-14 for a Software Operations Plan is incorporated into the LGS PPS technical manual.

#### 5.1.5 PSAI 5

*Site acceptance testing and installation testing are not covered under the Common Q Software Test Plan because they are considered to be licensee actions that are to be addressed during the development of a Common Q based application. As such, a project specific, site acceptance and installation test plan should be developed and used to address these aspects of software test planning. Because the Common Q SPM does not address all aspects of the BTP 7-14 Section B.3.2.4 criteria, an evaluation of compliance must be performed at the time of system development when the site and installation testing activities have been defined.*

Constellation's Engineering Change (EC) Process, CC-AA-102, "Configuration Change Control for Permanent Physical Plant Changes", provides the guidance to develop a test plan and identifies testing including pre-installation testing, construction testing, functional testing, software V&V, additional post installation testing, and post installation return to service tests. The Responsible Engineer (RE) determines testing acceptance criteria to assure that the configuration change adequately supports existing design basis requirements or meets new requirements that exist due to the implementation of the configuration change. The RE is responsible for preparing the EC testing acceptance criteria and requirements in accordance with CC-AA-107, "Configuration Change Acceptance Testing Criteria", CC-AA-107-1001, "Post Modification Acceptance Testing", and CC-AA-256 "Process for Managing Plant Modifications Involving Digital Instrumentation and Control Equipment and Systems", with input from the System Engineering, Maintenance, Operations, and other reviewers as applicable. The combination of these procedures provides various testing development, test methods and testing requirements. The System Manager (SM) reviews the acceptance criteria for Modification tests, Operability tests, and nonstandard Post Maintenance Testing (PMTs) that would most appropriately be performed as an Installation test provided in the configuration change package. The SM verifies the reasonableness of the testing required to verify the acceptance criteria and determines what procedure(s) needs to be used to perform the required testing. The SM develops a special test procedure if vendor tests, or work order activities of existing procedures are not adequate. The SM coordinates the efforts and resources associated with development and conduct of tests including briefing Operations on testing that is to be done after a system is placed back into service or after the plant has started up.

CC-AA-107 ensures all configuration changes (modifications) require testing. This testing verifies (if applicable):



- That the installed configuration corresponds to the design configuration and that the quality of the workmanship is acceptable. These typically consist of continuity checks, Non-Destructive Examination (NDE) of welds, leak checks, pressure tests, instrument calibration, bump check motors to ensure they rotate in the correct direction (clockwise or counterclockwise).
- These may also include validating assumptions or engineering judgments used as input into designs.
- That design requirements (i.e., required flows, response time requirements) are satisfied.
- Proper functioning of logic systems. These tests verify that inputs can provide the required automatic and normal functions including initiations, trips, and alarms. Interlocks function properly.
- That the modified SSCs have no unexpected or adverse impact upon existing systems and components.

In addition to Factory Acceptance Testing that is covered by the PPS provider and has guidelines in licensee procedure CC-AA-107-1002, CC-AA-107 identifies two types of testing to be completed and procedures to be developed by the RE & SE:

1. Site Acceptance Testing (SAT)
2. Modification Acceptance Testing (MAT)

SAT and MAT is identified in the EC but is controlled outside the EC process. The Engineering Change Process points to Constellation's Post Modification Testing and Special Instructions, CC-AA-107, for the details for performing testing. Modification and special testing are controlled by this process, which creates a SAT & MAT procedure or work order to perform post modification Functional Testing. The SAT & MAT demonstrate that modified or affected systems, structures, or components will perform satisfactorily in service and satisfy design requirements. The combined format demonstrates that modified or affected systems, structure, or components will perform satisfactorily in service and satisfy design requirements. The MAT will be used for Post Return to Service Testing. The SM is a qualified individual that is responsible for coordinating review and approval of MAT. This includes reviewing and concurring with the acceptance test criteria and requirements developed by the RE, in addition to the SAT and MAT development and performance, and Return to Service (RTS) for the EC. All EC and acceptance test criteria requirements are captured by at least one of the above types of tests.

The SAT is conducted in an operational environment to determine whether a system satisfies its acceptance criteria (i.e., initial requirements and current needs of the user) and to enable the licensee to determine whether to accept the system. The extent of Site Acceptance Testing is determined based on the system functionality, complexity of a change, and the susceptibility for equipment damage during shipping.

The MAT is performed to ensure design intent has been satisfied. Modification tests demonstrate that modified components properly function and the inter-relationship with other components within the affected boundary of the configuration change are not adversely impacted. Modification testing addresses both normal and abnormal operating conditions to the extent practicable. Since the test is to demonstrate proper function of the system as modified, actuation of sensors and components by the process medium should be required wherever possible. Some examples are valve stroke times, electrical circuit logic tests, system flow tests, demonstration of failure mode on loss of power, instrument system response tests, and



emergency system actuation tests. Modification tests are performed to written instructions, including acceptance criteria and per applicable procedures. Station procedures may be used for, or to augment, modification testing. Separate modification tests may not be required if compliance with equipment and system requirements is demonstrated by installer's testing. The MAT also provides guidance for power ascension testing if required.

The combination of SAT & MAT is a systematic philosophy that, in general, has an EC test the modification under all configurations:

- Test not only what has been added by the EC, but also what has been deleted,
- Test the EC thoroughly and at least one step beyond boundary of the EC to interfacing equipment (SSCs), which hasn't been modified,
- Avoid testing by simulation when equipment may be operated,
- Consider use of the Simulator and other methods to aid in developing and validating the test procedure/instruction and be sequenced to perform the most basic tests first, then proceed to perform more complex component and system level functional and acceptance tests.

Testing will be controlled with procedures or work orders that will use the MAT format. Many of the tests for the LGS PPS including the SAT will be performed with a procedure developed specifically for this EC due to the complexity of the testing.

Testing will be based on design requirements specified in the Westinghouse documents, as well as those specified in the EC Acceptance Test Criteria. Testing will also address license requirements associated with the LGS Technical Specification, which will include the approved changes for this modification. Testing will include hardware and software functional testing, verification of field inputs and outputs, post-installation testing, and integrated testing. Verification of response times, availability, and reliability of system hardware under normal and abnormal operating conditions will be performed to confirm the requirements in the LGS technical specification.

### 5.1.6 PSAI 6

*A licensee implementing an application based upon the Common Q platform should perform a review of the current Common Q Record of Changes document to assess the validity of previously derived safety conclusions if changes have been made to the Common Q SPM.*

The SPM has gone through a minor revision since the last NRC approval. This was an administrative revision to clarify that Westinghouse acquired the AC160 product line from ABB and any references to ABB's ownership of AC160 is historical in nature. No changes were made to the text of the topical report. This revision does not reduce any commitments. This revision was provided to the NRC for information in May 2021 (ML21146A201). As part of Constellation's vendor oversight activities, they will perform a review of the Common Q Record of Changes document, which includes this change to the SPM.

### 5.1.7 PSAI 7

*Secure Development and Operational Environment – An applicant or licensee referencing the Common Q SPM for a safety-related plant specific application should ensure that a secure development and*



*operational environment has been established for its plant specific application, and that it satisfies the applicable regulatory evaluation criteria of RG 1.152, Revision 3.*

Section 8 describes how the PPS project will meet the requirements in NRC Regulatory Guide 1.152 for a Secure Development and Operational Environment.

The NRC-approved Common Q SPM (Reference 6) describes the Westinghouse Secure Development Environment. As part of the Constellation vendor oversight activities, Constellation will verify the secure development environment at Westinghouse meets the criteria in Section 12 of the SPM.

See Section 8.2 for the Secure Operational Environment vulnerability assessment and the correlation to system requirements.

## **5.2 SYSTEM AND SOFTWARE DEVELOPMENT ACTIVITIES (D.4.2.1)**

The NRC-approved SPM (Reference 6), Section 4.3.2 describes the tasks and responsibilities for each life cycle phase. These tasks and responsibilities are applicable to the LGS PPS project and will be followed. The detailed description of analyses, reviews and test activities for each life cycle phase are described in the SPM Sections 3 (Software Safety Plan), 4 (Software Quality Assurance Plan), 5 (Software V&V Plan), 6 (Software Configuration Management Plan), 7 (Software Test Plan), and 12 (Secure Development and Operational Environment Plan).

### **5.2.1 Plant and Instrumentation and Control System Safety Analysis (D.4.2.1.1)**

As described in Section 3.3, there are no changes to the plant safety analysis associated with the LGS PPS project. According to the software classifications in the NRC-approved SPM (Reference 6), the PPS software in the AC160 controllers is classified as Protection (safety-critical) class. The Safety Display and the MTP software is classified as Important to Safety. This is documented in the LGS PPS Software Development Plan (Reference 25). The independent V&V will be performed in accordance with the NRC-approved SPM for Protection class software for the AC160 controller software and for Important to Safety for the Safety Display and MTP software.

### **5.2.2 Instrumentation and Control System Requirements (D.4.2.1.2)**

The project input documents are collected and defined in a configuration baseline<sup>238</sup>. These documents include Constellation input documents along with Westinghouse PPS product documents like the PPS System Requirements Specification (Reference 2). The attributes of the System Requirements Specification (i.e., Reference 2) are described in Section 3.3.3. The LGS PPS System Requirements Specification and System Design Specification are independently reviewed, traced to input documents identified in the configuration baseline, and approved.<sup>239</sup> The configuration baseline is then revised to incorporate the LGS PPS system requirements specification (Reference 21) and system design specification (Reference 21) for later system development life cycle activities.

A requirements traceability matrix (RTM) is created to trace the LGS PPS system requirements to hardware and software design, implementation and test.<sup>240</sup> The independent V&V performs a



requirements traceability analysis (RTA) in accordance with the Common Q SPM (Reference 6) Section 5.4.5.3.

### **5.2.3 Instrumentation and Control System Architecture (D.4.2.1.3)**

The LGS PPS System Design Specification (Reference 21) defines the LGS PPS system architecture. The technical elements described in Section 3.2 of this document are described in the LGS PPS System Design Specification (Reference 21). As described in Section 5.2.2, the LGS PPS System Design Specification is independently reviewed, approved, and baselined as an input to the ongoing life cycle activities.

### **5.2.4 Instrumentation and Control System Design (D.4.2.1.4)**

The PPS system design specification (References 21) defines the system design. It is traced bidirectionally using the requirements traceability matrix as described in the Common Q SPM (Reference 6), Section 5.4.5.3. The functional requirements also traced to design basis documents.

DI&C-ISG-06 (Reference 1), D.4.2.1.4 states, “DI&C system safety analyses should be reviewed to identify hardware, software, or human-system interfaces that have the potential to cause a hazard or are credited to eliminate or mitigate hazards.” The LGS PPS FMEA (Reference 40) identifies the hardware and human-system interface hazards and their mitigation or elimination, and the LGS PPS SHA (Reference 55) identifies the software hazards and their mitigation or elimination.

As described in Section 5.2.2, the LGS PPS System Requirements Specification and System Design Specification are independently reviewed, approved, and baselined as an input to the ongoing life cycle activities.

### **5.2.5 Software Requirements (D.4.2.1.5)**

The LGS PPS Software Requirements Specification (SRS) will be developed in accordance with the NRC-approved SPM (Reference 6), which states that the SRS complies in content but not format to IEEE Std 830-1998, “IEEE Recommended Practice for Software Requirements Specifications” as augmented by NRC Regulatory Guide 1.172, Rev. 1 (July 2013), “Software Requirements Specifications for Digital Computer Software used in Safety Systems of Nuclear Power Plants”.

The LGS PPS requirements are documented in the LGS PPS system requirements specification (Reference 2) and the LGS PPS system design specification (Reference 21). Those requirements that are allocated to software as described in Section 5, item c and documented in the SRS.

The LGS PPS SRS is the final set of requirements for the software in the system. The SRS documents the requirements for the software in each subsystem (e.g., BPL, LCL, ILP, etc.).

Information in the SRS will be in accordance with the information requirements for an SRS in Section 10.2 of the Common Q SPM



Like the LGS system requirements specification and system design specification, the SRS is independently reviewed, approved, and baselined as an input to the ongoing life cycle activities.

In addition, the RTM is updated showing the tracing of software requirements to the LGS system requirements specification (Reference 21) and system design specification (Reference 21).<sup>241</sup>

An independent V&V team develops module and/or unit test procedures and conducts those tests. An independent test team develops system test plans and procedures, and conducts the system testing. The RTM traces the SRS requirements to either test or inspection documents for requirements validation.<sup>242</sup>

### 5.2.6 Software Design (D.4.2.1.6)

The software design description (SDD) decomposes the software requirements to document the design and implementation of software components, modules, and units used to implement the LGS PPS. The NRC-approved SPM (Reference 6) states that the SDD must comply with IEEE Standard 1016-1998 (Reaffirmed 2009), “IEEE Recommended Practice for Software Design Descriptions”.

There are a number of SDDs that document the complete detailed design of each software element of the system and how the software components are combined into the application program. Each AC160 processor module type (e.g., BPL, LCL, ILP, Safety Display, and MTP) has an SDD.<sup>243</sup> These SDDs describe the software design of the LGS PPS application.

For the AC160 controller there are lower level software modules, referred to as Reusable Software Elements (RSE). These software modules are described in the SDDs and document their instantiation in the application. The independent V&V team writes the module test procedures and test reports for these RSEs.<sup>244</sup>

[

] <sup>a,c</sup> The analysis of the independence of the unused functions from the used functions was performed as part of the original qualification of the platform that was reviewed and approved by the NRC.

The traceability of the LGS SRS to the LGS SDDs will be documented in the RTM to aid in the V&V of the adequate design implementation of the SRS requirements.<sup>245</sup>

The tools used to generate the LGS PPS software are the same tools described in the Common Q topical report (Reference 4). The SPM (Reference 6), Section 3.3.10 defines the requirements for tools used for both development and V&V.

Similar to the LGS system requirements specification, the system design specification and the software requirements specification, the SDDs are independently reviewed, approved, and baselined as an input to the ongoing life cycle activities.



### 5.2.7 Software Implementation (D.4.2.1.7)

The generation of the LGS PPS application software and revised RSEs is governed by the requirements in the NRC-approved SPM (Reference 6), Westinghouse work instructions<sup>246</sup>, the Common Q coding standards (Reference 27), and the Common Q design restrictions (Reference 18).

The LGS PPS application software is reviewed by the independent V&V team for correct implementation of the software requirements.

Each RSE set has a test procedure and test report generated by the independent V&V team. The LGS PPS application software is tested by the independent test team. These tests are developed, performed and documented in accordance with the SPM (Reference 6), which leverages the guidance in IEEE Std 829, and was reviewed and approved by the NRC using the guidance in Regulatory Guide 1.170, “Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants” (Reference 35).

The NRC-approved SPM (Reference 6) states that the RSE module testing shall be performed in accordance with the Test Plan (Section 7 in the SPM) which is in compliance with IEEE Standard 1008-1987 (Reaffirmed 2009), “IEEE Standard for Software Unit Testing”. The RSE testing includes internal state testing.

The RSEs and LGS PPS software is under configuration control, is released using a software release record specifying the configuration baseline for which the software is released. The application software CMRR will identify the RSE libraries used for the application software.<sup>247</sup>

### 5.2.8 Software Integration (D.4.2.1.8)

Section 7 of the NRC-approved SPM (Reference 6) outlines the sequence of tests that define the integration process for the LGS PPS.

- RSE testing (or module testing) – this is the elemental level. The RSE is developed and tested independent of any application program by the independent V&V team.
- Unit testing – this is testing a function chart application in a PM646A processor module, in which RSEs and standard function blocks are instantiated to create the logic for the application. The Safety Display and the MTP software are considered unit software. Often unit testing is combined with Integration and System Validation testing. Unit testing is conducted by either the independent V&V team or the independent test team.
- Integration Test – is an informal test in preparation for the System Validation Test. Any anomalies identified during integration testing are resolved before the System Validation Test, if practical. If not, the open anomaly is tracked during formal System Validation testing.
- System Validation Test – this is formal integration testing of the software and hardware performed by the independent test team. The System Validation Test traces the test cases to the LGS PPS System Requirements Specification (Reference 2) and System Design Specification (Reference 21).



### 5.2.9 Instrumentation and Control System Testing (D.4.2.1.9)

Testing will be conducted in accordance with the Common Q SPM, Section 7 describing the levels of testing of the software modules and units (e.g., MTP and OM) culminating with an integrated system test. Section 7 of the SPM also describes the methodology for response time testing. Multiple runs of the reactor trip and ESFAS functions will be conducted to demonstrate the system meets the response time requirements.

The system testing includes a one-time System Validation Test that is conducted on the first PPS that is built. A Factory Acceptance Test (FAT) is conducted on subsequent LGS units of PPS. This is in accordance with the Common Q SPM (Reference 6). Exhibit 7-1 of the Common Q SPM lists the types of tests that will be conducted on the LGS PPS for FAT.

Both the independent V&V team and the independent test team execute the system test plan in the SPM (Reference 6), Section 7 on a complete, integrated PPS using a baseline version. The independent V&V team executes the module tests and the independent test team executes the system validation testing and FAT. The unit testing is either conducted by the independent V&V team or included in the system validation testing.

The RTM traces the test cases to the LGS system requirements specification (Reference 2), the system design specification (Reference 21), or the software requirements specification which will include the requirements to mitigate or eliminate hazards identified in the FMEA and SHA.

The system test reports will identify the PPS system configuration baseline and software CMRRs that were tested. System test results are documented in a test report. The NRC-approved SPM (Reference 6) states that the test report shall comply with IEEE Standard 829-1998, "IEEE Standard for Software Test Documentation", Section 11.

Similar to the LGS requirements and design documentation, the LGS PPS Test Plan and test documentation are independently reviewed and approved; and stored under configuration control.

### 5.2.10 Project Management Processes (D.4.2.2)

The LGS Project Plan (Reference 28) describes project management processes and project organization. It cites the Project Quality Plan that identifies the Westinghouse 10 CFR 50 Appendix B Quality Assurance procedures to be followed for the project. It describes the controls for identifying the project scope, determination of deliverables, lines of communication, formal and informal reviews, and interfaces with other internal and external organizations.

The LGS Project Plan provides for the establishment, documentation, and maintenance of a schedule that considers the overall project, as well as interactions of milestones. It provides for risk management, including problem identification, impact assessment, and development of risk-mitigation plans for risks that have the potential to significantly affect system quality goals.

The establishment of quality metrics throughout the life cycle to assess whether the quality requirements of IEEE Std 603-1991, Clause 5.3, are being met, in keeping with the additional guidance from IEEE Std



7-4.3.2-2003, Clause 5.3 is achieved by performing the metric processes defined in the NRC-approved SPM (Reference 6), Section 4.5.2.4.

Adequate control of software tools to support system development and software V&V processes, in keeping with the additional guidance in IEEE Std 7-4.3.2-2003, Clause 5.3.2 is achieved by following the NRC-approved SPM (Reference 6), Section 6 Software Configuration Management Plan. The LGS PPS Software Development Plan (Reference 25) describes the use of the various tools used for the LGS PPS.

Those tools used by the design team to develop the PPS application are used in a manner such that defects not detected by the software tool will be detected by independent verification and validation activities. Those tools used by the independent verification and validation team where defects are not detected by downstream IV&V activities have undergone a tool validation program that provides confidence that the necessary features of the software tool function as required.<sup>248</sup>

### **5.2.11 Software Quality Assurance Processes (D.4.2.3)**

The LGS PPS project will follow the software quality assurance plan in the NRC-approved SPM (Reference 6), Section 4.

### **5.2.12 Software Verification and Validation Processes (D.4.2.4)**

The LGS PPS project will follow the software V&V plan in the NRC-approved SPM (Reference 6), Section 5. Exhibit 2-1 in the SPM shows the independence requirements between the V&V and design team. The minimum requirement is that the independent V&V team and the design team shall report to two different directors in the organization. The Westinghouse current organization reporting structure for the independent V&V team and design team meets this requirement.<sup>249</sup>

### **5.2.13 Configuration Management Processes (D.4.2.5)**

The LGS PPS project will follow the software configuration management plan in the NRC-approved SPM (Reference 6), Section 6. The LGS Digital Modernization Project Configuration Management Plan (Reference 32) provides the project specific details for configuration management.



## **6 PPS - APPLYING A REFERENCED TOPICAL REPORT SAFETY EVALUATION (D.5)**

The PPS is based on the Common Q Platform. Westinghouse has on record an NRC-approved topical report on the Common Q Platform (Reference 4).

### **6.1 COMMON Q PLATFORM CHANGES (D.5.1.1)**

Managing changes to a safety system platform after the initial NRC Safety Evaluation Report (SER), and how these changes are reviewed by the NRC in a timely fashion, has been a topic of concern for digital software-based safety systems. The Common Q Platform received its original SERs from the NRC's Office of Nuclear Reactor Regulation (NRR) that encompassed a) the Topical Report including closeout of generic open items (GOIs) in February 2003 and b) the Software Program Manual in September 2004. In May 2021 Westinghouse received an SER from the NRC on the updated version of the Common Qualified Platform Topical Report (Reference 4), and in November 2018, Westinghouse received an SER from the NRC on the updated Software Program Manual for Common Q Systems (Reference 6).

There have been changes to the Common Q Platform since its approval. Westinghouse has a documented change process that evaluates platform changes. The process evaluates each change of the platform against the safety conclusions reached by the NRC in its safety evaluation report for the platform. This process is described in WCAP-17266-P, "Common Q Platform Generic Change Process" (Reference 12).

Appendix 5 of the Common Q Topical Report (Reference 13) is the output document for the change process described in Reference 12. The document provides a summary of changes and then a detailed recording of analysis and/or qualification documents, and a conclusion statement on the status of the change relative to the NRC safety conclusions. Reference 13 can be audited by the NRC staff to achieve reasonable assurance that Westinghouse is maintaining the Common Q Platform within the bounds of the safety conclusions in the safety evaluation of the platform.

#### **6.1.1 Common Q Platform Topical Report Revision**

The Common Q Platform Topical Report revision that applies to this licensing technical report and LAR is Revision 4 (see Reference 4)

### **6.2 RESOLUTION OF TOPICAL REPORT PLANT-SPECIFIC ACTION ITEMS (D.5.1.2)**

The Common Q Topical Report (Reference 4) has two Generic Open Items (GOIs) and 25 Plant-Specific Action Items (PSAIs). PSAI 3 is closed and does not need to be addressed by licensees.<sup>250</sup> This section addresses each for the LGS PPS. The Common Q Software Program Manual (Reference 6) also has PSAIs. These are addressed in Section 5.



## 6.2.1 Generic Open Items

Although the SER for the Common Q Topical Report lists 12 GOIs, all have been closed but two. These are addressed in this section.

### 6.2.1.1 GOI 8

GOI 8 states: *Westinghouse needs to provide in future submittals the design information for the loop controllers to support their diversity from the Common Q components. This is discussed in Section 4.4.4.3.2.*

This GOI refers to the loop controllers described in the Common Q Platform Appendix 4 (Reference 15). The loop controllers fulfill the function of a priority module as described in DI&C-ISG-04, Section 2 Command Prioritization (Reference 9). The PPS utilizes the CIM for the priority module function. The CIM design is documented in the technical report WCAP-17179-P, “AP1000<sup>®</sup> Component Interface Module Technical Report”, Reference 8. Westinghouse has docketed a previous revision 2 of WCAP-17179-P (see ML102170259 for non-proprietary version) for NRC review as part of the 10 CFR 52 AP1000 Design Certification process. It is a Tier 2\* document incorporated by reference (IBR) in the Vogtle 3&4 UFSAR. As shown in the references, WCAP-17179-P is currently at Revision 6. Since the release of Revision 6, Vogtle 3&4 submitted LAR 16-021 (ML16293A033) capturing all the changes since WCAP-17179-P, Revision 2, in a UFSAR Appendix 7A.

In addition to the review of the CIM design, the NRC targeted Vogtle 3&4 ITAAC 2.5.02.14 for NRC vendor QA inspection. The ITAAC covers the CIM life cycle phases from Design Requirements to Installation. The following NRC ADAMS accession numbers are the NRC ITAAC inspection reports on the CIM development: ML111890000, ML111890005, ML14058A995, ML14262A351, ML15363A360<sup>251</sup>.

The PPS D3 Analysis (Reference 11) describes the safety case for reaching the conclusion that CCF for the CIM has been adequately addressed.

### 6.2.1.2 GOI 12

GOI 12 states: *Westinghouse has not yet concluded seismic, environmental and Electromagnetic Compatibility (EMC) qualification testing of the following Common Q platform hardware components:*

- *CI528W Communications Interface Module*
- *ATS-PCNB-007 – PC Node Box*
- *10160D05 Processor Module*
- *10160D06 Fiber Optic Module*
- *10160D07 Input / Output Module*
- *10160D08 Synchronization Module*
- *10160D09 Power Supply Module*

*These hardware components are required to be tested and qualified for the specific plant conditions prior to being placed into operation within a safety system application.*



The PPS does not use this equipment in the PPS architecture, so this GOI does not apply to the PPS (this equipment is related to a new alternate Flat Panel Display System architecture under development and not deployed for the LGS PPS).

## 6.2.2 Plant-Specific Action Items

There are 25 PSAIs for the Common Q Platform Topical Report. One of these PSAIs, PSAI 3, has been resolved generically and therefore is not addressed here. The other 24 PSAIs are addressed in this section.

### 6.2.2.1 PSAI 1

PSAI 1 states: *Each licensee implementing a specific application based upon the Common Q platform must assess the suitability of the S600 I/O modules to be used in the design against its plant-specific input/output requirements. See Section 4.1.1.1.2.*

The PPS System Requirements Specification (Reference 2), Section 4.2 and Appendix A, defines the interface input/output requirements for the PPS. The PPS System Design Specification (Reference 21), Appendix E, allocates these interface input/output requirements to the appropriate AC160 S600 I/O.

### 6.2.2.2 PSAI 2

PSAI 2 states: *A hardware user interface that replicates existing plant capabilities for an application may be chosen by a licensee as an alternative to the FPDS. The Review of the implementation of such a hardware user interface would be a plant-specific action item. See Section 4.1.2.*

The LGS PPS is not using an alternative to the flat panel display system (FPDS) described in the Common Q Topical Report (Reference 4). Therefore, this PSAI does not apply to the LGS PPS.

### 6.2.2.3 PSAI 4

PSAI 4 states: *Each licensee implementing a Common Q application must verify that its plant environmental data (i.e., temperature, humidity, seismic, and electromagnetic compatibility) for the location(s) in which the Common Q equipment is to be installed are enveloped by the environment considered for the Common Q qualification testing, and that the specific equipment configuration to be installed is similar to that of the Common Q equipment used for the tests. The licensee must also ensure that the plant specific common Q system configuration does not exceed the configuration used during platform qualification testing. See Sections 4.2.2.1.1, 4.2.2.1.2, and 4.2.2.1.3.*

*The Common Q test specimen was configured for seismic testing using dummy modules to fill all the used rack slots. As part of the verification of its plant-specific equipment configuration the licensee must check that it does not have any unfilled rack slots. See Section 4.2.2.1.2.*

The LGS PPS EQ Summary Report (Reference 36) analyzes the EQ of the components that make up the PPS and concludes that the testing and results encompass LGS site requirements for the PPS. The spare AC160 controller slots are filled by the AC160 dummy module.<sup>252</sup>



Further equipment qualification testing is required after the detailed hardware design is complete. The EQSR representing this equipment qualification testing will be submitted subsequent to the initial LAR submittal.

#### 6.2.2.4 PSAI 5

PSAI 5 states: *On the basis of its review of the Westinghouse software development process for application software, the NRC staff concludes that the Common Q software program manual SPM specifies plans that will provide a quality software life cycle process, and that these plans commit to documentation of life cycle activities that will permit the NRC staff or others to evaluate the quality of the design features upon which the safety determination will be based. When a license amendment process is used for implementation of a Common Q based safety system, the NRC staff will review the implementation of the life cycle process and the software life cycle process design outputs for specific applications on a plant-specific basis. See Section 4.3.2.*

As stated in DI&C-ISG-06 (Reference 1) Section D.4.2, “Sections D.4.2.1.1 through D.4.2.1.4 address life cycle activities that are part of the NRC review scope. Sections D.4.2.1.5 through D.4.2.1.9 describe process evaluations that are part of the NRC review scope. The evaluation of the design outputs using the process described in Sections D.4.2.1.5 through D.4.2.1.9 are not within the scope of the LAR review. The licensee is responsible for ensuring vendor use of procedures and the acceptability of all vendor work products discussed in Sections D.4.2.1.1 through D.4.2.1.9.”

Section D.4.2.1.1 through D.4.2.1.4 represent the design life cycle phases respectively:

- Plant and Instrumentation and Control System Safety Analysis
- Instrumentation and Control System Requirements
- Instrumentation and Control System Architecture
- Instrumentation and Control System Design

It is understood that the licensee is responsible for ensuring vendor use of correct procedures and the acceptability of all vendor work products discussed in these phases. The NRC staff will also evaluate the implementation of the life cycle process and the software life cycle process design outputs for the PPS for these life cycle phases listed above. This represents the Common SPM life cycle phases 1) Concept and 2) Requirements Analysis (see Reference 6, Section 1.4.1).

As stated in DI&C-ISG-06 above, *Sections D.4.2.1.5 through D.4.2.1.9 are not within the scope of the LAR review.* Section D.4.2.1.5 through D.4.2.1.9 represent the design life cycle phases respectively:

- Software Requirements
- Software Design
- Software Implementation
- Software Integration
- Instrumentation and Control System Testing

This represents the Common Q SPM life cycle phases (see Reference 6, Section 1.4.1):



- Requirements Analysis
- Design
- Implementation or Coding
- Test

The LGS vendor oversight plan describes how LGS will verify Westinghouse use of procedures, and will verify the acceptability of Westinghouse work products to the requirements of the Common Q SPM.

#### 6.2.2.5 PSAI 6

PSAI 6 states: *When implementing a Common Q safety system (i.e., PAMS, PPS, or DPPS), the licensee must review the timing analysis and validation tests for that Common Q system in order to verify that it satisfies its plant-specific requirements for accuracy and response time presented in the accident analysis in Chapter 15 of the safety analysis report. See Sections 4.1.1.4 and 4.1.3.4 of this SE as well as Sections 4.4.1.3, 4.4.2.3, and 4.4.3.3 of Reference 3 for additional information on this item.*

Section 3.2.11 describes how the response time criteria for the Common Q LGS PPS is created and how it will be demonstrated that the PPS calculated response times satisfy the LGS UFSAR safety analysis. These response time requirements are captured in Section 7.1 of the LGS PPS system requirements specification (Reference 2). The Common Q SPM, Section 7, describes the testing to be performed on the PPS. The response time of the PPS will be validated to confirm the system meets the timing analysis results (see the Common Q SPM Exhibit 7-1). The accuracy requirements for the LGS PPS are defined in the PPS System Design Specification (Reference 21) Section 7.2. The accuracy requirements are validated by test as described in the Common Q SPM test plan Section 7.3.1.5 and Exhibit 7-1. The LGS vendor oversight plan describes how the licensee will verify that Westinghouse properly propagates these requirements through the design, implementation, and test of the PPS.

#### 6.2.2.6 PSAI 7

PSAI 7 states: *The OM and the MTP provide the human machine interface for the Common Q platform. Both the OM and the MTP will include display and diagnostic capabilities unavailable in the existing analog safety systems. The Common Q design provides means for access control to software and hardware such as key switch control, control to software media, and door key locks. The human factors considerations for specific applications of the Common Q platform will be evaluated on a plant-specific basis. See Sections 4.4.1.3, 4.4.2.3, 4.4.3.3, and 4.4.4.3.6 of Reference 3 for additional information on this item.*

See DI&C-ISG-04 Position 10 disposition in Section 3.2.21.

Constellation has engaged INL to perform the human factors evaluation for the Safety Displays.

Section 3.3.2.5 describes how access control meets the criteria of IEEE Std 603-1991.



#### 6.2.2.7 PSAI 8

PSAI 8 states: *If the licensee installs a Common Q PAMS, PPS or DPPS, the licensee must verify on a plant-specific basis that the new system provides the same functionality as the system that is being replaced, and meets the functionality requirement applicable to those systems. See Sections 4.4.1.3, 4.4.2.3, and 4.4.3.3 of Reference 3 for additional information on this item.*

Sections 3.2 - 3.4 describe the functions of the PPS. Some of these functions are changed or new, and the safety case for these are included in those sections. The System Requirements Specification (Reference 2), Section 5, defines the system functional requirements for the PPS to meet the functionality described herein. These functional requirements will be traced through the system development life cycle through implementation and test.

#### 6.2.2.8 PSAI 9

PSAI 9 states: *Modifications to plant procedures and/or TS due to the installation of a Common Q safety system will be reviewed by the NRC staff on a plant-specific basis. Each licensee installing a Common Q safety system shall submit its plant-specific request for license amendment with attendant justification. See Sections 4.4.1.3, 4.4.2.3, and 4.4.3.3 of Reference 3 for additional information on this item.*

The changes to the technical specifications as a result of the Digital Modernization Project are included as an attachment to the LAR. The technical specification changes include the elimination of some manual surveillance requirements related to the PPS. WCAP-18461-P-A (Reference 54) is the NRC-approved WCAP that explains the process for evaluating the AC160 and CIM diagnostics with the standard Westinghouse PWR tech specs to credit removing manual surveillance testing from those tech specs. Appendix A in this LTR applies the same process using the LGS tech specs to determine what manual surveillance tests can be removed as a result of the analysis of the AC160 and CIM diagnostics with relationship with the overall PPS architecture and Failure Modes and Effects Analysis. The WCAP includes a number of Licensee Required Actions, and the WCAP NRC SER has 4 Application Specific Action Items (ASAI's). These are dispositioned in Appendix A. Appendix A describes which surveillances would be removed from the tech specs, but the complete set of tech spec markups is a separate attachment to the LAR. The tech spec changes in the LAR attachment takes into account the architectural change of the plant safety systems as a result of the PPS upgrade as well as the removal of certain surveillances as a result of the analysis in Appendix A for crediting self-diagnostics.

#### 6.2.2.9 PSAI 10

PSAI 10 states: *A licensee implementing any Common Q application (i.e., PAMS, PPS, or DPPS) must prepare its plant-specific model for the design to be implemented and perform the FMEA for that application. See Section 5.0 and 4.1.3.4 of this SE as well as Sections 4.4.1.3, 4.4.2.3, and 4.4.3.3 of Reference 3 for additional information on this item.*

The model for the LGS PPS is defined in the PPS System Design Specification (Reference 21). The FMEA (Reference 40) for the LGS PPS is summarized in Section 3.2.22.



#### 6.2.2.10 PSAI 11

PSAI 11 states: *A licensee implementing any Common Q application (i.e., PAMS, PPS, or DPPS) shall demonstrate that the plant-specific Common Q application complies with the criteria for defense against common-mode failure in DI&C systems and meets the requirements of BTP 7-19. See Sections 4.1.6 of this SE as well as Sections 4.4.2.3, 4.4.3.3, and 4.4.4.3.3 of Reference 3 for additional information on this item.*

The LGS defense against common-mode failure (i.e., common cause failure) is addressed in Section 3.2.23.

#### 6.2.2.11 PSAI 12

PSAI 12 states: *A licensee implementing a Common Q DPPS shall define a formal methodology for overall response time testing. See Section 4.4.3.3 of Reference 3 for additional information on this item.*

As part of the PPS license amendment request, Constellation is proposing elimination of specific technical specification surveillance requirements including response time by crediting AC160 diagnostics. Appendix A - "Elimination of Specific PPS Technical Specification Surveillance Requirements" provides the analysis and justification for this technical specification change. The LGS PPS is tested at the factory and during installation to confirm that the response time for the system is met. The methodology used is found in the Common Q SPM, Exhibit 7-1.

#### 6.2.2.12 PSAI 13

PSAI 13 states, *The analysis of the capacity of the shared resources to accommodate the load increase due to sharing. Section 4.4.4.3.1 of Reference 3 for additional information on this item.*

This PSAI is in reference to the Common Q Topical Report Appendix 4 (Reference 15) that describes an architecture that integrates the functions of the plant protection system, core protection calculator system and the post-accident monitoring system. The LGS license amendment is only replacing the RPS/NSSSS/ECCS functions and RG 1.97 variable display functions and does not include a separate Core Protection Calculator System as described in the Common Q Topical Report Integrated Solution Appendix. The RG 1.97 monitoring display function is integrated with the PPS Safety Display. The design of the PPS with the additional functionality of the post-accident monitoring system will conform to the Common Q application design restrictions (Reference 18) for CPU load and AF100 restriction requirements.

#### 6.2.2.13 PSAI 14

This PSAI states: *The licensee implementing Common Q applications must ascertain that the implementation of the Common Q does not render invalid any of the previously accomplished TMI action items. See Section 5.0.*

The LGS UFSAR was reviewed for TMI commitments. The following commitments in the UFSAR are relevant to the PPS upgrade:



LGS UFSAR Section 1.13, “TMI-2 Related Requirements for New Operating Licenses contains the TMI action items for the plant. For NUREG-0737m Enclosure 2, there are several commitments that are relevant to the PPS upgrade and are dispositioned here.

Item I.D.1, “CONTROL ROOM DESIGN REVIEWS,” LGS performed a Control Room Design Review. Constellation has engaged INL to perform the HFE evaluation on the MCR modifications to assess the impact, if any, on the original design review documented in the UFSAR.

For Item I.D.2 “PLANT SAFETY PARAMETER DISPLAY CONSOLE,” the UFSAR credits the LGS Plant Monitoring System SPDS function. Some of the inputs to the SPDS come from the safety-related PPS. In support of the requirements for SRM-SECY-093-087, Position 4, for independent and diverse displays of the LGS Critical Safety Functions, those PPS inputs for the SPDS will be provided by sharing that input PPS signal prior to input signal being processed by the PPS. This will be accomplished by splitting the signal at the PPS input for the SPDS with a safety qualified isolator. Those PPS outputs for the SPDS (e.g., isolation valve actuation status), will be provided by providing the actuating device feedback through the CIM and to the Y-Port to the non-safety DCS that then provides the data to the Plant Monitoring System. See also the response to GOI 8, Section 6.2.1.1.

Item II.B.4 “TRAINING FOR MITIGATING CORE DAMAGE” requires the applicant to develop a program to ensure that all operating personnel are trained in the use of installed plant systems to control or mitigate an accident in which the core is severely damaged. LGS will be upgrading their plant reference simulator to reflect the new PPS systems and human system interfaces. The control room operators will be trained and qualified using the upgraded simulator before the new PPS is placed in service for the operating plant.

II.D.3 “RELIEF AND SAFETY VALVE POSITION INDICATION,” requires RCS relief and safety valves be provided with a positive indication in the control room derived from a reliable valve position detection device or a reliable indication of flow in the discharge pipe. There are clarifications included as part of this requirement. The UFSAR identifies two systems to address this requirement: 1) a non-safety acoustic monitoring system and 2) a safety-grade suppression pool temperature monitoring system. SRV acoustic sensors and suppression pool temperature elements are not being replaced as part of the PPS upgrade. However, the MCR indication for these sensors (status lights, indicators) are being replaced by the PPS Safety Displays. Constellation has engaged INL to perform the HFE evaluation on the MCR modifications to confirm that a positive indication is provided to the operators for SRV position indication via the PPS Safety Displays.

II.E.4.2 “CONTAINMENT ISOLATION DEPENDABILITY” has seven positions and 7 clarifications. The LGS UFSAR response to this requirement credits the following systems that will be replaced with the new PPS:

- RCIC
- HPCI
- RWCUC

The new PPS will interface with the RWCUC by initiating isolation signals to the RWCUC. The RCIC and HPCI functions are being replaced by the new PPS. Implementing these functions in the PPS will not



invalidate the responses. The functionality of the RCIC and HPCI systems are being enhanced by adding automatic level control and pressure control. Therefore the descriptions in the UFSAR response to this requirement remains unchanged.

II.F.1 ACCIDENT MONITORING INSTRUMENTATION requires in part that the displays and controls added to the control room, to meet this requirement, do not increase the potential for operator error. An HFE evaluation will be conducted for all control room modifications as a result of the PPS modification to ensure there is no increase in the potential for operator error and the modifications are in compliance with the responses in this UFSAR chapter.

II.F.2 INSTRUMENTATION FOR DETECTION OF INADEQUATE CORE COOLING requires in part instrumentation to provided unambiguous, and easy-to-interpret indication of inadequate core cooling (ICC). The PPS modification does not impact the existing post accident monitoring instrumentation including reactor water level instrumentation. The PPS implementation will preserve the LGS UFSAR display and indication requirements for inadequate core cooling in order to meet RG 1.97, Revision 2 for qualification and continuous indication.

#### II.G.1 POWER SUPPLIES FOR PRESSURIZER RELIEF VALVES, BLOCK VALVES AND LEVEL INDICATORS

The LGS is a Boiling Water Reactor and does not have a pressurizer.

#### II.K.1.5 ASSURANCE OF PROPER ENGINEERED SAFETY FEATURES FUNCTIONING

The safety-related valves, positioning requirements, and positive controls to assure the valves remain positioned in a manner to ensure the proper operation of engineered safety features is not modified as a result of the DI&C Modernization Project.

#### II.K.1.10 REVIEW AND MODIFY, AS REQUIRED, PROCEDURES FOR REMOVING SAFETY-RELATED SYSTEMS FROM SERVICE (AND RESTORING TO SERVICE) TO ASSURE OPERABILITY STATUS IS KNOWN

Any changes to surveillance requirements to ensure the status of the PPS is operable are included Appendix A of this LTR and reflected in the technical specification markups included in the LAR. Operating procedures will be updated, including alarm response procedures when PPS self-diagnostic alarms occur in the MCR.

#### II.K.1.17 TRIP PRESSURIZER LEVEL BISTABLE SO THAT LOW PRESSURE (RATHER THAN PRESSURIZER LOW PRESSURE AND PRESSURIZER LOW LEVEL COINDICENCE) WILL INITIATE SAFETY INJECTION

The LGS is a Boiling Water Reactor and does not have a pressurizer.

#### II.K.1.22 PROPER FUNCTIONING OF HEAT REMOVAL SYSTEMS



The functional requirements for the heat removal systems are unchanged as a result of the DI&C Modernization Project. The defense in depth and diversity between the non-safety main feedwater system and the auxiliary heat removal systems is maintained.

#### II.K.1.23 DESCRIBE ALL USES AND TYPES OF REACTOR VESSEL LEVEL INDICATION FOR BOTH AUTOMATIC AND MANUAL INITIATION OF SAFETY SYSTEMS. DESCRIBE OTHER INSTRUMENTATION THAT MIGHT GIVE THE OPERATOR THE SAME INFORMATION ON PLANT STATUS

Constellation has engaged INL to perform the HFE evaluation on the MCR modifications including any changes to the MCR for reactor vessel level indication for both automatic and manual initiation of safety systems. Automatic initiation functionality of RPS, PCRVICS, ECCS, and ATWS (RRCS) is unchanged as a result of the DI&C Modernization Project.

#### II.K.3.13 SEPARATION OF HPCI AND RCIC SYSTEM INITIATION LEVELS - ANALYSIS AND IMPLEMENTATION

The RCIC auto close of the steam supply valve has been carried over to the PPS logic which will enable RCIC to restart on low water level. The PPS does not impact or change the NEDO-24951 evaluation and conclusions. The functional requirements for RCIC and HPCI are unchanged as a result of the DI&C Modernization Project.

#### II.K.3.15 MODIFY BREAK DETECTION LOGIC TO PREVENT SPURIOUS ISOLATION OF HPCI AND RCIC SYSTEMS

The functional requirements for HPCI and RCIC are unchanged as a result of the DI&C Modernization Project.

#### II.K.3.16 REDUCTION OF CHALLENGES AND FAILURES OF RELIEF VALVES - FEASIBILITY STUDY AND SYSTEM MODIFICATIONS

The low water level isolation setpoint, low-low set relief or equivalent manual actions, and MSIV testing frequency are unchanged as a result of the DI&C Modernization Project.

#### II.K.3.17 REPORT ON OUTAGES OF ECCS SYSTEMS LICENSEE REPORT AND PROPOSED TECHNICAL SPECIFICATION CHANGES

N/A. This is an historical commitment (only 1<sup>st</sup> five years of operation).

#### II.K.3.18 MODIFICATION OF ADS LOGIC - FEASIBILITY FOR INCREASED DIVERSITY FOR SOME EVENT SEQUENCES

The functional requirements for the ADS logic are unchanged as a result of the DI&C Modernization Project.

#### II.K.3.21 RESTART OF CORE SPRAY AND LPCI SYSTEMS



The functional requirements for the restart of LPCI and CS are unchanged as a result of the DI&C Modernization Project.

#### II.K.3.22 AUTOMATIC SWITCH-OVER OF RCIC SYSTEM SUCTION – VERIFY PROCEDURES AND MODIFY DESIGN

The functional requirements for RCIC system suction valve logic to automatically switch suction from the CST to the suppression pool on low CST level are unchanged as a result of the DI&C Modernization Project.

#### II.K.3.24 CONFIRM ADEQUACY OF SPACE COOLING FOR HPCI AND RCIC SYSTEMS

HPCI and RCIC room unit coolers are not controlled via the PPS and no changes to unit cooler power supplies are being made.

#### II.K.3.25 EFFECT OF LOSS OF AC POWER ON PUMP SEALS

The DI&C Modernization Project does not include the cooling water to the reactor coolant pump seal cooling systems the RECW system and the recirculation pump seal purge system.

#### II.K.3.27 PROVIDE COMMON REFERENCE LEVEL FOR VESSEL LEVEL INSTRUMENTATION

The reactor vessel water common reference for level instrumentation is unchanged as a result of the DI&C Modernization Project.

#### II.K.3.28 VERIFY QUALIFICATION OF ACCUMULATORS ON ADS VALVES

No impact to the LGS response as a result of the DI&C Modernization Project.

#### II.K.3.44 EVALUATION OF ANTICIPATED TRANSIENTS WITH SINGLE FAILURE TO VERIFY NO FUEL FAILURE

The functional requirements for RRCS (except for the elimination of feedwater runback), RCIC, and HPCI are unchanged as a result of the DI&C Modernization Project. Any change in operator actions will be part of the MCR human factors engineering evaluation for the DI&C Modernization Project.

#### III.D.1.1 PRIMARY COOLANT OUTSIDE CONTAINMENT

The instrumentation and the leak reduction program are not impacted as part of the DI&C Modernization Project.

### 6.2.2.14 PSAI 15

This PSAI states: *During the Software development process, the licensee must specify plant specific requirements for system automatic self-testing features that are needed to ensure proper functioning of the Common Q application during operation. See Section 4.1.1.3.*



The plant-specific requirements for system automatic self-testing features that are needed to ensure proper function of the Common Q application during operation is specified in the PPS System Requirements Specification (Reference 2), Section 8.2 and in the PPS System Design Specification (Reference 21), Section 6. The service/test functions of the LGS PPS are described in Sections 3.2.7 and 0 in this document.

#### 6.2.2.15 PSAI 16

This PSAI states: *A licensee implementing a Common Q DPPS shall ensure that no more than four processor modules are installed within a single AC160 controller. See Section 2.1.*

As shown in the architecture drawing of the four channel PPS in Section 3.2, Figure 3.2-2, there are no more than four PM646A processor modules in a single AC160 controller (i.e., the LCL AC160).

#### 6.2.2.16 PSAI 17

This PSAI states: *A licensee implementing a Common Q DPPS must ensure that all hardware components used for system development are approved for use in nuclear safety system class 1E applications and are listed in Table 1. See Section 2.1 for a discussion of the hardware components of the Common Q platform.*

Section 4 describes the Common Q modules that will be used for the LGS PPS. All of them are listed on Table 1 of the safety evaluation except for the CIM and the [ ]<sup>a,c</sup> power supply. See Section 6.2.1.1 (GOI 8) regarding NRC review of the CIM design and development. The [ ]<sup>a,c</sup> is a Class 1E-qualified power supply that is used in conjunction with the Quint power supply to provide a redundant cabinet power supply system that is diverse in design to avoid a CCF. The [ ]<sup>a,c</sup> is used for the Waterford 3 Common Q Core Protection Calculator System.

#### 6.2.2.17 PSAI 18

This PSAI states: *The licensee implementing Common Q applications must ensure that administrative controls are put into place to ensure that changes to setpoints are only performed while the system is not being relied upon to perform its safety functions. The affected division of the Common Q safety system must be declared inoperable prior to implementation of setpoint changes. See Section 4.1.3.4.*

Table 3.2.21-1 DI&C-ISG-04 Compliance, Position 10 describes the administrative controls for changing setpoints in the LGS PPS. The architecture identifies 4 channels and 4 divisions. A channel will be declared inoperable when a setpoint change is made for that channel. A LGS procedure will be developed to declare a PPS channel inoperable and put the PPS channel in maintenance bypass when changing a PPS setpoint.<sup>253</sup>

#### 6.2.2.18 PSAI 19

This PSAI states: *A licensee implementing a specific application based upon the Common Q platform must ensure that the serial communications link between the MTP and the Processor Module is disabled by means of a physical disconnection (i.e., cable is removed from the serial port at the front of the PM646A). Alternative means of disconnecting this serial communication link may be considered,*



*however, any means of disabling this communication link which rely upon software logic would invalidate the DI&C-ISG-04 conformance safety conclusions in Section 4.1.3.4 Staff Position 1, Point 10 of this SE.*

The serial communications link between the MTP and the PM646A, referred to in this PSAI, is the programming cable that allows the MTP to load a new program into the PM646A. DI&C-ISG-04 compliance to the requirement that a physical disconnection (i.e., cable is removed from the serial port at the front of the PM646A) is addressed in Table 3.2.21-1 DI&C-ISG-04 Compliance, Position 10.

#### **6.2.2.19 PSAI 20**

*This PSAI states: A licensee implementing an application based upon the Common Q platform that utilizes fiber optic cables to connect HSL's between safety divisions shall ensure that all plant specific environmental qualification requirements for this cabling are met. See Section 4.2.2.2.*

Constellation is developing a new Fiber Optic cable specification specific for the DMP. Its document number and title are NE-381, "Nuclear Safety Related Specification for Fiber-Optic Instrumentation and Control System Cable". This document will ensure the fiber optic cable used for the HSLs meet the LGS site environmental qualification requirements.

#### **6.2.2.20 PSAI 21**

*This PSAI states: A licensee implementing an application based upon the Common Q platform that includes implementation of HSL must perform a site specific analysis to quantify the impact of higher electromagnetic emissions on operation of locally mounted equipment. See Section 4.2.2.1.3.*

The LGS Preliminary Equipment Qualification Summary Report (Reference 36) confirms that the electromagnetic emissions from the HSL do not adversely affect the operation of locally mounted equipment.

#### **6.2.2.21 PSAI 22**

*This PSAI states: A licensee implementing an application based upon the Common Q platform that uses AI685 modules configured for either RTD or Thermocouple input must ensure that the installation includes a metallic barrier in front of the module. See Section 4.2.2.1.3.*

The LGS PPS uses the AI687 and AI688 analog input modules in place of the AI685 analog input module as shown in Figure 3.2-2. Therefore this PSAI does not apply to the LGS PPS.

#### **6.2.2.22 PSAI 23**

*This PSAI states: A licensee implementing an application based upon the Common Q platform should perform a review of the current Common Q Record of Changes document to assess the validity of previously derived safety conclusions if changes have been made to the Common Q platform hardware, software, or processes defined in the Common Q TR.*



The product revision levels for all Common Q platform equipment will be finalized before FAT for the PPS. The Common Q Topical Report record of changes document (Reference 13) is a living document that is updated when platform changes are processed in accordance with Reference 12. LGS, via the vendor oversight plan, will compare the equipment part numbers to those listed in Table 1 of the safety evaluation. Where differences exist in part number or product revision, LGS will review the topical report record of changes document (Reference 13) for adequate qualification documentation that demonstrate that the changes do not invalidate safety conclusions in the safety evaluation of the Common Q platform.

#### 6.2.2.23 PSAI 24

PSAI 24 states: *A licensee implementing an application based upon the Common Q platform that relies on the FPDS to perform safety critical functions shall perform an evaluation to address the added reliance on the FPDS to accomplish the required safety functions. The affects of not having the necessary information available on the FPDS during the design basis event should be considered and addressed in this evaluation.*

The safety displays are redundant for each division. As defined in the Common Q SPM (Reference 6), safety critical functions are those functions that are “necessary to directly perform RPS control actions, ESFAS control actions, and safe shutdown control actions”. The Safety Display functions are described in Section 3.2.8. Although the Safety Displays will be used to identify the protection function system level actuation to be manually initiated, the actuation initiation signal will be a hardwired confirm switch that sends the initiating signal to the ILP<sup>254</sup>. All of these manual system level actuations are backups to the automatic functions in the PPS.<sup>255</sup> It is the automatic PPS functions that are credited in the UFSAR.<sup>256</sup>

The PPS D3 Analysis (Reference 11) postulates the loss of the complete PPS, including the safety displays, and identifies the required diverse and independent displays and controls to cope with a CCF.

#### 6.2.2.24 PSAI 25

This PSAI states: *A licensee implementing an application based upon the Common Q platform that relies upon the use of ITPs and the AF100 busses to provide separation between safety and non-safety signals must evaluate the plant-specific design against the independence criteria of IEEE 7-4.3.2-2003, Section 5.6.*

As shown in Figure 3.2-1, the AF100 bus resides within one division of the PPS architecture providing communication among the subsystems (e.g., SDs, MTP, BPL, LCL, ILP, ITP) and does not interface to external boundaries such as non-safety systems or other PPS divisions. Therefore this PSAI does not apply. Figure 3.2-2 shows the connection of the AF100 bus to the CI527 Communication Interface to the SDs and MTP, and the CI631 Communication Interface to the AC160s in one division. Only the unidirectional, fiber optically isolated HSL is used for PPS interchannel and interdivisional communication.



## 7 PPS - COMPLIANCE/CONFORMANCE MATRIX FOR IEEE STANDARDS 603-1991 AND 7-4.3.2-2003 (D.6)

This section provides a compliance/conformance table for IEEE Std 603-1991 and IEEE Std 7-4.3.2-2003. Table 7-1 Compliance/Conformance Matrix for IEEE Std 603 and IEEE Std 7-4.3.2 provides a summary of compliance and a cross reference to sections in this document that explain the compliance/conformance. The Compliance/Conformance column will have the following code:

- C: Complies
- PC: Partially Complies
- E: Exception
- N/A: Not applicable

**Table 7-1 Compliance/Conformance Matrix for IEEE Std 603 and IEEE Std 7-4.3.2**

IEEE Std 603 Clause	IEEE Std 7-4.3.2 Clause	Title	Compliance/Conformance	Section(s)
4.1	4*	Safety System Design Basis	C	3.3.1 Clause 4.1
4.2			C	3.3.1 Clause 4.2
4.3			C	3.3.1 Clause 4.3
4.4			C	3.3.1 Clause 4.4
4.5			C	3.3.1 Clause 4.5
4.6			C	3.3.1 Clause 4.6
4.7			C	3.3.1 Clause 4.7
4.8			C	3.3.1 Clause 4.8
4.9			C	3.3.1 Clause 4.9
4.10			C	3.3.1 Clause 4.10
4.11			C	3.3.1 Clause 4.11



IEEE Std 603 Clause	IEEE Std 7-4.3.2 Clause	Title	Compliance/Conformance	Section(s)
4.12			C	3.3.1 Clause 4.12
5.1	5.1*	Single Failure Criterion	C	3.2.22 3.2.24.1.1
5.2	5.2*	Completion of Protective Action	C	3.3.2.1
5.3	5.3	Quality	C	3.3.2.11 5
	5.3.1	Software Development	C	5.2
	5.3.1.1	Software Quality Metrics	C	5.2.10
	5.3.2	Software Tools	C	5.2.10
	5.3.3	Verification and Validation	C	5.2.12
	5.3.4	Independent V&V Requirements	C	5.2.12
	5.3.5	Software Configuration Management	C	5.2.13
	5.3.6	Software Project Risk Management	C	5.2.10
5.4	5.4	Equipment Qualification	C	4
	5.4.1	Computer System Testing	C	4
	5.4.2	Qualification of Existing Commercial Computers	C	3.3.2.11 6.1
5.5	5.5	System Integrity	C	3.3.2.2
	5.5.1	Design for Computer Integrity	C	3.6.3.1.2
	5.5.2	Design for Test and Calibration	C	3.2.24.2.1
	5.5.3	Fault Detection and Self-Diagnostics	C	3.2.24.2.2
5.6	5.6	Independence	C	3.5.14.5



IEEE Std 603 Clause	IEEE Std 7-4.3.2 Clause	Title	Compliance/Conformance	Section(s)
5.6.1		Between Redundant Portions of a Safety System	PC	3.5.14.1
5.6.2		Between Safety Systems and Effects of Design-Basis Event	C	3.5.14.2
5.6.3		Between Safety Systems and Other Systems	C	3.5.14.3
5.6.4		Detailed Criteria	C	3.5.14.4
5.7	5.7*	Capability for Testing and Calibration	C	3.2.24.1.2
5.8	5.8*	Information Displays	N/A – No specified criteria	N/A
5.8.1		Displays for Manually Controlled Actions	C	3.2.24.1.3
5.8.2		System Status Indication	C	3.2.24.1.4
5.8.3		Indication of Bypasses	C	3.2.24.1.5
5.8.4		Location	C	3.2.24.1.6
5.9	5.9*	Control of Access	C	3.3.2.5
5.10	5.10*	Repair	C	3.3.2.6
5.11	5.11	Identification	C	3.2.24.1.7 3.6.2.1.2
5.12	5.12*	Auxiliary Features	N/A – No specified criteria	N/A
5.12.1		Auxiliary Features	C	3.5.14.6.1
5.12.2		Other Auxiliary Features	C	3.5.14.6.2
5.13	5.13*	Multi-Unit Stations	N/A	3.3.2.7



IEEE Std 603 Clause	IEEE Std 7-4.3.2 Clause	Title	Compliance/Conformance	Section(s)
5.14	5.14*	Human Factors Considerations	C	3.5.14.7
5.15	5.15	Reliability	C	3.3.1 Clause 4.9 3.6.1.1.2
6.1	6*	Automatic Control	C	3.6.3.1.3
6.2		Manual Control	C	3.6.3.1.4
6.3		Interaction between the Sense and Command Features and Other Systems	N/A – No specified criteria	N/A
6.3.1		Requirements	C	3.6.2.1.3
6.3.2		Provisions	C	3.6.2.1.3
6.4		Derivation of System Inputs	C	3.6.5.1
6.5		Capability for Testing and Calibration	N/A – No Criteria	N/A
6.5.1		Checking the Operational Availability	C	3.3.2.3
6.5.2		Assuring the Operational Availability	C	3.3.2.3
6.6		Operating Bypasses	E	3.3.2.8
6.7		Maintenance Bypass	C	3.3.2.9
6.8		Setpoints	C	3.3.2.10
7.1	7*	Automatic Control	C	3.6.3.1.5
7.2		Manual Control	C	3.6.3.1.4
7.3		Completion of Protective Action	C	3.3.2.1
7.4		Operating Bypass	E	3.3.2.8
7.5		Maintenance Bypass	C	3.3.2.9



IEEE Std 603 Clause	IEEE Std 7-4.3.2 Clause	Title	Compliance/Conformance	Section(s)
8.1	8*	Electrical Power Sources	C	3.5.12
8.2		Non-electrical Power Sources	N/A – PPS does not use non-electrical power sources	3.5.12
8.3		Maintenance Bypass	C	3.5.12

\*The standard does not add additional criteria beyond that stated in IEEE Std 603-1991.



## **8 PPS - SECURE DEVELOPMENT AND OPERATIONAL ENVIRONMENT (D.8)**

This section describes the secure development and operational environment of the PPS meeting the guidance in both DI&C-ISG-06 (Reference 1) and RG 1.152 (Reference 17).

### **8.1 SECURE DEVELOPMENT ENVIRONMENT**

The PPS is designed and developed by Westinghouse within their facility up to and including the FAT (except for the first LGS system, see Section 5.1.7). Once FAT is completed, the PPS is shipped to LGS and stored until it is installed in the plant.

While the PPS is at the Westinghouse facility, it is designed and implemented using a secure development environment. The secure development environment is described in the Common Q SPM (Reference 6), Section 12.2.1.2. The NRC evaluated the secure development environment controls. Based on the NRC's review of the Westinghouse Common Q secure development environment as described in the Common Q SPM (Reference 6), the staff concluded that the described controls meet the requirements of RG 1.152 (Reference 17).

Constellation's vendor oversight plan will include verifying that Westinghouse complies with the requirements in the SPM for a secure development environment. This will address the NRC's Plant Specific Action Item 7 in their safety evaluation report for the SPM:

*Secure Development and Operational Environment – An applicant or licensee referencing the Common Q SPM for a safety-related plant specific application should ensure that a secure development and operational environment has been established for its plant specific application, and that it satisfies the applicable regulatory evaluation criteria of RG 1.152, Revision 3.*

### **8.2 SECURE OPERATIONAL ENVIRONMENT**

The NRC stated in its safety evaluation in the Common Q Topical Report (Reference 4), *“Although application software is not within the scope of this review, platform features that contribute to the SDOE for the application are identified and discussed. Credit may be taken for the use of these security capabilities in establishing a secure operational environment for a plant specific safety-related application.”*

The PPS System Design Specification (Reference 21), Section 11, defines the secure operational environment requirements. To meet the criteria of RG 1.152, a vulnerability assessment is included (see Section 8) to confirm that the necessary secure operational environment requirements have been captured in the PPS System Requirements Specification (Reference 2), the PPS System Design Specification (Reference 21) or other document.



## 8.2.1 Secure Operational Environment Vulnerability Assessment

This assessment addresses the secure operational environment for 1) deficiencies in the design that may allow inadvertent, unintended, or unauthorized access or modifications to the safety system that may degrade its reliability, integrity or functionality during operations, and 2) the potential inability of the system to sustain the safety function in the presence of undesired behavior of connected systems as described in RG 1.152 (Reference 17).

The Common Q SPM (Reference 6), Section 12 includes the vulnerability assessment ensuring that the system is developed without undocumented codes (e.g., backdoor coding), unwanted functions or applications, and any other coding that could adversely affect the reliable operation of the digital system. The NRC has reviewed these controls as part of the review of the Common Q SPM (see Safety Evaluation Report, Section 3.2.13, embedded in Reference 6).

### 8.2.1.1 PPS System Architecture

The PPS system architecture is depicted in Figure 3.2-1 and 3.2-2. It consists of the following components:

- AC160 – AC160 controllers perform the PPS safety function (i.e., BPL, LCL and ILP, see Sections 3.2.1 - 3.2.3)
- CIM – the CIM performs the PPS safety component control and is described in Section 3.2.5.
- Safety Display (SD) – There are two SDs per division in the control room and provide the operator with PPS information (e.g., PPS Trip and Bypass Status). The SD also allows the operator to perform system level manual actuations as well as individual component control (See Section 3.2.8).
- MTP – The MTP is a local display system within the locked PPS cabinet that provides system status information, adjustment for addressable constants, and provides for testing the PPS. The MTP also provides the AOI data link to the DCS, and an interface to an IRIG data link for time synchronization and a unidirectional, fiber optically isolated data link to the DCS (see Section 3.2.7).
- AF100 – The AF100 bus is a network within a PPS channel/division to allow the sharing of data between the AC160 controllers, the SDs and the MTP. This network does not extend beyond the boundaries of the channel/division (see Section 3.2.21).
- HSL – The HSL is a point-to-point data link which is used to communicate data within a channel when real time performance is critical (e.g., between BPL and LCL AC160 controllers within a PPS channel) and between channels/divisions (see Section 3.2.21).
- Non-safety Ovation components for SOE and Shared Signals (see Sections 3.5.4 and 3.5.3 respectively)

### 8.2.1.2 PPS Potential Vulnerability Assessment Process

A system's secure operational environment assessment addresses 1) the digital exposure along connectivity pathways for the system including direct and indirect connectivity, 2) the physical exposure of the system, including direct and indirect connectivity, 3) the effectiveness of the communication flow controls, and 4) the effectiveness of the access control and authorization mechanisms. As part of these



assessments, vulnerabilities associated with inadvertent access or changes to a system are examined and failures or unpredictable behavior of connected systems are identified and addressed. This process identifies secure operational environment vulnerabilities associated with inadvertent access or changes to the system by performing an analysis of how the system's functions are accessed. Vulnerabilities related to failures or unpredictable behaviors of connected systems are identified by examination of systems, networks, and communication systems that could be potential pathways for compromise.

This secure operational environment vulnerability assessment documents the controls that are in place as defined by the System Requirements Specification (Reference 2), the System Design Specification (Reference 21), or other document citation to mitigate the vulnerabilities identified.

### 8.2.1.3 Vulnerability Identification

Using Figures 3.2.-1 and 3.2-2 as a reference, digital connectivity pathways are assessed and potential vulnerabilities are identified.

Assessed interfaces to the PPS include:

- The PPS has an AF100 network interface for communication within a division.
- The PPS has HSLs that can communicate within a channel and between channels.
- The MTP and SDs support removable media to allow for saving and loading addressable constants.
- Each division of the PPS has two SDs in the control room. The SD provides the capability to change system addressable constants, activate bypasses, perform component control and manual system level actuations using a conform switch, and individual component control. The SDs also provide display of RG 1.97 variables.
- Each division of the PPS has an MTP. The MTP provides the capability to perform tests, change PPS addressable constants, and activate bypasses.
- The MTP provides an interface to an IRIG data link for time synchronization
- The MTP provides the AOI unidirectional, fiber optically isolated data link to the DCS.
- Each AC160 controller, MTP, and SD provides a connection point for reprogramming or reconfiguring the PPS.
- The MTP has the capability to reboot into Windows to allow the use of the AC160 ACC tool for loading new applications to the AC160 processor modules in a division. The AC160 controller will be inoperable for these activities.
- The CIM Y port is an external communication to the non-safety DCS. Its communication is in compliance with DI&C-ISG-04 (see Section 3.2.21).

[

] <sup>a,c</sup>



### 8.2.1.4 Mitigating System Requirements

#### 8.2.1.4.1 Safety System Independence Features

The following types of interfaces between the PPS and external systems are summarized below along with independence features that protect the safety system from failures of external systems:

1. The MTP connects to the DCS. The MTP transmits data and logs via a fiber optically isolated UDP protocol (e.g., a unidirectional Ethernet link) to the non-safety related DCS. This is referred to as the AOI.
2. The MTP interfaces with the IRIG data link that time synchronizes the PPS MTPs of the four divisions. Each MTP has its separate IRIG data link to synchronize time within the division. [

]<sup>a,c</sup> The conclusion is that such human intervention would not adversely impact the PPS safety functions.

3. The MTP and SD support removable media to allow for loading setpoints and other data that ultimately configure the safety functions in the AC160.

]<sup>a,c</sup> In addition, the MTP contains physical controls (locked cabinet, secure location) in addition to procedural controls (plant site procedures) to ensure that only authorized removable media is inserted into the MTP or SD.<sup>259</sup>

4. The PPS uses the AF100 bus to communicate between the AC160 controllers, the SDs and MTP within a division. The AF100 bus does not extend beyond the boundary of a PPS division.<sup>260</sup>
5. The PPS uses the HSL to communicate between AC160 controllers within a division and to other PPS divisions. As described in the Common Q Topical Report, Section 4.5, the HSL is a unidirectional data link and is fiber optically isolated when used across PPS divisions.<sup>261</sup>
6. The CIM Y-port is used for non-safety DCS control of safety-related components and for component feedback to the DCS. The CIM prioritizes the commands from the safety system and non-safety system. [

]<sup>a,c</sup>

#### 8.2.1.4.2 Compliance with IEEE Std 603-1991, Clause 5.9 Control of Access

Refer to Section 3.3.2.5 for compliance to IEEE Std 603-1991, Clause 5.9.

### 8.2.1.5 Summary of Vulnerabilities, Identified Controls, and Overall Effectiveness of Controls

Table 8.2.1.5-1 Summary of Vulnerabilities, Controls, and Overall Effectiveness identifies the assessed interfaces, associated vulnerabilities, description of controls, assessment of effectiveness of controls, and references to system requirements for the controls. The requirements cited in Table 8.2.1.5-1 Summary of Vulnerabilities, Controls, and Overall Effectiveness will be traced through the LGS PPS development life



cycle for correct implementation through design, implementation, and test, as required by RG 1.152 (Reference 17).



**Table 8.2.1.5-1 Summary of Vulnerabilities, Controls, and Overall Effectiveness**

a,c



















## 9 DISTRIBUTED CONTROL SYSTEM

LGS DEHS is an Ovation Distributed Control System (DCS). The DMP expands this DCS to include the DPS, RRCS and Automated Operator Control Aids functions.

### 9.1 RRCS NEW SAFETY CLASSIFICATION

The RRCS replacement and the Diverse Protection System (DPS) are based on the Ovation platform as depicted in Section 9.2. The RRCS Ovation replacement will perform the same RRCS functions as the existing RRCS except for the feedwater runback function (see Section 9.6).

The current classification of the RRCS is safety-related. The purpose of the RRCS is to fulfill the requirements for the ATWS rule 10 CFR 50.62. One of the requirements of the ATWS rule is that the ATWS system (i.e., RRCS) “must be designed to perform its function in a reliable manner and be independent (from the existing reactor trip system) from sensor output to the final actuation device.”

Although the rule states the equipment must be designed to perform its function in a reliable manner, it does not require the system to be safety-related to meet that criterion. The replacement RRCS is implemented on the Ovation Platform. Although the platform is non-safety related, the reliability of the platform, as demonstrated by the Ovation DCS Platform Reliability Analysis (Reference 65), ensures that the RRCS functions will be performed in a reliable manner (see Section 9.5).

Regarding software reliability, Section 9.4 describes the software QA program for the RRCS. This software development program is comparable to a safety-related software development process (except for the organizational independence for V&V) and therefore ensures the RRCS will perform its functions reliability as required by 10 CFR 50.62.

The same functions, that exist in the current RRCS, are replicated in the Ovation-based RRCS (except for the elimination of feedwater runback). The final actuation device for RRCS ARI will remain independent. The ARI scram valves will be retained in the new architecture. The RRCS will perform the automatic SLCS initiation. The existing SLCS manual initiation consists of safety-related switches that connect directly into the RRCS logic. The SLCS manual initiation will be part of the PPS as a soft control function at the SD.

In summary, changing the classification of the RRCS to non-safety related for the Ovation-based RRCS upgrade meets the requirements of 10 CFR 50.62.

### 9.2 DCS ARCHITECTURE

The LGS non-safety Ovation Distributed DCS expands the existing Ovation Turbine Control and Protection functions to include the functionality of the DPS, RRCS, Automated Operator Aids functions as shown in Figure 9.2-1.

The RRCS/DPS is on a dedicated redundant controller on the DCS network (Drop 4/54). The protection function actuation signals of the RRCS/DPS go to the CIM Z-port via a 1E isolator.



The Automated Operator Aids (Section 9.8) are included in Drops 10/60 and 11/61, and these are connected to the CIM Y-port (via RNIs residing in the PPS cabinet) to allow the DCS network to control components and to obtain component feedbacks from the CIM. These feedback indications support the required diverse indications for the DPS and SRM/SECY-93-087 Position 4 displays. They also interface with the Ovation SOE modules to capture sequence of events data.

Drops 141 and 142 are the interface between the PPS MTP unidirectional UDP/IP datalinks from each PPS Division and the Ovation DCS network.

Drop 212 is the Ovation workstation that supports the human/system interface for the RRCS and DPS.





**Figure 9.2-1 DCS Architecture**



## 9.3 RRCS/DPS SEPARATION AND DIVERSITY

### 9.3.1 Separation

The Ovation-based RRCS and DPS are integrated in a standalone redundant controller utilizing a separate LGS power source than the PPS. It will share the same sensors as the PPS. The sensor cabling will be terminated at the PPS cabinet and the sensor signal cabled to the DPS/RRCS will go through a qualified isolator also located in the PPS cabinet providing electrical isolation between the RRCS/PPS.<sup>262</sup>

The sensors and isolators are powered by the PPS power supply system. The PPS power supply system is described in Section 3.2.8. Due to the diversity characteristics of the power supply design, there is reasonable assurance that the power supply system is not susceptible to a CCF, thus maintaining functional independence of the sensors between the two systems.

The ATWS rule, 10 CFR 50.62 states that the diversity between the two systems must be maintained from sensor output to final actuating device.<sup>263</sup> The sensor configuration for the RRCS meets this rule. Following the NRC review guidance in BTP 7-19, the analog sensor information is shared between the DPS and the PPS. The analog sensor input signal is terminated at the PPS cabinet and split to the RRCS/DPS to the Ovation remote I/O module located in the PPS cabinet. The signal propagates to the DPS/RRCS via fiber optical cable providing PPS 1E electrical isolation protection.<sup>264</sup> The Ovation remote I/O module is considered a PPS RG 1.75 associated circuit. The module goes through an equipment qualification program to ensure that the remote I/O module cannot adversely affect the PPS safety functions.

The RRCS and DPS output signals to the actuating devices go through the CIM via the Z-port. The CIM is described in Section 3.2.4. The extensive testing performed on the CIM and the diversity attributes of the CIM design are described in the PPS D3 Analysis (Reference 11). As a result, there is reasonable assurance that the CIM is not susceptible to a CCF. It can be concluded then, that the actuation signals from the RRCS and DPS are functionally independent from the PPS.

The DPS/RRCS can control individual components through the CIM Y-port. [

] <sup>a,c</sup> These component control signals from the DPS/RRCS are sent through fiber to the Remote Node Interface (RNI) as shown in Figure 3.2.22-1.

### 9.3.2 Diversity

Those portions of RRCS/DPS from sensor output (except for the terminations described in the previous section) to RRCS/DPS actuation signal output are diverse from the PPS. As stated in the previous section, the RRCS/DPS actuation signal outputs go through the Z-port of the CIM and there is reasonable assurance that the CIM is not susceptible to a CCF.

The RRCS/DPS is based on the Ovation platform. The D3 Analysis (Reference 11) describes how the Ovation platform is diverse from the PPS in the following areas defined by NUREG-6303 (Reference 64):

- Human Diversity



- Design Diversity
- Software Diversity
- Functional Diversity\*
- Signal Diversity
- Equipment Diversity

\*By design the RRCS is functionally diverse from the PPS to address the ATWS rule. The DPS is a new design developed to implement backup automatic and manual protection functions in the case the PPS suffers a CCF. The functionality of the DPS is based on the analysis results of the D3 CCF Coping Analysis (Reference 11). The DPS functional requirements are documented separately from the PPS functional requirements incorporating these required functions from the analysis.

## 9.4 DCS SOFTWARE QUALITY ASSURANCE

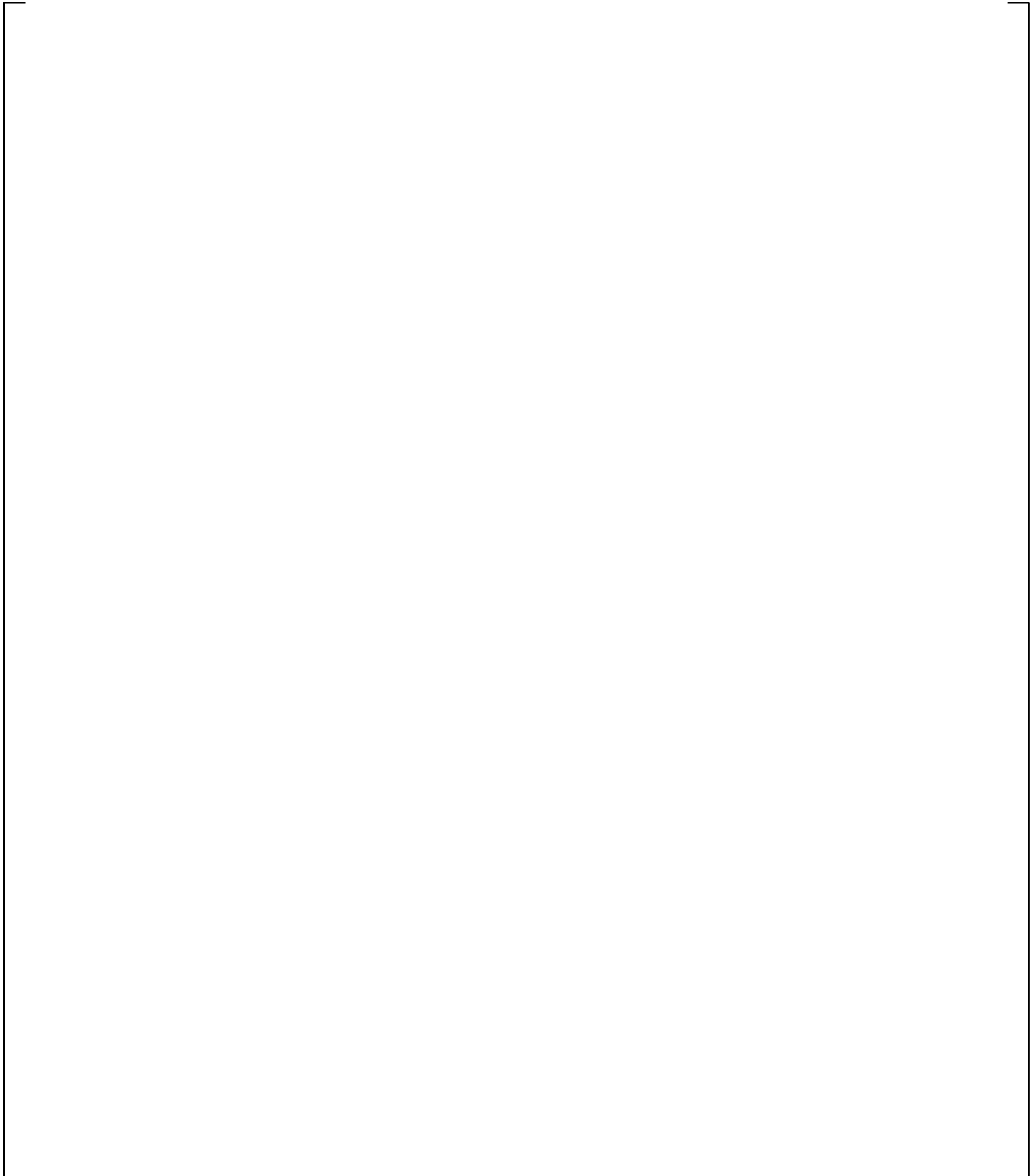
The software for the DCS, including the RRCS/DPS functions, is governed by WNA-PD-00421-GEN, “Control and Information Systems Engineering System Quality Assurance Program,” Reference 63 (SQAP). It includes the lifecycle, configuration management, and verification and validation processes applied to the project. The project will create a System QA and Implementation Plan. The combination of Reference 63 and the project specific System QA and Implementation Plan are considered the overall project SQAP.

The software development process described in the SQAP addresses:

- System Classification and Screening
- System Life Cycle Activities
- System Configuration Management
- System Verification and Validation
- Requirements Management
- Software Coding Standard Practices

The project-specific System QA and Implementation Plan identifies all project documentation required for the application. Figure 9.4-1 shows the project documents that will be produced for the DCS. The development lifecycle for the DCS is of sufficient rigor to ensure the RRCS/DPS perform the necessary backup protection functions in a reliable manner.





**Figure 9.4-1 Software Design Process for DCS**



## 9.5 DCS RELIABILITY

The DCS is based on the Ovation platform. The reliability analysis for the platform is documented in WNA-AR-00039-GEN (Reference 65). It summarizes the reliability of each component in the platform, including those components used for the RRCS/DPS functions. [

]<sup>a,c</sup> The level of reliability of the Ovation platform provides the basis for an Ovation-based DCS to perform its RRCS functions in a reliable manner to meet the ATWS rule.

## 9.6 RRCS FUNCTIONS

The RRCS is designed to provide a redundant and diverse method of shutting down the reactor, in the unlikely event that the RPS does not scram the reactor as a result of an anticipated operating transient. The RRCS logic is initiated when either the high reactor pressure or low reactor water level setpoints are reached. A signal is then sent to the ARI valves that blocks scram air header supply and vents the CRD scram air header to insert the control rods into the reactor. A signal is also transmitted to the RPT breakers to trip the reactor recirculation pumps to reduce the reactor power.

The RRCS receives input from four sensor channels for each function and performs 2oo4 coincidence logic to initiate a function. Should a channel be bypassed, the coincidence logic is reduced to 2oo3.

In the current system, an initiation of the RRCS logic by high reactor pressure will cause the feedwater pumps to automatically runback. If reactor power has not decreased to a predetermined level, within a specified period of time, the RRCS logic will initiate a feedwater runback (FWRB) and the injection of a neutron poison solution into the reactor, via the SLCS, and shut down the reactor. The RRCS FWRB system has given LGS operational problems including:

- LGS has experienced spurious automatic FWRB that has challenged plant operations with a potential LOCA signal to within 2 feet.
- RRCS FWRB (which reduces feedwater turbine speed to minimum without injecting into the reactor) can and does complicate operations while controlling level during an ATWS.

For these reasons, LGS has chosen to eliminate the automatic FWRB function as part of the DMP, while retaining the manual FW pump trip function.

The RRCS FWRB function was intended to mitigate the consequences of an ATWS event by stopping feedwater flow into the vessel, which reduces the core subcooling, thereby reducing the core power generation. GE Hitachi Nuclear Energy analysis, 0000-0097-1195-R0, "Exelon Nuclear Limerick Units 1 and 2 Thermal Power Optimization Task T0902: Anticipated Transients Without Scram," Revision 0, December 2009, provided the ATWS analysis of record (AOR) for LGS Units 1 and 2. CEG has conducted a qualitative evaluation to justify that the LGS ATWS analysis results in the LGS AOR remain valid with elimination of the automatic RRCS FWRB. This evaluation also affirms that the FWRB does not provide any meaningful mitigation function during the LGS ATWS event.

The AOR includes specific values for FWRB delay time and runback rate. The runback rate for ATWS events in the AOR is more conservative (i.e., water level drops more slowly) when compared with a



quicker feedwater reduction when the FWRB is eliminated (e.g., when compared with a flow reduction due to a loss of steam to drive the LGS turbine-driven FW pump following steam line isolation). Therefore, the FWRB elimination has an insignificant impact on the long term ATWS response in peak suppression pool temperature and containment pressure. In addition, since, in the AOR, the FWRB happens after the timing of peak vessel pressure, the FWRB elimination has no impact on the peak vessel pressure.

In terms of peak cladding temperature (PCT) the AOR states that the generic ATWS assessment in NEDC-33879P is used for the LGS ATWS PCT evaluation, and therefore the AOR does not need to explicitly analyze ATWS PCT. Section 3.14.2 of NEDC-33879P also states that the PCT has substantial margin for all plants, and the observed PCT for all plants has been at least 600°F to 700°F below the corresponding 10 CFR 50.46 acceptance criterion of 2200°F. With the automatic FWRB eliminated, there is no change to the integrated time at significant oxidation temperature for the ATWS scenario. The maximum local oxidation criterion continues to be satisfied, and the fuel local cladding oxidation is below the 10 CFR 50.46 limit of 17% of total cladding thickness. Therefore, the PCT and cladding oxidation criteria are also met for FWRB elimination in the generic ATWS evaluation.

Based on this qualitative evaluation, CEG has concluded that the ATWS acceptance criteria for maintaining reactor vessel integrity, containment integrity, and a coolable core geometry will continue to be met with elimination of the RRCS automatic FWRB feature. In addition, the current AOR ATWS analysis conclusions will remain valid with the elimination of the automatic FWRB function.

## 9.7 DPS FUNCTIONS

The DPS functions are those defined in the LGS D3 Analysis (Reference 11). These functions are needed to be implemented in a Diverse Protection System to cope with a postulated PPS CCF. The list of DPS functions are:

[

] <sup>a,c</sup>

Additional Manual Controls to provide the full complement of SRM/SECY-93-087 Position 4 Controls include:

[

] <sup>a,c</sup>



[

] <sup>a,c</sup>

These functions are defined in a separate functional design specification for the DPS (Reference 69).

## 9.8 AUTOMATED OPERATOR AIDS

The Automated Operator Aids is a new feature of the Digital Modernization Project that will automate certain operator controls, that were previously performed manually by the operator from the MCR, to assist in testing and to confirm the plant is configured and ready for safety functions in the PPS. Automating these controls for specific surveillances and system readiness will reduce the exposure to human error. The existing manner in which these manual functions are performed use safety-related controls because they interfaced with safety-related components. Although these functions manipulate safety-related components, the functions themselves are not safety-related and therefore are being transferred to the non-safety DCS and making use of the CIM Y-port for access to the safety-related components.

The types of automated functions that are performed include:

- Checking that pre-requisites for system operation are satisfied and all precautions observed.
- Performing automated system and equipment alignment in readiness for operation.
- Allowing pauses in automated sequences for manual operator actions; upon completion can continue with sequence.
- Allowing an operator to pause or cancel an automated sequence at any time.
- Providing operator monitoring of the automation progress with operator alerts upon failure to complete a sequence.
- An automated control aid is selected at the DCS HMI when the required pre-condition is met.
- Automated control aids that are not allowable are greyed out on the DCS HMI.
- After the automated control aid selection, operator confirmation is required prior to activating the automated control aid.
- For some automated control aids, a selection may cause a message to be displayed (e.g., an interlock is bypassed).
- A DCS HMI display aids in monitoring equipment operation and status.
- An operator can establish or call up pre-defined trends for monitoring.
- Automated Operator Control Aids interface with safety related components via the CIM Y-Port. [

] <sup>a,c</sup>

- Functions are non-safety



Automated control aids are provided for the following systems, which were previously performed manually by the operator in the MCR:

- ADS / SRVs
  - ADS Pressure Control
  - ADS Automatic Depressurization
- Core Spray
  - Core Spray Standby Mode
  - Core Spray Loop Full Flow Test
  - Loop Core Spray Pump, Valve and Flow Test
  - Loop Core Spray Pump Comprehensive and Valve Exercise Test
  - Loop Core Spray System Response Time Test
  - A(B) Loop core Spray Valve Test – Cold Shutdown
  - Shutdown to Standby from Test Modes
- HPCI
  - HPCI Standby Mode
  - HPCI Suppression Pool Transfer to Condensate Storage Tank (CST)
  - HPCI Shutdown to Standby
- RCIC
  - RCIC Standby Mode
  - RCIC Suppression Pool Transfer to CST
  - RCIC Shutdown to Standby
- RHR
  - RHR Standby Mode
  - RHR Suppression Pool Cooling Mode
  - RHR Containment Spray Mode
  - RHR Shutdown Cooling Mode
  - RHR Pump, Valve, and Flow Tests Mode
  - RHR Pump Comprehensive Test
  - RHR Loop Cold Shutdown Valve Test
  - RHR Shutdown to Standby

The DCS Ovation drop that will perform the logic for these controls are Drops 10/60 and 11/61 as shown in Figure 9.2-1. The HSI for the Automated Operator Control Aids can be accessed from any Ovation workstation on the DCS network. The functional requirements for the Automated Operator Aids is defined in the DCS Functional Design Specification, WNA-DS-05080-GLIM, Reference 46.



## **9.9 HUMAN SYSTEM INTERFACE**

The Ovation Workstation is used as the HSI to for RRCS/DPS. The system level RRCS/DPS manual controls are soft controls via the Ovation Workstation. An HFE review (including Integrated System Validation) of the RRCS/DPS displays will be conducted to ensure operators can adequately access the required manual controls for RRCS/DPS functions in accordance with NUREG-0711.



## 10 REFERENCES

1. DI&C-ISG-06, “Digital Instrumentation and Controls Licensing Process Interim Staff Guidance,” ML18269A259, Revision 2, United States Nuclear Regulatory Commission
2. Limerick Generating Station Plant Protection System Digital Modernization Project System Requirement Specification, WNA-DS-04899-GLIM, Revision 0
3. AP1000® Protection and Safety Monitoring System Architecture Technical Report, WCAP-16675-P, Revision 10, Westinghouse Electric Company LLC
4. Common Qualified Platform Topical Report, WCAP-16097-P-A, Revision 5, Westinghouse Electric Company LLC
5. Plant Protection System (PPS) Performance Specification, NE-402, Revision 2, Constellation Energy
6. Software Program Manual for Common Q™ Systems, WCAP-16096-P-A, Revision 5.1, Westinghouse Electric Company LLC
7. Physical Independence of Electric Systems, Regulatory Guide 1.75, Revision 2, US Nuclear Regulatory Commission
8. AP1000 Component Interface Module Technical Report, WCAP-17179-P, Revision 6, Westinghouse Electric Company LLC
9. DI&C-ISG-04, Highly-Integrated Control Rooms—Communications Issues (HICRc) Interim Staff Guidance, ML083310185, Revision 1, United States Nuclear Regulatory Commission
10. S600 I/O Hardware Advant Controller 160 for Westinghouse Version 1.3 Reference Manual, W13BDS005740R501, Rev 0, Westinghouse Electric Company LLC
11. Limerick Generating Stations Units 1 & 2 Digital Modernization Project Defense in Depth and Diversity Common Cause Failure Coping Analysis, WNA-AR-01074-GLIM, Revision 1, Westinghouse Electric Company LLC
12. Common Q Platform Generic Change Process, WCAP-17266-P, Revision 1, Westinghouse Electric Company LLC
13. Common Qualified Platform Record of Changes, WCAP-16097-P Appendix 5, Revision 5, Westinghouse Electric Company LLC
14. Wolf Creek Nuclear Operating Corporation Wolf Creek Generating Station Docket No. 50-482 Amendment to Renewed Facility Operating License, March 31, 2009, US Nuclear Regulatory Commission (ML090610317)
15. Common Qualified Platform Integrated Solution, WCAP-16097-P-A Appendix 4, Revision 0, Westinghouse Electric Company LLC
16. Guidance for the Review of Changes to Human Actions, NUREG-1764, Revision 1 (ML072640413), United States Nuclear Regulatory Commission
17. Criteria for Use of Computers in Safety System of Nuclear Power Plants, Regulatory Guide 1.153, Revision 3 (ML102870022), United States Nuclear Regulatory Commission
18. Application Restrictions for Generic Common Q Qualification, WNA-DS-01070-GEN, Revision 16, Westinghouse Electric Company LLC
19. ALS Diversity Analysis, 6002-00031, Revision 0, CS Innovations, LLC
20. Technical Specifications Limerick Generating Station, Unit No. 1 Docket No. 50-352 Appendix “A” to License No. NPF-39
21. Limerick Generating Station Plant Units 1 & 2 Protection System Upgrade System Design Specification, WNA-DS-04900-GLIM, Revision 0



22. CIM Diversity Analysis, WNA-AR-01054-GEN, Revision 0, Westinghouse Electric Company LLC
23. Preparation of Alarm Response Cards/Procedures, AD-LG-101-1005, Revision 2, Constellation Energy
24. Wolf Creek Nuclear Operating Corporation Wolf Creek Generating Station Docket No. 50-482 Amendment to Renewed Facility Operating License,” March 31, 2009 (ML090610317), US Nuclear Regulatory Commission
25. Limerick Generating Station Plant Protection System Digital Modernization Project Software Development Plan, WNA-PD-00671-GLIM, Revision 0, Westinghouse Electric Company LLC
26. Evaluation of Common Cause Failure Susceptibility of Component Interface Module, WNA-LI-00096-GEN, Revision 0, Westinghouse Electric Company LLC
27. Coding Standards and Guidelines for Common Q Systems, 00000-ICE-3889, Revision 16, Westinghouse Electric Company LLC
28. LGS PPS DMP Project Management Plan, WPMR-PMP-2020-000076, Revision 0, Westinghouse Electric Company LLC
29. Southern Nuclear Operating Company Vogtle Electric Generating Plant Unit 4, Resubmittal of ITAAC Closure Notification on Completion of ITAAC 2.5.02.14 [Index Number 553], ND-17-0824, 22 May 2017 (ML17143A244), Southern Company
30. ITAAC 2.5.01.14 Closure Verification Evaluation Form, September 22, 2017 (ML17268A064) US Nuclear Regulatory Commission
31. Not used.
32. Limerick Generating Station Plant Protection System Digital Modernization Project Configuration Management Plan, WNA-PC-00071-GLIM, Revision 1, Westinghouse Electric Company LLC
33. System Analyses for Elimination of Selected Response Time Testing Requirements - BWR Owners' Group Licensing Topical Report, NEDO-32291 (and supplement), GE Nuclear Energy
34. Not used.
35. Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, Regulatory Guide 1.170, Revision 1, US Nuclear Regulatory Commission
36. Comparison of Equipment Qualification Hardware Testing for Common Q Applications to Limerick Requirements, EQ-EV-386-GLIM, Revision 0
37. Not used.
38. Not used.
39. Limerick 1&2 Determination of Power Consumption and Heat Load for Plant Protection System, WNA-CN-00658-GLIM, Revision 0, Westinghouse Electric Company LLC
40. Limerick Generating Station Plant Protection System Upgrade Failure Modes and Effects Analysis, WNA-AR-01050-GLIM, Revision 0, Westinghouse Electric Company LLC
41. Not used.
42. Limerick PPS Reliability Calculation, WNA-AR-01100-GLIM, Revision 0, Westinghouse Electric Company LLC
43. Reliability and Availability Analysis Methods, WNA-IG-00064-GEN, Revision 3, Westinghouse Electric Company LLC
44. Limerick Generating Station Plant Protection System Digital Modernization Project Units 1&2 Project Quality Plan, WNA-PQ-00538-GLIM, Revision 1, Westinghouse Electric Company LLC.
45. AP1000 Protection and Safety Monitoring System - System Integration Test CIM Priority Test Report, APP-PMS-T2R-080, Revision 1, Westinghouse Electric Company LLC



46. LGS Distributed Control System Functional Design Specification, WNA-DS-05080-GLIM, Rev. 0, Westinghouse Electric Company LLC.
47. LGS Digital Modernization Project PPS J1 Functional Logic Diagrams Index, WNA-J1-00001-GLIM, Revision 0, Westinghouse Electric Company LLC
48. LGS Digital Modernization Project PPS J3 Functional Logic Diagrams Index Part 1, WNA-J3-00001-GLIM, Revision 0, Westinghouse Electric Company LLC
49. LGS Digital Modernization Project PPS J3 Functional Logic Diagrams Index Part 2, WNA-J3-00002-GLIM, Revision 0, Westinghouse Electric Company LLC
50. LGS Digital Modernization Project PPS J5 Functional Logic Diagrams Index, WNA-J5-00001-GLIM, Revision 0, Westinghouse Electric Company LLC
51. LGS PPS to DCS Interface Specification, WNA-DS-05091-GLIM, Revision A, Westinghouse Electric Company LLC
52. Human Factors Engineering Program Plan for Constellation Safety Related Instrumentation and Control Upgrades, INL/LTD-21-64899, Revision 0, Idaho National Laboratory
53. LGS Turbine Control System Upgrade Failure Modes and Effects Analysis, WNA-AR-00267-GLIM, Revision 4, Westinghouse Electric Company LLC
54. Common Q Platform and Component Interface Module System Elimination of Technical Specification Surveillance Requirements, WCAP-18461-P-A, Revision 1, Westinghouse Electric Company LLC
55. Limerick Generating Station Plant Protection System Upgrade Preliminary Software Hazards Analysis, WNA-AR-01051-GLIM, Rev. 0, Westinghouse Electric Company LLC
56. Limerick Generating Station Plant Protection System Upgrade Response Time Calculations, WNA-CN-00603-GLIM, Revision 0, Westinghouse Electric Company LLC
57. Reliability and Availability Analysis Methods, WNA-IG-00064-GEN, Rev. 3, Westinghouse Electric Company LLC
58. Not used.
59. Not used.
60. PPS Accuracy Calculation for Limerick Generating Station, WNA-CN-00662-GLIM, Revision 0, Westinghouse Electric Company LLC
61. CIM-SRNC Test Tool Design Spec, WNA-DS-02904-GEN, Revision 0, Westinghouse Electric Company LLC
62. Not used.
63. Control & Information System Engineering System Quality Assurance Plan, WNA-PD-00421-GEN, Revision 4, Westinghouse Electric Company LLC
64. Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems, NUREG-6303, December 1994, U.S. Nuclear Regulatory Commission
65. Ovation DCS Platform Reliability, WNA-AR-00039-GEN, Revision 3, Westinghouse Electric Company LLC
66. Addendum to Summary Qualification Report of Hardware Testing for Common Q Applications, WCAP-17415-P, Revision 1, Westinghouse Electric Company LLC
67. FMEA of AP1000 Protection and Safety Monitoring System, WCAP-16438-P, Revision 9, Westinghouse Electric Company LLC
68. LGS Feedwater Runback Elimination – ATWS Analysis, 006N8836, Revision 0, GE Hitachi Nuclear Energy (GEH Proprietary Information)
69. CEG LGS 1&2 Distributed Control System Functional Design Specification, WNA-DS-05080-GLIM, Revision 0, Westinghouse Electric Company LLC



70. LGS Units 1&2 PPS DMP Functional Logic Specification, WNA-DS-05129-GLIM, Revision 0, Westinghouse Electric Company LLC
71. Common Q Platform Reliability, WNA-AR-01026-GEN, Revision 0, Westinghouse Electric Company LLC



## **APPENDIX A ELIMINATION OF SPECIFIC PPS TECHNICAL SPECIFICATION SURVEILLANCE REQUIREMENTS**

### **A.1 INTRODUCTION**

#### **A.1.1 Purpose**

The purpose of this appendix is to provide the necessary analysis to justify the elimination of specific Technical Specification (TS) Surveillance Requirements (SRs) related to the PPS. Based on NRC review, this will potentially culminate with the elimination of the need to perform specific surveillances on PPS equipment based on the Common Q platform. This will lead to increased duration of plant operations with full PPS redundancy and reduced operational and maintenance resources over the lifecycle of the PPS.

The scope of this appendix is limited to LGS Units 1&2 TS SRs that apply to the PPS. SR candidates for elimination are outlined in Section A.1.3 of this appendix and are defined within Sections 3/4.3.1, 3/4.3.2, and 3/4.3.3 in the current set of the LGS TS (Reference 20 [Unit 1]). Note that these sections of the TS are being revised as part of the LAR, however the sections of the TS cited herein are the current TS.

#### **A.1.2 Background**

TS establish requirements a nuclear facility must meet during operations. The basis for these specifications can be traced up to 10 CFR 50, “Domestic Licensing of Production and Utilization Facilities”, Section 36 “Technical Specifications”. Specifically relating to the safety system of a nuclear plant is 10 CFR 50.36(c)(ii)(A) which establishes limiting safety system settings for nuclear reactors.

To demonstrate that the PPS is operable, which ensures that limiting conditions of operation (LCOs) are met, the TS stipulate various SRs (per 10 CFR 50.36(c)(3)). These SRs range from functional tests and calibrations, to visual inspections; and are performed on a periodic interval governed by the LGS Surveillance Frequency Control Program. The number of functions related to the PPS coupled with the SR frequency, results in significant testing that is to be performed over the life of the PPS.

Westinghouse submitted and received NRC approval for topical report WCAP-18461-P-A, “Common Q Platform and Component Interface Module System Elimination of Technical Specification Surveillance Requirements” (Reference 54). The WCAP analysis details necessary justification for the elimination of certain SRs based on Westinghouse NSSS TS. These SR eliminations take full advantage of the Common Q platform self-diagnostic features.

The methodology to eliminate TS SRs in WCAP-18461-P-A (Reference 54) assumes a prototypical architecture and performs an analysis on that architecture using an FMEDA table and the Westinghouse NSSS TS.



### A.1.3 Scope of Analysis

This analysis will provide a comparison of the differences in architecture between that used in the WCAP analysis and the PPS architecture. Based on these differences, any changes to the analysis are documented herein and the surveillances of focus are those stated in the LGS TS:

- TABLE 3.3.1-2 “REACTOR PROTECTION SYSTEM RESPONSE TIMES”
- TABLE 4.3.1.1-1, “REACTOR PROTECTION SYSTEM INSTRUMENTATION SURVEILLANCE REQUIREMENTS”, Functional Units 3 – 11. Functional Units 1 – 3 are not within the domain of the PPS, and Functional Unit 12 is Manual Scram is excluded since it is not credited in the LGS UFSAR Chapter 15 analysis (i.e., only automatic reactor trip is credited).
- TABLE 3.3.2-3, “ISOLATION SYSTEM INSTRUMENTATION RESPONSE TIMES”
- TABLE 4.3.2.1-1, “ISOLATION ACTUATION INSTRUMENTATION SURVEILLANCE REQUIREMENTS”, all Functional Units except for Manual Initiation functions since they are not credited in the LGS UFSAR Chapter 15 analysis (i.e., only automatic initiation is credited).
- TABLE 3.3.3-3, “EMERGENCY CORE COOLING SYSTEM RESPONSE TIMES”
- TABLE 4.3.3.1-1, “EMERGENCY CORE COOLING SYSTEM ACTUATION INSTRUMENTATION SURVEILLANCE REQUIREMENTS”, all Functional Units except for Manual Initiation functions since they are not credited in the LGS UFSAR Chapter 15 analysis (i.e., only automatic initiation is credited).
- TABLE 4.3.7.5-1, “ACCIDENT MONITORING INSTRUMENTATION SURVEILLANCE REQUIREMENTS”

For each of these tables in the LGS TS, SRs are required for Channel Check, Channel Functional Test, Channel Calibration, and Response Time. This analysis will focus on these four surveillance tests for RPS, ECCS and NSSSS (i.e., Isolation Actuation).

WCAP-18461-P-A, “Common Q Platform and Component Interface Module System Elimination of Technical Specification Surveillance Requirements”, Reference 54, is an NRC-approved topical report providing an acceptable approach to eliminating technical specification (TS) surveillance requirements (SRs) related to the Common Q Platform and the Component Interface Module (CIM) and Safety Remote Node Controller (SRNC) System. The scope of WCAP-18461-P-A is limited to TS SRs that would apply to an instrumentation and control (I&C) safety system using the Common Q Platform and the CIM/SRNC system. This appendix applies the analysis approach in WCAP-18461-P-A to the LGS PPS to determine the SRs that can be eliminated.

### A.1.4 PPS Architecture

WCAP-18461-P-A, Reference 54, analyzes the SRs to a typical PPS architecture. This architecture is described in Section 2.1 and Appendix A of the topical report. The differences between the architecture in WCAP-18461-P-A and the LGS PPS architecture as shown in Figure 3.2-2 are as follows:

- The AP1000 PMS architecture represented in WCAP-18461-P-A (Reference 54) has more redundancy within the division than in the PPS architecture. The PMS architecture has two redundant BPL, LCL, and ILP AC160 racks whereas the PPS architecture has single AC160s for these subsystems redundant PM646As.



- The CI631 configuration for the LCL and the ILP is different than the LCL and ILP in the AP1000 PMS architecture (see Sections 3.2.2 and 3.2.4).
- The architecture in WCAP-18461-P-A includes a separate AC160 rack for the Post Accident Monitoring System (PAMS), whereas the LGS PPS architecture does not have this PAMS rack but adds a third BPL PM646A processor module to process RG 1.97 variables. This is also the difference in architecture for the BPL in which the AC160 rack has 3 PM646A processor modules vs. two in WCAP-18461-P-A.
- The S600 I/O configuration for the BPL in the topical report includes an AO650 module. The PPS architecture does not include the AO650 in the BPL, however the ILP uses the AO650, so it is analyzed as part of the Logic System Functional Test. The S600 modules depicted in Figure A.1-1 for the BPL in WCAP-18461-P-A are also used by the PPS BPL, although their slot positions in the AC160 rack are different. This differentiation does not affect this analysis because the analysis is not dependent upon the position of the S600 I/O modules in the AC160 rack. However, the DI621 digital input module is used to process reactor trip input signals. This is discussed in Section A.6.2.1.
- The PPS LCL has more DI621 modules and DO620 modules than the LCL in the topical report. The number of modules and their use is germane to the analysis and will be taken into consideration.
- The topical report LCL and ILP deploy only one CI631, whereas the PPS LCL and ILP use a dual-redundant CI631 configuration similar to the APR1400 Safety System design. This difference does not impact the diagnostics identified in Table 5.1-3 in WCAP-18461-P-A (Reference 54).
- The topical report ITP and the PPS ITP have the same complement of S600 I/O modules and communication interfaces. This is important because the ITP is an aggregator of diagnostic information to be reported to the MCR.
- The PPS MTP and the topical report MTP have the same architecture except the PPS MTP as an IRIG-B time synchronization card that is not used for a safety function and therefore is not germane to the analysis. Its vulnerability to the architecture is analyzed in Section 8.2.1.3 and its compliance to DI&C-ISG-04 is addressed in Section 3.2.21.
- There are two SDs per division in the LGS PPS, whereas there is only one topical report SD. As described in Section 3.2.8, the SDs allow the operator to identify the manual system level actuation to be initiated accompanied by a hardwired confirm switch that initiates the actuation. The SDs also allow for individual safety-related component control. Neither of these actions are credited in the accident analysis and therefore do not require a surveillance.<sup>266</sup>
- The LGS PPS architecture has an interposing relay panel called the HARP and a RPS TU that are not described in WCAP-18461-P-A (Reference 54). The HARP is used by the PPS for actuating components (Section 3.5.9) and the RPS TS is used for reactor scram (see Sections 3.2.3 and 3.5.6).

### A.1.5 Single Failure Criteria

In evaluating the single failure criteria, it is necessary to consider single failures together with all other identifiable, but non-detectable failures that may be present in the system. Failures not detected by self-diagnostics are expected to be detected by a surveillance test. With the methodology for eliminating SRs within this appendix, the diagnostics must cover these postulated failure modes. This is done by starting with LGS PPS FMEA (WNA-AR-01050-GLIM, Reference 40), which shows that the PPS is single



failure tolerant. The Failure Modes, Effects, and Diagnostics Analyses (FMEDAs) in WCAP-18461-P-A (Reference 54), Section 6 are based on the failure modes of the AP1000 Protection and Safety Monitoring System. These tables demonstrate diagnostic coverage for the aforementioned failure modes. The LGS PPS FMEA (Reference 40) was compared with the FMEDAs listed in WCAP-18461-P-A (Reference 54), Section 6 to ensure that the failure modes outlined in these tables are bounding.

## **A.2 PPS DIVISION FAULT INDICATION/ANNUNCIATION PATH**

Annunciation is necessary to alert operators when a fault is detected by self-diagnostics within the PPS. There are multiple ways that the operator can be informed of a PPS fault. These are:

- Alarm annunciation by the DCS when it receives a PPS Division Fault Alarm over the AOI data link.
- Visual Indication on the SDs in the MCR
- Technician observation of local status indication and/or the MTP display at the equipment location

Based on the analysis of the differences between the LGS PPS architecture and the PPS architecture described in WCAP-18461-P-A (Reference 54), these are the same alarm pathways described in WCAP-18461-P-A (Reference 54), Section 4.4. There are various alarm signals that are generated from the PPS architecture, some of which are used to indicate a fault within the system. These alarms are indicated on the SDs and MTPs (as described in Sections 3.2.8 and 0), as well as transmitted to the MCR for annunciation via AOI data link to the DCS. The Division Fault Alarm Path described in WCAP-18461-P-A (Reference 54), Section 4.4 is the same for the LGS PPS.

### **Indication and Alarm Path FMEDAs**

The components that are part of both the safety path and the annunciation path are shown in WCAP-18461-P-A (Reference 54), Section 4.4, that demonstrate the diagnostic coverage for these components.

## **A.3 SELF-DIAGNOSTIC FUNCTIONS**

Section 5 of WCAP-18461-P-A (Reference 54) contains the FMEDA tables which demonstrate that postulated failure modes of the PPS equipment can credit the platform/application self-diagnostics to eliminate TS surveillance testing. The diagnostics being credited to cover these failure modes are contained within the various tables within that section of WCAP-18461-P-A (Reference 54). Based on the analysis of the architectural differences between the LGS PPS and the PPS in WCAP-18461-P-A (Reference 54), for those modules used in the LGS architecture, the annunciation described in the FMEDA tables is the same.

## **A.4 APPLICATION DIAGNOSTICS**

The LGS PPS application software contains self-diagnostic functions that are carried out within the ITP PM646A processor modules and the MTP. There are many self-diagnostic functions that monitor the system for errors and report these errors up to the ITP to initiate a Division Fault Alarm. [ ]<sup>a,c</sup>



[ ]<sup>a,c</sup> However, only the following are credited within FMEDAs within this topical report and are applicable to the LGS PPS. These are described in WCAP-18461-P-A (Reference 54), Section 5.3. For each application diagnostic the corresponding PPS System Design Specification (Reference 21) requirement or section number is identified:

- Inter-Channel Comparison Check (PPS-SyDS-371)
- [ ]<sup>a,c</sup> (PPS-SyDS-40071, 40073, 1113)
- [ ]<sup>a,c</sup> (PPS-SyDS-397)
- Application Self-Diagnostics for CIM Component Feedbacks (Section 4.2.1.1)

The application diagnostic described in WCAP-18461-P-A (Reference 54) for the RT Matrix Fault detection will be different for the LGS PPS. Divisions 1 and 2 in the LGS PPS architecture interface, have an RPS TU interface to a set of pilot solenoid valves to initiate a reactor scram (see Sections 3.2.3 and 3.5.6). Similar to the approach described in WCAP-18461-P-A (Reference 54), the ITP will monitor the reactor trip demand signal from the LCLs to the RPS TU feedback signals. If there is an inconsistency between the two after a configurable amount of time, then a Division Fault Alarm will be generated. Figure A.4-1 shows the location of these ITP feedback signals (CM1, CM3, CM5, CM 7). The requirement to do this monitoring is in the PGS PPS System Design Specification (Reference 21) (PPS-SYDS-377).

The Inter-Channel Comparison Check is being performed by the MTP instead of the ITP as described in WCAP-18461-P-A (Reference 54). The purpose for this change is to offload the ITP processing module. The ITP will still be used to share inter-channel data using the HSL. The ITP will pass on that inter-channel data to the MTP via the AF100 bus to execute the inter-channel comparison application diagnostic. The safety case for this change is discussed in Section A.6.1.



a,c

**Figure A.4-1 RPS TU feedback Signals**



## **A.5 PPS SYSTEM HEALTH OBSERVATIONS BY PLANT PERSONNEL**

Section 5.4 of WCAP-18461-P-A (Reference 54) describes the plant personnel actions that will be necessary to ensure adequate operation of the LGS PPS self-diagnostics. Section A.8.8 describes the LGS personnel observations that will be used to assure the self-diagnostics are functioning properly.

## **A.6 LGS PPS FMEA AND AC160/CIM FMEDA TABLES**

WCAP-18461-P-A (Reference 54), Section 6 takes each failure mode from the AP1000 Protection and Safety System FMEA and cross references the PPS self-diagnostics to demonstrate coverage. The architecture of the LGS PPS and the AP1000 Protection and Safety Monitoring System (Reference 67) are similar, so there will be similarities between the two FMEAs. This section highlights the differences in the FMEA's and addresses those differences.

[

] <sup>a,c</sup>



[

]a,c



[  
] <sup>a,c</sup>

The general approach to showing TS SRs can be eliminated described in WCAP-18461-P-A (Reference 54) is used for the LGS PPS.

### A.6.1 Channel Check Elimination Analysis

To eliminate manual Channel Check SRs, WCAP-18461-P-A (Reference 54) describes the ITP Inter-Channel Comparison Check being credited to provide the same information as a manual check of redundant channels. The definition for Channel Check in the existing LGS technical specifications is:

*A CHANNEL CHECK shall be the qualitative assessment of channel behavior during operation by observation. This determination shall include, where possible, comparison of the channel indication and/or status with other indications and/or status derived from independent instrument channels measuring the same parameter.*

For the PPS, the Inter-Channel Comparison application diagnostic is being executed in the MTP instead of the ITP. This change is due the differences in architecture between the AP1000 PMS and the LGS PPS. The AP1000 PMS had an additional subsystem called the Integrated Communications Processor (ICP) which has similar functionality to the ITP. [

] <sup>a,c</sup> The MTP Inter-Channel Comparison Application diagnostic performs the same function described in WCAP-18461-P-A (Reference 54), Sections 2.1.9 and 5.3.1). The MTP will rely on the ITP to acquire the inter-channel data and that data will be provided to the MTP via the AF100 bus for the Inter-Channel Comparison application diagnostic. The alarming described in WCAP-18461-P-A (Reference 54) for comparison deviations is unchanged and sourced from the MTP rather than the ITP. The MTP Inter-Channel Comparison application diagnostic is developed in accordance with the requirements of the Common Q Software Program Manual (Reference 6) for Important to Safety software. This process requires IV&V and traceability of requirements in the same manner as the Inter-Channel Comparison application diagnostic developed for the ITP.

Since the MTP Inter-Channel Comparison Check is configured to alarm when at least one of four BPL measure channels deviate from the others by a configurable value then there is no reason to do a manual Channel Check on these functions. A Division Fault Alarm is generated when this condition occurs. This Division Fault Alarm is sent over the AOI data link for DCS annunciation. Table A.6.1-1 lists the applicable technical specification functions that are impacted by this elimination.

There is an exception to this and that is for contact inputs going through the PPS DI621 module as identified by a Note 1 in Table A.6.1-1. Performing an Inter-Channel Comparison PPS application diagnostic for these contact inputs is obviated by the condition that when one BPL channel contact input changes state an alarm immediately occurs. Thus the Channel Check requirement for the contact inputs identified by Note 1 in Table A.6.1-1 can be eliminated.



**Table A.6.1-1 LGS Channel Check Eliminations**

<b>Table/Function (Existing LGS Technical Specifications)</b>	<b>Description</b>	<b>Instruments Measure Redundant Processes</b>	<b>Function Based on Sensor Value</b>	<b>Can be Eliminated</b>
4.3.1.1-1, Function 1a	IRM Neutron Flux – High	Yes <sup>1</sup>	Yes <sup>1</sup>	Yes <sup>1</sup>
4.3.1.1-1, Function 1b	Inoperative	N/A	N/A	N/A
4.3.1.1-1, Function 2a	APRM Neutron Flux – Upscale (Setdown)	N/A <sup>2</sup>	N/A <sup>2</sup>	N/A <sup>2</sup>
4.3.1.1-1, Function 2b	Simulated Thermal Power - Upscale	N/A <sup>2</sup>	N/A <sup>2</sup>	N/A <sup>2</sup>
4.3.1.1-1, Function 2c	Neutron Flux - Upscale	N/A <sup>2</sup>	N/A <sup>2</sup>	N/A <sup>2</sup>
4.3.1.1-1, Function 2d	Inoperative	N/A	N/A	N/A
4.3.1.1-1, Function 2e	2-Out-Of-4 Voter	Yes <sup>1</sup>	Yes <sup>1</sup>	Yes <sup>1</sup>
4.3.1.1-1, Function 2f	OPRM Upscale	N/A <sup>2</sup>	N/A <sup>2</sup>	N/A <sup>2</sup>
4.3.1.1-1, Function 3	Reactor Vessel Steam Dome Pressure - High	Yes	Yes	Yes
4.3.1.1-1, Function 4	Reactor Vessel Water Level-Low, Level 3	Yes	Yes	Yes
4.3.1.1-1, Function 5	Main Steam Line Isolation Valve - Closure	N/A <sup>1</sup>	N/A <sup>1</sup>	N/A <sup>1</sup>
4.3.1.1-1, Function 6	Deleted from technical specifications	N/A	N/A	N/A
4.3.1.1-1, Function 7	Drywell Pressure - High	Yes	Yes	Yes
4.3.1.1-1, Function 8a	Scram Discharge Volume Water Level - High  Level Transmitter	Yes	Yes	Yes



<b>Table/Function (Existing LGS Technical Specifications)</b>	<b>Description</b>	<b>Instruments Measure Redundant Processes</b>	<b>Function Based on Sensor Value</b>	<b>Can be Eliminated</b>
4.3.1.1-1, Function 8b	Scram Discharge Volume Water Level - High  Float Switch	N/A <sup>1</sup>	N/A <sup>1</sup>	N/A <sup>1</sup>
4.3.1.1-1, Function 9	Turbine Stop Valve - Closure	N/A <sup>1</sup>	N/A <sup>1</sup>	N/A <sup>1</sup>
4.3.1.1-1, Function 10	Turbine Control Valve Fast  Closure, Trip Oil	Yes	Yes	Yes
4.3.1.1-1, Function 10	Turbine Control Valve Fast  Pressure - Low	N/A <sup>1</sup>	N/A <sup>1</sup>	N/A <sup>1</sup>
4.3.1.1-1, Function 11	Reactor Mode Switch Shutdown Position	N/A <sup>1</sup>	N/A <sup>1</sup>	N/A <sup>1</sup>
4.3.1.1-1, Function 12	Manual Scram	N/A	N/A	N/A
4.3.2.1-1, Function 1a	Reactor Vessel Water Level  1) Low, Low, Level 2 1, 2, 3  2) Low, Low, Low - Level 1	Yes	Yes	Yes
4.3.2.1-1, Function 1b	Deleted from technical specifications	N/A	N/A	N/A
4.3.2.1-1, Function 1c	Main Steam Line  Pressure - Low	Yes	Yes	Yes
4.3.2.1-1, Function 1d	Main Steam Line  Flow - High	Yes	Yes	Yes
4.3.2.1-1, Function 1e	Condenser Vacuum - Low	Yes	Yes	Yes
4.3.2.1-1, Function 1f	Outboard MSIV Room	Yes	Yes	Yes



<b>Table/Function (Existing LGS Technical Specifications)</b>	<b>Description</b>	<b>Instruments Measure Redundant Processes</b>	<b>Function Based on Sensor Value</b>	<b>Can be Eliminated</b>
	Temperature – High			
4.3.2.1-1, Function 1g	Turbine Enclosure - Main Steam  Line Tunnel Temperature - High	Yes	Yes	Yes
4.3.2.1-1, Function 1h	Manual Initiation	N/A	N/A	N/A
4.3.2.1-1, Function 2a	Reactor Vessel Water Level  Low - Level 3	Yes	Yes	Yes
4.3.2.1-1, Function 2b	Reactor Vessel (RHR Cut-In 1, 2, 3 Permissive) Pressure - High	Yes	Yes	Yes
4.3.2.1-1, Function 2c	Manual Initiation	N/A	N/A	N/A
4.3.2.1-1, Function 3a	RWCS $\Delta$ Flow - High	Yes <sup>1</sup>	Yes <sup>1</sup>	Yes <sup>1</sup>
4.3.2.1-1, Function 3b	RWCS Area Temperature - High	Yes	Yes	Yes
4.3.2.1-1, Function 3c	RWCS Area Ventilation $\Delta$ Temperature - High	Yes	Yes	Yes
4.3.2.1-1, Function 3d	SLCS Initiation	N/A <sup>1</sup>	N/A <sup>1</sup>	N/A <sup>1</sup>
4.3.2.1-1, Function 3e	Reactor Vessel Water Level  Low, Low, - Level 2	Yes	Yes	Yes
4.3.2.1-1, Function 3f	Manual Initiation	N/A	N/A	N/A
4.3.2.1-1, Function 4a	HPCI Steam Line $\Delta$ Pressure - High	Yes	Yes	Yes



<b>Table/Function (Existing LGS Technical Specifications)</b>	<b>Description</b>	<b>Instruments Measure Redundant Processes</b>	<b>Function Based on Sensor Value</b>	<b>Can be Eliminated</b>
4.3.2.1-1, Function 4b	HPCI Steam Supply Pressure, Low	Yes	Yes	Yes
4.3.2.1-1, Function 4c	HPCI Turbine Exhaust Diaphragm Pressure - High	Yes	Yes	Yes
4.3.2.1-1, Function 4d/e	HPCI Equipment Room Temperature – High $\Delta$ Temperature - High	Yes	Yes	Yes
4.3.2.1-1, Function 4f	HPCI Pipe Routing Area Temperature - High	Yes	Yes	Yes
4.3.2.1-1, Function 4g	Manual Initiation	N/A	N/A	N/A
4.3.2.1-1, Function 4h	HPCI Steam Line $\Delta$ Pressure Timer	N/A	N/A	N/A
4.3.2.1-1, Function 5a	RCIC Steam Line $\Delta$ Pressure - High	Yes	Yes	Yes
4.3.2.1-1, Function 5b	RCIC Steam Supply Pressure - Low	Yes	Yes	Yes
4.3.2.1-1, Function 5c	RCIC Turbine Exhaust Diaphragm Pressure - High	Yes	Yes	Yes
4.3.2.1-1, Function 5d/e	RCIC Equipment Room Temperature – High RCIC Equipment Room $\Delta$ Temperature - High	Yes	Yes	Yes
4.3.2.1-1, Function 5f	RCIC Pipe Routing Area Temperature - High	Yes	Yes	Yes



<b>Table/Function (Existing LGS Technical Specifications)</b>	<b>Description</b>	<b>Instruments Measure Redundant Processes</b>	<b>Function Based on Sensor Value</b>	<b>Can be Eliminated</b>
4.3.2.1-1, Function 5g	Manual Initiation	N/A	N/A	N/A
4.3.2.1-1, Function 5h	RCIC Steam Line $\Delta$ Pressure Timer	N/A	N/A	N/A
4.3.2.1-1, Function 6a	Reactor Vessel Water Level  1) Low, Low - Level 2 1, 2, 3  2) Low, Low, Low - Level 1	Yes	Yes	Yes
4.3.2.1-1, Function 6b	Drywell Pressure - High	Yes	Yes	Yes
4.3.2.1-1, Function 6c	North Stack Effluent Radiation - High	Yes <sup>1</sup>	No <sup>1</sup>	No <sup>1</sup>
4.3.2.1-1, Function 6d	Deleted	N/A	N/A	N/A
4.3.2.1-1, Function 6e	Reactor Enclosure Ventilation Exhaust Duct - Radiation - High	Yes <sup>1</sup>	Yes <sup>1</sup>	Yes <sup>1</sup>
4.3.2.1-1, Function 6f	Deleted	N/A	N/A	N/A
4.3.2.1-1, Function 6g	Deleted	N/A	N/A	N/A
4.3.2.1-1, Function 6h	Drywell Pressure - High/ Reactor Pressure - Low	Yes	Yes	Yes
4.3.2.1-1, Function 6i	Primary Containment Instrument Gas to Drywell $\Delta$ Pressure - Low	N/A	N/A	N/A
4.3.2.1-1, Function 6j	Manual Initiation	N/A	N/A	N/A



<b>Table/Function (Existing LGS Technical Specifications)</b>	<b>Description</b>	<b>Instruments Measure Redundant Processes</b>	<b>Function Based on Sensor Value</b>	<b>Can be Eliminated</b>
4.3.2.1-1, Function 7a	Reactor Vessel Water Level  Low, Low - Level 2	Yes	Yes	Yes
4.3.2.1-1, Function 7b	Drywell Pressure - High	Yes	Yes	Yes
4.3.2.1-1, Function 7c	Refueling Area Unit 1 Ventilation Exhaust Duct Radiation - High  Refueling Area Unit 2 Ventilation Exhaust Duct Radiation - High	Yes <sup>1</sup>	No <sup>1</sup>	No <sup>1</sup>
4.3.2.1-1, Function 7d	Reactor Enclosure Ventilation Exhaust Duct Radiation - High	Yes <sup>1</sup>	Yes <sup>1</sup>	Yes <sup>1</sup>
4.3.2.1-1, Function 7e	Deleted	N/A	N/A	N/A
4.3.2.1-1, Function 7f	Deleted	N/A	N/A	N/A
4.3.2.1-1, Function 7g	Reactor Enclosure Manual Initiation	N/A	N/A	N/A
4.3.2.1-1, Function 7h	Refueling Area Manual Initiation	N/A	N/A	N/A
4.3.3.1-1, Function 1a	Reactor Vessel Water Level -  Low Low Low, Level 1	Yes	Yes	Yes
4.3.3.1-1, Function 1b	Drywell Pressure - High	Yes	Yes	Yes
4.3.3.1-1, Function 1c	Reactor Vessel Pressure - Low	Yes	Yes	Yes
4.3.3.1-1, Function 1d	Manual Initiation	N/A	N/A	N/A



<b>Table/Function (Existing LGS Technical Specifications)</b>	<b>Description</b>	<b>Instruments Measure Redundant Processes</b>	<b>Function Based on Sensor Value</b>	<b>Can be Eliminated</b>
4.3.3.1-1, Function 2a	Reactor Vessel Water Level -  Low Low Low, Level 1	Yes	Yes	Yes
4.3.3.1-1, Function 2b	Drywell Pressure - High	Yes	Yes	Yes
4.3.3.1-1, Function 2c	Reactor Vessel Pressure - Low	Yes	Yes	Yes
4.3.3.1-1, Function 2d	Injection Valve Differential Pressure - Low (Permissive)	Yes	Yes	Yes
4.3.3.1-1, Function 2e	Manual Initiation	N/A	N/A	N/A
4.3.3.1-1, Function 3a	Reactor Vessel Water Level -  Low Low, Level 2	Yes	Yes	Yes
4.3.3.1-1, Function 3b	Drywell Pressure - High	Yes	Yes	Yes
4.3.3.1-1, Function 3c	Condensate Storage Tank Level - Low	Yes	Yes	Yes
4.3.3.1-1, Function 3d	Suppression Pool Water Level - High	Yes	Yes	Yes
4.3.3.1-1, Function 3e	Reactor Vessel Water Level -  High, Level 8	Yes	Yes	Yes
4.3.3.1-1, Function 3f	Manual Initiation	N/A	N/A	N/A
4.3.3.1-1, Function 4a	Reactor Vessel Water Level -  Low Low Low, Level 1	Yes	Yes	Yes
4.3.3.1-1, Function 4b	Drywell Pressure - High	Yes	Yes	Yes



<b>Table/Function (Existing LGS Technical Specifications)</b>	<b>Description</b>	<b>Instruments Measure Redundant Processes</b>	<b>Function Based on Sensor Value</b>	<b>Can be Eliminated</b>
4.3.3.1-1, Function 4c	ADS Timer	N/A	N/A	N/A
4.3.3.1-1, Function 4d	Core Spray Pump Discharge Pressure - High	Yes	Yes	Yes
4.3.3.1-1, Function 4e	RHR LPCI Mode Pump Discharge Pressure - High	Yes	Yes	Yes
4.3.3.1-1, Function 4f	Reactor Vessel Water Level - Low, Level 3	Yes	Yes	Yes
4.3.3.1-1, Function 4g	Manual Initiation	N/A	N/A	N/A
4.3.3.1-1, Function 4h	ADS Drywell Pressure Bypass Timer	N/A	N/A	N/A
4.3.7.5-1, Function 1	Reactor Vessel Pressure	Yes	Yes	Yes
4.3.7.5-1, Function 2	Reactor Vessel Water Level	Yes	Yes	Yes
4.3.7.5-1, Function 3	Suppression Chamber Water Level	Yes	Yes	Yes
4.3.7.5-1, Function 4	Suppression Chamber Water Temperature	Yes	Yes	Yes
4.3.7.5-1, Functions 5, 7 - 10	Deleted	N/A	N/A	N/A
4.3.7.5-1, Function 6	Primary Containment Pressure	Yes	Yes	Yes
4.3.7.5-1, Function 11	Primary Containment Post LOCA Radiation Monitors	Yes <sup>1</sup>	Yes <sup>1</sup>	Yes <sup>1</sup>
4.3.7.5-1, Function 12	North Stack Wide Range Accident Monitor	Yes <sup>1</sup>	Yes <sup>1</sup>	Yes <sup>1</sup>



<b>Table/Function (Existing LGS Technical Specifications)</b>	<b>Description</b>	<b>Instruments Measure Redundant Processes</b>	<b>Function Based on Sensor Value</b>	<b>Can be Eliminated</b>
4.3.7.5-1, Function 13	Neutron Flux	Yes <sup>1</sup>	Yes <sup>1</sup>	Yes <sup>1</sup>

1. These are contact inputs. Those rows with “Yes” across with this note are required in technical specifications to have a channel check. Those with N/A across the row with this note do not require a channel check. Those contact inputs that require a channel check, can be eliminated because when a channel contact input actuates, an immediate alarm will occur. This obviates the needs to monitor these contact inputs as part of channel check.
2. The trip output signals (Neutron Flux Upscale/Simulated Thermal Power - Upscale/APRM Inoperative/OPRM Upscale) from all four APRM channels go to each of the four APRM 2-out-of-4 voters. Each of the APRM 2-out-of-4 Voters provides an input to one PPS channel (APRM 2oo4 Voter 1 to PPS channel A, APRM 2oo4 Voter 2 to PPS channel B, APRM 2oo4 Voter 3 to PPS channel C and APRM 2oo4 Voter 4 to PPS channel D).

### Channel Check Summary

Table A.6.1-1 indicates the channel check SRs that can be eliminated for the PPS functions listed.

### A.6.2 PPS Channel Functional Test/Logic System Functional Test SR Elimination

The RPS, ECCS, and NSSSS Channel Functional Test according to the LGS technical specifications is:

*1.6 A CHANNEL FUNCTIONAL TEST shall be:*

*a. Analog channels - the injection of a simulated signal into the channel as close to the sensor as practicable to verify OPERABILITY of all devices in the channel required for channel OPERABILITY.*

*b. Bistable channels - the injection of a simulated signal into the sensor to verify OPERABILITY of all devices in the channel required for OPERABILITY.*

*The CHANNEL FUNCTIONAL TEST may be performed by any series of sequential, overlapping or total channel steps and each step must be performed within the Frequency in the Surveillance Frequency Control Program for the devices included in the step.*

The PPS integrates the logic functions for the RPS, ECCS and NSSSS. These existing logic functions are analog, so definition a) applies. The Logic System Functional Test in the existing LGS Technical Specifications is defined as:

*1.20 A LOGIC SYSTEM FUNCTIONAL TEST shall be a test of all logic components required for OPERABILITY of a logic circuit, from as close to the sensor as practical up to, but not including the*



*actuated device, to verify OPERABILITY. The LOGIC SYSTEM FUNCTIONAL TEST may be performed by any series of sequential, overlapping or total system steps such that the entire logic system is tested.*

These tests are required in TS 4.3.1.2 for RPS, 4.3.2.2 for Isolation Functions (i.e., NSSSS), and 4.3.3.2 for ECCS in the existing LGS Technical Specifications. This analysis will demonstrate that the PPS self-diagnostics have sufficient coverage to replace the Channel Functional Test listed in LGS Technical Specifications Tables 4.3.1.1-1, 4.3.2.1-1, 4.3.3.1-1 and Logic System Functional Test for RPS, NSSSS, and ECCS for the PPS, with discreet equipment operability tests not covered by the self-diagnostics.

As described in Section 3.2, there are three levels of the PPS architecture that must be addressed for SRs. WCAP-18461-P-A (Reference 54) goes through these levels of architecture explaining how the diagnostics provide coverage for the Westinghouse definitions for Channel Operational Test and Actuation Logic Test. Since the architectures between the LGS PPS and the architecture used in WCAP-18461-P-A (Reference 54) are so similar, only the differences will be discussed in this appendix.

#### **A.6.2.1 Channel Functional Test**

*The CHANNEL FUNCTIONAL TEST may be performed by any series of sequential, overlapping or total channel steps and each step must be performed within the Frequency in the Surveillance Frequency Control Program for the devices included in the step.*

The LGS Channel Functional Test is the SR for the Level 1 (BPL) and Level 2 (LCL) of the LGS PPS architecture. The existing LGS Technical Specification Tables 4.3.1.1-1, 4.3.2.1-1, 4.3.3.1-1 identify the RPS, NSSSS, and ECCS functions that require a Channel Functional Test. Note: in some cases the NSSSS bistable function is determined in the ILP to accommodate the location of the terminated signals (see Section 3.2.4).

The Westinghouse Channel Operational Test described in WCAP-18461-P-A (Reference 54) is the equivalent test to the LGS Technical Specifications Channel Functional Test.

As described in Section A.1.4 the only differences in architecture between the LGS PPS and the architecture in WCAP-18461-P-A (Reference 54) for the BPL is a third PM646A processor module to process RG 1.97 variables, and the absence of the AO650 module in the BPL. The PAMS variables do not require a Channel Functional Test, only a Channel Check and Channel Calibration. Channel Check of these variables is included in Section A.6.1. Channel Calibration is redefined by the LAR changes to the technical specifications and will still be required to be performed.

The analysis in WCAP-18461-P-A (Reference 54) examines the simulated test path for the Channel Functional Test (aka Westinghouse Channel Operational Test) and lists the equipment involved. Figure 7.1-1 in WCAP-18461-P-A (Reference 54) shows the BPL signal path. This figure directly applies to the LGS BPL signal path. Section 7.1.2 lists the PPS modules involved in the Westinghouse Channel Operational Test. The same PPS equipment is involved for the safety signal path for all these functions [

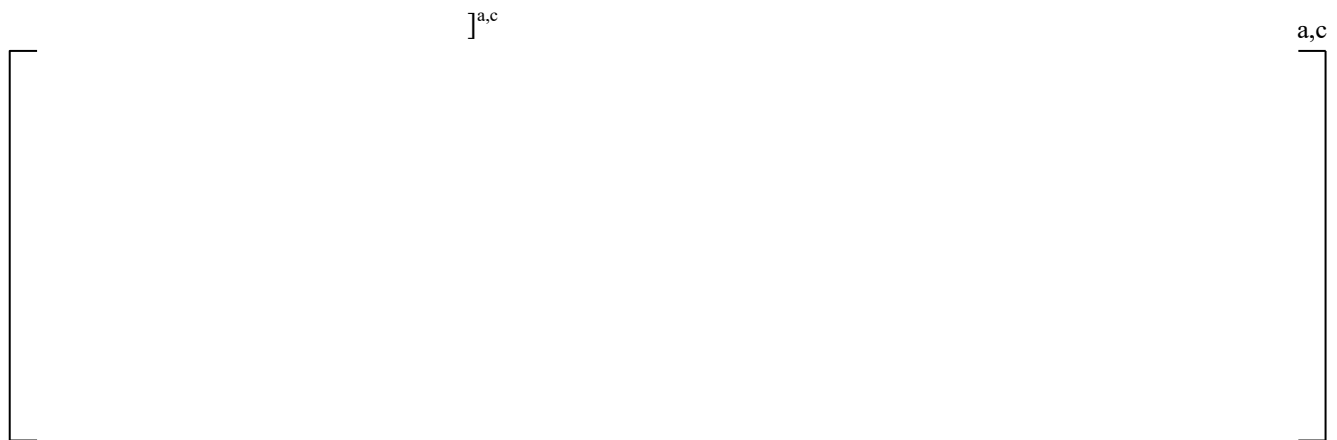
] <sup>a,c</sup>



Section 3.4.1 describes the configurations for two cases for reactor trip functions with response times  $\leq 124\text{ms}$ . The first configuration is for those reactor trip functions with response times  $\leq 50\text{ms}$ . In those cases, the BPL does not process input data for the fast reactor trip functions. As shown in Figure 3.4-1, the contact input is wired directly into the LCL digital input module and processed by the LCL PM646A processor module for coincidence voting.

The second configuration is for those reactor trip functions with response times  $> 50\text{ms}$  and  $\leq 124\text{ms}$ . In those cases, the HSL is not used as the communication between the BPLs and the LCLs, but rather the BPL PM646A processor module sends the trip signals to the LCL via a hardwired connection from the BPL digital output module to the LCL digital input module. This is done to eliminate the delays associated with the HSL communication. What is lost is the self-diagnostics that come with the HSL communication.

[



**Figure A.6.2-1 RPS Scram Matrix WWDT Configuration**

As noted earlier, there are analog and contact inputs that come directly into the ILP that are compared to a setpoint (in the case of the analog signals) that can initiate an isolation function. Similar to the BPL, the analog inputs into the ILP and the ILP processing of these inputs is covered by the same diagnostics that are analyzed for the BPL. [



Therefore periodic operability tests are required for the digital input channels that initiate an isolation function.

### ***Channel Functional Test Elimination Conclusion and Additional Considerations***

Based on the analysis of WCAP-18461-P-A (Reference 54) as augmented in this section, the general requirement for PPS Channel Functional Test can be replaced with specific SRs to verify operability of the following equipment in the PPS safety function actuation path: 1) DI621s, 2) DO620s, and 3) RPS TU.

The reliability of the DI621, DO620, and the RPS TU are as follows (per Reference 42):

[

]<sup>a,c</sup>

These failure rates represent less than one failure per every 24 months. The test frequency for these PPS manual SRs can be every 24 months, based on this data.

### **Manual System Level Actuations**

The TS require a Channel Functional Test for the following system level Manual Initiation Functions:

- Manual Scram
- Main Steam Line Isolation
- RHR System Shutdown Cooling Mode Isolation
- Reactor Water Cleanup System Isolation
- High Pressure Coolant Injection System Isolation
- Reactor Core Isolation Cooling System Isolation
- Primary Containment Isolation
- Reactor Enclosure Isolation
- Refueling Area Isolation
- Core Spray System
- Low Pressure Coolant Injection Mode of RHR System
- High Pressure Coolant Injection System
- Automatic Depressurization System

The TS markups for the LAR eliminate the system level manual actuations because they are not credited in the Chapter 15 safety analysis to mitigate an AOO or Postulated Accident. The LAR will explain how these system level manual actuations do not meet the four criteria in 10 CFR 50.36 to require a surveillance.

There is no need to manually verify the setpoints/addressable constants within the PPS due to the application software addressable constant verification described in Section 3.2.12.3 which is the same approach described in WCAP-18461-P-A (Reference 54), Section 5.3.2.



### A.6.2.2 Logic System Functional Test

*A LOGIC SYSTEM FUNCTIONAL TEST shall be a test of all logic components required for OPERABILITY of a logic circuit, from as close to the sensor as practical up to, but not including the actuated device, to verify OPERABILITY. The LOGIC SYSTEM FUNCTIONAL TEST may be performed by any series of sequential, overlapping or total system steps such that the entire logic system is tested.*

WCAP-18461-P-A (Reference 54) describes the Westinghouse Actuation Logic Test and the Actuation Logic Output Test. The scope of these tests is equivalent to the LGS Technical Specification Logic System Functional Test. LGS existing Technical Specifications Sections 4.3.1.2 (RPS), 4.3.2.2 (Isolation Actuation [NSSSS]), and 4.3.3.2 (ECCS) specify the functions that require a Logic System Functional Test. The same PPS equipment is involved for the safety signal path for all these functions (except the fast reactor trip functions as described in Section A.6.2.1).

The analysis in WCAP-18461-P-A (Reference 54) examines the simulated test path for both these Westinghouse tests that are equivalent to the LGS Logic System Functional and depicts the PPS modules involved (see Figures 7.1-2 and 7.1-3 in WCAP-18461-P-A).

The differences in LGS PPS and WCAP-18461-P-A architecture are described in Section A.1.4. The major difference in the two architectures is the introduction of the RPS TU and HARP interfaces (see Sections 3.5.6 and 3.5.9), and the AO650 in the ILPs (see Section 3.2.4). For RPS logic functional test is discussed in Section A.6.2.1.

For ECCS and NSSS, the CIM analysis in Section 7.1.4 of WCAP-18461-P-A (Reference 54) describes three CIM configurations [

] <sup>a,c</sup> The CIM uses an interposing HARP for the interface to the actuating components. The CIM Analysis in WCAP-18461-P-A (Reference 54) also describes the CIM providing power to the actuating device. For the LGS PPS the power for actuating devices is provided by plant power. [

] <sup>a,c</sup>

As described in Section 3.2.4, some input signals are terminated at the ILP cabinet and can generate an asset protection actuation function. Since these are asset protection functions and not plant protection functions, they are not included in this analysis.

The ILP has multiple DO620 Digital Output Modules for those actuating equipment interfaces that do not require a CIM for multiple access to the component. For those DO620 output channels that initiate a protective actuation function, a periodic operability test of these DO620 output channels is required.

The ILP uses the AO650 for HPCI and RCIC flow control. WCAP-18461-P-A (Reference 54) does not include a FMEDA table for the AO650 or its TU. Therefore, the AO650 analog output channels used for HPCI and RCIC flow control will require periodic surveillance for these outputs.

As a result of the analysis, the CIM output through the HARP, the DO620 output channels that initiate a protective actuation, and the AO650 analog output channels used for HPCI and RCIC flow control need



to be periodically tested for operability. The reliability and testing frequency for the DO620 is discussed in Section A.6.2.1. The reliability (unavailability) of the HARP is  $8\text{E-}05$  based on the PPS reliability analysis (Reference 42). The reliability of the AO650 is  $3.577\text{E-}06$  failure per hour (Reference 71). Based on these reliability figured, the test frequency can be 24 months.

### **A.6.3 PPS Response Time SR Elimination**

The foundation for the Response Time SR elimination analysis examines only failures that can cause a response time delay, since operability of the PPS safety signal path has been considered in Sections A.6.1 and A.6.2. These failures are those that will either effect the cycle time of the PM646A processor module application program (CONTRM) or hardware failures that result in response time delays. Therefore, to eliminate Response Time SRs, it must be demonstrated that both the CONTRM cycle time and hardware are covered by diagnostics. The scope of this analysis is the PPS response time from PPS input signal termination to PPS RPS TU output for RPS, and the HARP for NSSSS and ECCS.

The AO650 in the ILP is used for HPCI and RCIC flow control. Since WCAP-18461-P-A (Reference 54) does not evaluate the diagnostic coverage of the AO650, it cannot be excluded in the context of response time. In the case of HPCI flow control, a response time periodic surveillance of the AO650 outputs performing that function is required. It can be combined with other response time surveillance tests to verify the AO650 response time. In the case of RCIC flow control, there is no response time requirement and therefore these AO650 outputs for RCIC flow control do not need a SR for response time.

#### **A.6.3.1 Methodology**

Since the architectures between the PPS and that described in WCAP-18461-P-A (Reference 54) are similar, the methodology described in WCAP-18461-P-A (Reference 54) can be applied. For PPS RPS the response time signal path is shown in Figure A.6.3.1-1. For ECCS and NSSS, the same BPL signal path will be taken through the LCL, however, instead of hardwired outputs to the RPS Scram Matrix, the safety path signal continues through the HSL to the ILPs as shown in Figure A.6.3.1-2.

For the fast reactor trip configurations and their safety signal paths, refer to Figures 3.4-1 and 3.4-2.



a,c

**Figure A.6.3.1-1 PPS RPS Signal Path**



**Figure A.6.3.1-2 ECCS/NSSSS Signal Path**

Note that the ECCS/NSSSS response time signal path includes the HARP (not shown connected to the CIM – see Section 3.5.9), that is an interposing relay panel using solid state relays.<sup>268</sup>

As stated in WCAP-18461-P-A (Reference 54), the methodology used to eliminate RTT is as follows:

1. Determine all Response Time test paths.
2. Once all paths are determined, the scope of the components that make up the functional paths for response time testing can be determined.
3. Analyze the components identified in Step 1 for potential failures that could generate delays in response time. For identified failures, identify diagnostics to be credited to ensure the response time will not degrade. This is done by analyzing the components in three groups:
  - a. Input Modules
  - b. Processing and Communication Components
  - c. Output Modules



### A.6.3.2 Response Time Paths

As shown in Figures A.6.3.1-1 and A.6.3.1-2, the PPS modules involved for RPS/NSSSS/ECCS functions are the same modules listed in WCAP-18461-P-A (Reference 54) Table 7.3-1 except for the RPS TU and HARP.

**Table A.6.3.2-1 PPS RPS Safety Signal Path Modules**

Type of Component	PPS Rack Components within SR Paths
Input Modules	- AI687 - AI688 - DI621
Processing/Communication	- PM646A - BIOB - CI631 - HSL
Output Modules	- DO620 - Safety Remote Node Controller (SRNC) - Component Interface Module (CIM) - RPS TU <sup>1</sup>

Note:

1. The RPS TU is an interposing relay termination unit and is part of the PPS portion of the RPS trip paths, thus included in this analysis.

### A.6.3.3 Module Analyses

The modules listed in Table A.6.3.2-1 are evaluated in WCAP-18461-P-A (Reference 54), Section 7.3.2, except for the RPS TU and for the CIM.

The RPS TU and the HARP are included in the PPS response time paths due to the interface they provide for the PPS RPS functions (see Section 3.5.6) and for ECCS/NSSSS actuations (see Section 3.5.9) respectively. Since the RPS TU and HARP contain no software or electro-mechanical components (for these specific paths), they have been screened out from contributing to response time degradation, as long as operability can be surveilled.<sup>269</sup>

The analysis in WCAP-18461-P-A (Reference 54) concludes that all the modules in the safety signal path in the architecture have diagnostics to detect a degradation in response time, a manual response time test of the architect is not required, so long as those components without diagnostics (e.g., DI621, DO620, RPS TU, and HARP) are periodically surveilled for operability. Based on the analysis of the similarities between the architecture in WCAP-18461-P-A (Reference 54) and the LGS PPS architecture, the same conclusion can be made.



## A.7 SUMMARY

The evaluations for PPS Channel Check, Channel Functional Test, and Logic System Functional test show that some surveillances can be replaced with specific SRs for targeted portions of the LGS PPS architecture. This is summarized as follows:

1. **Channel Check** - All PPS manual Channel Check SRs can be eliminated except as noted below:

TABLE 4.3.1.1-1, "REACTOR PROTECTION SYSTEM INSTRUMENTATION SURVEILLANCE REQUIREMENTS", Functional Units 1 – 2 are not within the domain of the PPS.

All current channel checks for variables can be eliminated as described in Section A.6.1.

2. **Channel Functional Test of the PPS** – The Channel Functional Test can be replaced for Tables 4.3.1.1-1, 4.3.2.1-1, 4.3.3.1-1 and Section 4.3.4.2.1 in the existing LGS Technical Specifications with a PPS SR covering the 1) DI621 input channels processing signals for a protective action signal, 2) DO620 out channels initiating reactor trip signals, and 3) RPS TU.

These tests can be performed utilizing the RPS TU feedback signals to the ITP or in combination with other surveillance tests for other systems. Based on the PPS reliability analysis (Reference 42), these components only need a surveillance test every 24 months.

3. **Logic System Functional Test** – The Logic System Functional Test can be replaced for SRs 4.3.1.2 (RPS), 4.3.2.2 (Isolation Actuation [NSSSS]), and 4.3.3.2 (ECCS) with a PPS SR covering the following:
  - DO620 output channels initiating a protective actuation at the ILP
  - AO650 output channels used for HPCI and RCIC flow control
  - The CIM output through the HARP to the actuating component. The CIM/HARP interface provides component feedback to the command response.

These surveillances can be performed utilizing the actuating component feedback signals or in combination with other surveillance tests for other systems. Based on the discussion in Section A.6.2.2, these components only need a surveillance test every 24 months..

4. **Response Time Testing** – PPS Response Time Testing can be eliminated from Tables 3.3.1.-2, 3.3.2-3, 3.3.3-3 and Section 4.3.4.2.3, and use only allocated times for the digital PPS portion of the Response Time SR for RPS, NSSSS, and ECCS. The one exception is HPCI flow control using the AC650. A response time surveillance is required for these AO650 outputs. This surveillance can be performed in combination with other surveillance tests.

The TS markups attached to the LAR remove the surveillance requirements for the system level manual actuations. This is because the LGS Chapter 15 Safety Analysis does not credit manual system level actuations to mitigate AOOs and Postulated Accidents. The justification for this is based on the four criteria in 10 CFR 50.36 and is explained as part of the TS markups in the LAR.



## A.8 LICENSEE REQUIRED ACTIONS

WCAP-18461-P-A (Reference 54) lists 8 Licensee Required Actions to be addressed when applying the topical report. This section provides dispositions for each Licensee Required Action as it applies to the PPS.

- A.8.1 LRA\_1** - Identification of where the licensee's plant-specific architecture deviates from the architecture described within Appendix A of this topical report, along with an analysis of the contrast between the two (e.g., an alternative to the ITP functions listed in this topical report if the licensee's architecture does not include an ITP).

Section A.1.4 identifies the differences between the PPS architecture and the architecture described in Appendix A within WCAP-18461-P-A (Reference 54). The PPS architecture includes an ITP.

- A.8.2 LRA\_2** - The licensee will have to compare the plant-specific application FMEA with the failure modes identified in the FMEDA tables within this analysis. This should be done to conclude that the FMEA herein is bounded by the plant-specific application FMEA.

Section A.6 describes the differences between the PPS FMEA and the FMEA in WCAP-18461-P-A (Reference 54). Those differences are then demonstrated to be covered by the FMEDA tables in WCAP-18461-P-A (Reference 54).

- A.8.3 LRA\_3** – Identification of licensee's plant-specific functions that deviate from those within the applicable standard technical specifications (NUREG-1431/NUREG-1432) will need to be analyzed to remove the applicable SRs. The analysis/methodology in this topical report provides a framework for this task. Additionally, the licensee needs to ensure that the assumptions made regarding the TS in Appendix B.2 are met in the current licensing basis, otherwise necessary changes will need to be implemented.

The LGS technical specifications are different than the standard NUREG-1431/NUREG-1432 technical specifications used in WCAP-18461-P-A (Reference 54). Therefore, the assumptions listed in the topical report are not applicable to this analysis. The analysis in Section A.6 compares the LGS SRs and the PPS equipment in the safety path for the safety functions listed in technical specification Tables 3.3.1-2, 4.3.1.1-1, 3.3.2-3, 4.3.2.1-1, 3.3.3-3, 4.3.3.1-1, and 4.3.7.5-1 to identify the SRs that can be eliminated and which SRs must remain as summarized in Section A.7.

- A.8.4 LRA\_4** – For SRs involving the CIM (i.e., ALOT and Trip Logic Tests), where the CIM output continuity test is disabled or suppressed, the licensee needs to ensure the downstream actuation device is periodically exercised by the CIM (e.g., valve stroke SR initiated with the CIM). Additional assurance for the remaining SRs involving the CIM is provided by ensuring all remaining downstream devices are periodically exercised by the CIM.

The LGS technical specifications identify Logic System Functional Tests. The scope of these tests is analyzed and the Summary in Section A.7 identifies the need for a manual surveillance of



the CIM output through the HARP to the actuating component. The CIM/HARP interface provides component feedback to the command response. This SR is dependent on the actuating component feedback, so the test frequency should be the same as that for the actuating component.

- A.8.5 LRA\_5** – The licensee will have to ensure that alarm response procedures for the safety system are adequate for plant operators to respond to a failure identified by the safety system self-diagnostics.

Constellation will be writing a new Alarm Response Procedure using their Alarm Response Procedure Preparation document AD-LG-101-1005 (Reference 23). Section 4.1.1 of that document requires the preparer of the Alarm Response Card to include the following attributes for the new PPS Alarm Response for a PPS Fault Alarm:

1. The meaning and significance of an alarm.
2. The automatic actuation associated with that alarm. (Note: There is no automatic actuation associated with A PPS Fault Alarm)
3. The appropriate operational actions to the alarm.
4. The causes associated with the alarm.
5. The setpoint associated with the alarm. (Note: There is no setpoint associated with A PPS Fault Alarm)

- A.8.6 LRA\_6** – When applying this WCAP, the licensee needs to document that any existing interdependencies between surveillance requirements that may be impacted by the elimination of an SR is addressed in the technical specification bases.

The following cases in which potential TS interdependencies between SRs by the elimination of PPS SRs are:

1. The TS markups create a new definition, Sensor Channel Calibration, specifically for the PPS, to disconnect the Channel Functional Test requirement in the definition for Channel Calibration, since the PPS self-diagnostics eliminate the need for this SR. The sensor inputs to the PPS will need a Sensor Channel Calibration SR.
2. Current TS allow certain sensors to be excluded from response time testing. Referring to the BWR Owners' Group Analysis (Reference 33), credit for existing TS surveillance tests that verify sensor functionality is one of the bases for allowing this exclusion. Reference 33, Section 6, identifies all the TS surveillance test types ("calibrations, functional testing, logic system functional testing and channel checks") and concludes that, "Response time degradation is more likely to be detected during calibrations, functional tests, or channel checks which are performed at the same or more frequent surveillance intervals (18 months, quarterly or monthly, and once/shift respectively) than RTTs."

Although Channel Check, Channel Functional Testing, and Logic System Functional Testing are being eliminated by PPS self-diagnostics, the PPS application diagnostic Channel Comparison performs the same automatic function as the manual Channel Check. This PPS



application diagnostic can detect sensor malfunction by comparing sensors across four channels and annunciating when a channel sensor is deviating.

As stated in #1, a new Sensor Channel Calibration definition is added specifically for the PPS. This test shall:

*be the adjustment, as necessary, of the sensor output such that it responds with the necessary range and accuracy to known values of the parameter which the channel monitors. Sensor contact inputs shall be verified to provide the appropriate signal. Calibration of sensor channels with resistance temperature detector (RTD) or thermocouple sensors may consist of an in-place qualitative assessment of sensor behavior and normal calibration of the remaining adjustable devices in the channel. Neutron detectors may be excluded from SENSOR CHANNEL CALIBRATION. The SENSOR CHANNEL CALIBRATION may be performed by any series of sequential, overlapping, or total channel steps such that the entire sensor channel is calibrated, and each step must be performed within the Frequency in the Surveillance Frequency Control Program for the devices included in the step.*

The definition excludes neutron detectors from Sensor Calibration. According to Reference 33:

*Note 1 states that neutron detectors are excluded from CHANNEL CALIBRATION because they are passive devices, with minimal drift, and because of the difficulty of simulating a meaningful signal. Changes in neutron detector sensitivity are compensated for by performing the 7 day calorimetric calibration (SR 3.3.1.1.2) and the 1000 MWD/T LPRM calibration against the TIPs (SR 3.3.1.1.8).*

The equivalent SR 3.3.1.1.2 in the LGS TS is Note (d) in the existing TS Table 4.3.1.1-1 that will be maintained in the revised TS. The equivalent SR 3.3.1.1.8 in the LGS TS is Note (f) in the same existing TS Table 4.3.1.1-1.

The application diagnostic, Channel Comparison, and the new Sensor Channel Calibration provide sufficient verification of the operability of the sensors currently eliminated from response time testing.

- A.8.7 LRA\_7** – When applying this WCAP, if the licensee’s safety system architecture does not consist of an ITP, the licensee will need to provide a description of how failures identified by self-diagnostics will be reported to plant operators.

The PPS architecture includes an ITP, so the failures identified by self-diagnostics are reported to the plant operators in the same manner as described in WCAP-18461-P-A (Reference 54).

- A.8.8 LRA\_8** – The licensee will provide a description of plant administrative controls that will provide assurance that faults are captured and investigated. This may include items such as operator rounds, and system engineer monthly reports that evaluate and document the health, errors, and



faults of the safety system. In doing so, the anticipated actions in Section 5.4 of this WCAP will be met.

The following plant administrative controls will be in place to assure that the PPS self-diagnostics are being captured. These plant administrative controls include:

1. Conduct of Operations– During routine operator rounds and MCR activities, the following tasks are performed by operators:
  - Panel monitoring to include identification of abnormal system indications
  - MCR annunciator response procedures

Plant activities and alarms are logged in accordance with plant procedures, which are continuously maintained and retrievable. Abnormalities identified are captured in Issue Reports, which are periodically trended by engineering.

2. System Health Checks – Engineering performs routine assessment of the material condition health of the plant equipment and identifies issues that impact or could impact its functional reliability in accordance with company procedures. The Corrective Action Program is used to improve system health and the overall plant performance, safety, and reliability. PPS is defined as a critical system which requires periodic system health monitoring and walk-down of the system. The PPS checks include the following:
  - Failure trending of sub-components based on Issue Report reviews
  - Performance Monitoring Trends – input instrument drift and recalibration frequency
  - Review of PPS Event log for health status, alarms, faults
  - Review of Operations logs
  - Walk-downs of the PPS system

Periodic activities are performed commensurate with system safety significance.

Documentation and trending of system health is procedurally governed to include issue analysis and both short and long range planning and response.

## **A.9 APPLICATION SPECIFIC ACTION ITEMS**

In addition to the Licensee Required Actions in WCAP-18461-P-A (Reference 54), the NRC Safety Evaluation Report includes Application Specific Action Items that must be addressed by each licensee applying WCAP-18461-P-A. This section provides the dispositions for each Application Specific Action Item.

### **A.9.1 ASAI 1**

ASAI 1 states, “The current CIM output solid-state relays are designed to only interface with DC components. If the CIM system is required to interface with AC powered components for a specific application, then a modified version of the current CIM design with different solid-state relays capable of handling the AC loads, which is still under development, needs to be used. A licensee referencing this topical report should perform additional assessment of the modified CIM design to make sure that the findings related to the CIM self-diagnostic functions in this SE are still applicable.”



The CIM design does not need to be modified to interface with the LGS AC loads. As described in Section 3.5.9.1, a High Amperage Relay Panel (HARP) provides the interface between the CIM and the LGS actuating components. This interposing relay panel is included in the analysis in Section A.6.2.2 that identifies the necessary SR for this interface.

### **A.9.2 ASAI 2**

ASAI 2 states, “For specific application cases which use CIMs in series, for interfacing with components with power lock-out requirements, or with intentionally disabled output tests, a licensee referencing this topical report should ensure that the surveillance detect relevant failures which are not covered by the CIM output test self-diagnostic functions.”

As explained in the CIM analysis in Section A.6.2.2, these CIM configurations are not used in the LGS PPS. With the introduction of the HARP, a PPS SR is required to verify the operation of the CIM/HARP interface to actuating components.

### **A.9.3 ASAI 3**

ASAI 3 states, “A licensee referencing this topical report should perform an assessment of all plant specific self-diagnostic functions to be credited for SR elimination to determine if they satisfy applicable operability verification criteria.”

All the self-diagnostic functions used in the PPS are described in WCAP-18461 (Reference 54) except for the [ ]<sup>a,c</sup> application diagnostic (see Section A.4).

### **A.9.4 ASAI 4**

ASAI 4 states, “When performing a comparison of application FMEA with the FMEDA tables in WCAP-18461, the following actions should be performed:

1. Identify any failure modes that are plant specific (i.e., not identified in the WCAP-18461 FMEDA tables) and perform an analysis of system self-diagnostic features to determine if each failure mode is detectable by an existing function or if a new plant application diagnostic function is required.
2. Review all application self-diagnostic functions identified in the FMEA and FMEDA tables and verify that each function is either included in the system design or is identified as a system application requirement to be developed and implemented in the system design.
3. Identify any components or subsystems in the WCAP-18461 FMEDA tables that are not being implemented in the plant design or are being implemented in the plant specific design in a manner different than described in Section 2.1, “Base Architecture,” of the WCAP-18461.
4. Each of the functions performed by these components or sub-systems should then be analyzed to determine the effects of any reduced diagnostic coverage.”

Responses:



1. The failure modes that are plant specific (i.e., not identified in the WCAP-18461 FMEDA tables) are identified and analyzed, to determine if each failure mode is detectable by an existing function or if a new plant application diagnostic function is required, in Section A.6.
2. The application diagnostics that will be implemented in the LGS PPS and their respective requirements numbers in either the PPS System Requirements Specification (Reference 2) or the PPS System Design Specification (Reference 21) are specified in Section A.4.
3. WCAP-18461-P-A (Reference 54) describes an integrated PPS that includes a PAMS and a Diesel Load Sequencer function. There is also an architecture for a Core Protection Calculator System. Not all components in the FMEDA tables are used in the PPS, however the components used for the LGS PPS are in the FMEDA tables (Section 6 of WCAP-18461-P-A, Reference 54). Section A.1.4 describes the architectural differences between the LGS PPS and the PPS architecture in WCAP-18461-P-A (Reference 54).

The LCL/BPL DI621 and DO620 modules are used differently than described in WCAP-18461-P-A (Reference 54). This is explained in Sections 3.4.1 and A.6.2.1. As a result, specific SRs are identified.

4. The FMEA analysis in Section A.6 demonstrates that the diagnostic coverage of these components in the FMEDAs in WCAP-18461-P-A (Reference 54), Section 6 address the FMEA failure modes.



## APPENDIX B

## ENDNOTES

---

<sup>1</sup> LGS UFSAR, Section 1.2.4.2.1

<sup>2</sup> Plant Protection System (PPS) Performance Specification, Section 3.1.1

<sup>3</sup> Plant Protection System (PPS) Performance Specification, Section 4.2

<sup>4</sup> LGS UFSAR Figure 7.2-2

<sup>5</sup> GE BWR/4 Technology Manual Chapter 4.4.1

<sup>6</sup> Plant Protection System (PPS) Performance Specification, Section 3.1.2

<sup>7</sup> LGS UFSAR Chapter 7.1.2.1.3

<sup>8</sup> LGS UFSAR Chapter 7.3.1.1.1

<sup>9</sup> LGS UFSAR Chapter 8.3.1.1.3.6

<sup>10</sup> LGS UFSAR Chapter 7.6.1.8.3

<sup>11</sup> LGS UFSAR Chapter 7.6.1.8.3.1

<sup>12</sup> LGS UFSAR Chapter 7.6.1.8.3.2

<sup>13</sup> LGS UFSAR Chapter 7.6.1.8.3.3

<sup>14</sup> LGS UFSAR Chapter 7.6.1.8.3.4

<sup>15</sup> Plant Protection System (PPS) Performance Specification, Section 3.1.3

<sup>16</sup> LGS UFSAR Chapter 7.4.1.2.3.1

<sup>17</sup> LGS UFSAR Chapter 7.4.1.2.3.2

<sup>18</sup> LGS UFSAR Chapter 7.4.1.2.3.3

<sup>19</sup> LGS UFSAR Chapter 7.4.1.2.3.5

<sup>20</sup> LGS UFSAR Figure 7.1-1

<sup>21</sup> LGS UFSAR Figure 7.2-4

<sup>22</sup> LGS UFSAR Figure 7.2-5

<sup>23</sup> LGS UFSAR Chapter 7.2.1.1.4.1

<sup>24</sup> LGS UFSAR Chapter 7.2.2.1.1.1.7

<sup>25</sup> LGS UFSAR Chapter 7.2.1.1.4.1

<sup>26</sup> LGS UFSAR Chapter 7.2.1.1.4.1

<sup>27</sup> LGS UFSAR Chapter 7.2.1.1.4.3

<sup>28</sup> LGS UFSAR Chapter 7.2.1.1.4.1

<sup>29</sup> LGS UFSAR Chapter 7.2.1.1.4.3

<sup>30</sup> LGS UFSAR Chapter 7.2.1.1.4.4

<sup>31</sup> Automatic reactor trip upon receipt of a high-high radiation signal from the Main Steam Line Radiation Monitoring System was removed as the result of an analysis performed by General Electric in NEDO-31400A. The NRC approved the results of this analysis as documented in the SER (letter to George J. Beck, BWR Owner's Group from A.C. Thadani, NRC, dated May 15, 1991).

<sup>32</sup> LGS UFSAR Chapter 7.2.1.1.4.5

<sup>33</sup> LGS UFSAR Chapter 7.6.1.4.5.1.1.1

<sup>34</sup> LGS UFSAR Chapter 7.2.2.1.1.1.7

<sup>35</sup> LGS UFSAR Chapter 7.2.1.1.4.9

<sup>36</sup> LGS UFSAR Chapter 7.2.1.1.4.9

<sup>37</sup> LGS UFSAR Chapter 7.2.1.1.6.1.2

<sup>38</sup> LGS UFSAR Chapter 7.2.1.1.8

<sup>39</sup> LGS UFSAR Chapter 7.2.1.1.6.2.1

<sup>40</sup> GE BWR/4 Technology Manual Chapter 4.4.1

<sup>41</sup> GE BWR/4 Technology Manual Chapter 4.4.2.2

<sup>42</sup> LGS UFSAR Chapter 7.1.2.1.2.1

<sup>43</sup> GE BWR/4 Technology Manual Chapter 4.4.2.3

<sup>44</sup> GE BWR/4 Technology Manual Chapter 4.4.3.1



- 
- 45 GE BWR/4 Technology Manual Chapter 4.4.3.3
  - 46 LGS UFSAR Chapter 7.3.1.1.2.1
  - 47 LGS UFSAR Chapter 7.3.1.1.2.3
  - 48 LGS UFSAR Figure 7.3-26
  - 49 GE BWR/4 Technology Manual Chapter 10.4.3.3.2
  - 50 LGS UFSAR Chapter 7.3.1.1.2.4.3
  - 51 LGS UFSAR Chapter 7.6.1.3.3.2.2.1
  - 52 LGS UFSAR Chapter 7.6.1.3.3.2.2.4
  - 53 LGS UFSAR Chapter 7.3.1.1.2.4.4
  - 54 LGS UFSAR Chapter 7.6.1.3.3.2.3.3
  - 55 LGS UFSAR Chapter 7.6.1.3.3.2.3.4
  - 56 LGS UFSAR Chapter 7.3.1.1.2.4.5.1
  - 57 LGS UFSAR Chapter 7.3.1.1.2.4.5.3
  - 58 LGS UFSAR Chapter 7.3.1.1.2.4.5.4
  - 59 LGS UFSAR Chapter 7.3.1.1.2.4.5.6
  - 60 LGS UFSAR Chapter 7.3.1.1.2.4.6.1
  - 61 LGS UFSAR Chapter 7.3.1.1.2.4.6.3
  - 62 LGS UFSAR Chapter 7.3.1.1.2.4.6.4
  - 63 LGS UFSAR Chapter 7.1.2.1.11.2
  - 64 LGS UFSAR Chapter 7.3.1.1.2.4.7
  - 65 LGS UFSAR Chapter 7.1.2.1.11.3.1
  - 66 LGS UFSAR Chapter 7.3.1.1.2.4.8
  - 67 LGS UFSAR Chapter 7.3.1.1.2.4.9
  - 68 LGS UFSAR Chapter 7.6.1.3.3.4.2.1
  - 69 LGS UFSAR Chapter 7.6.1.3.3.4.2.2
  - 70 LGS UFSAR Chapter 7.3.1.1.2.4.10
  - 71 LGS UFSAR Chapter 7.6.1.3.3.4.3.3
  - 72 LGS UFSAR Chapter 7.6.1.3.3.4.3.4
  - 73 LGS UFSAR Chapter 7.3.1.1.2.4.11.1
  - 74 LGS UFSAR Chapter 7.3.1.1.2.4.11.3
  - 75 LGS UFSAR Chapter 7.3.1.1.2.4.11.4
  - 76 LGS UFSAR Chapter 7.3.1.1.2.4.11.6
  - 77 LGS UFSAR Chapter 7.6.1.3.3.5.3.2
  - 78 LGS UFSAR Chapter 7.6.1.3.3.5.3.3
  - 79 LGS UFSAR Chapter 7.3.1.1.2.4.13
  - 80 LGS UFSAR Chapter 7.6.1.3.3.3.1
  - 81 LGS UFSAR Chapter 7.3.1.1.2.11
  - 82 LGS UFSAR Chapter 7.3.1.1.1
  - 83 LGS UFSAR Chapter 7.3.1.1.1.1.8
  - 84 LGS UFSAR Figure 7.3-4
  - 85 LGS UFSAR Figure 7.3-6
  - 86 LGS UFSAR Chapter 7.3.1.1.1.1.2
  - 87 LGS UFSAR Chapter 7.3.1.1.1.1.3
  - 88 LGS UFSAR Chapter 7.3.1.1.1.1.4
  - 89 LGS UFSAR Chapter 7.3.1.1.1.1.7
  - 90 LGS UFSAR Chapter 7.3.1.1.1.1.5
  - 91 LGS UFSAR Chapter 7.3.1.1.1.1.9
  - 92 LGS UFSAR Chapter 7.3.1.1.1.1.11.2
  - 93 LGS UFSAR Chapter 7.3.1.1.1.2.2
  - 94 LGS UFSAR Chapter 7.3.1.1.1.2.8
  - 95 LGS UFSAR Chapter 7.3.1.1.1.2.7
  - 96 LGS UFSAR Chapter 7.3.1.1.1.2.2
  - 97 LGS UFSAR Chapter 7.3.1.1.1.2.3



- 
- <sup>98</sup> LGS UFSAR Chapter 7.3.1.1.1.2.6  
<sup>99</sup> LGS UFSAR Chapter 7.3.1.1.1.2.4  
<sup>100</sup> LGS UFSAR Figure 7.3-4  
<sup>101</sup> LGS UFSAR Chapter 7.3.1.1.1.2.5  
<sup>102</sup> LGS UFSAR Chapter 7.3.1.1.1.2.9  
<sup>103</sup> LGS UFSAR Chapter 7.3.1.1.1.2.11.2  
<sup>104</sup> LGS UFSAR Chapter 7.3.1.1.1.3.6  
<sup>105</sup> LGS UFSAR Chapter 7.3.1.1.1.3.2  
<sup>106</sup> LGS UFSAR Chapter 7.3.1.1.1.3.8  
<sup>107</sup> LGS UFSAR Chapter 7.3.1.1.1.3.7  
<sup>108</sup> LGS UFSAR Chapter 7.3.1.1.1.3.3  
<sup>109</sup> LGS UFSAR Chapter 7.3.1.1.1.3.3  
<sup>110</sup> LGS UFSAR Chapter 7.3.1.1.1.3.3  
<sup>111</sup> LGS UFSAR Chapter 8.1.6.1.14 a.5  
<sup>112</sup> LGS UFSAR Chapter 7.3.1.1.1.3.4  
<sup>113</sup> LGS UFSAR Chapter 7.3.1.1.1.3.10  
<sup>114</sup> LGS UFSAR Chapter 7.3.1.1.1.3.5  
<sup>115</sup> LGS UFSAR Chapter 7.6.1.2  
<sup>116</sup> LGS UFSAR Chapter 7.3.1.1.1.3.9  
<sup>117</sup> LGS UFSAR Chapter 7.3.1.1.1.3.11.2  
<sup>118</sup> LGS UFSAR Chapter 7.3.1.1.1.4.1  
<sup>119</sup> LGS UFSAR Chapter 7.3.1.1.1.4.2  
<sup>120</sup> LGS UFSAR Chapter 7.3.1.1.1.4.11.1  
<sup>121</sup> LGS UFSAR Chapter 7.3.1.1.1.4.3  
<sup>122</sup> LGS UFSAR Chapter 7.3.1.1.1.4.3  
<sup>123</sup> LGS UFSAR Chapter 7.3.1.1.1.4.5  
<sup>124</sup> LGS UFSAR Chapter 7.6.1.2  
<sup>125</sup> LGS UFSAR Chapter 7.3.1.1.1.4.9  
<sup>126</sup> LGS UFSAR Chapter 7.3.1.1.1.4.11.2  
<sup>127</sup> LGS UFSAR Chapter 5.4.6.1.1.1  
<sup>128</sup> LGS UFSAR Chapter 7.6.1.3.3.3.2  
<sup>129</sup> LGS UFSAR Chapter 7.6.1.3.3.3.2  
<sup>130</sup> LGS UFSAR Chapter 7.6.1.3.3.3.3  
<sup>131</sup> LGS UFSAR Chapter 7.3.1.1.2.4.13  
<sup>132</sup> LGS UFSAR Chapter 7.4.1.2.1.1  
<sup>133</sup> LGS UFSAR Chapter 7.4.1.2.1.2  
<sup>134</sup> LGS UFSAR Chapter 7.4.1.2.2.2  
<sup>135</sup> LGS UFSAR Chapter 7.4.1.2.3.3  
<sup>136</sup> LGS UFSAR Chapter 7.4.1.2.3.4  
<sup>137</sup> LGS UFSAR Chapter 7.4.1.2.3.8  
<sup>138</sup> LGS UFSAR Chapter 7.4.1.2.5.1  
<sup>139</sup> LGS UFSAR Chapter 7.4.1.2.5.2  
<sup>140</sup> LGS UFSAR Chapter 7.6.1.8.3  
<sup>141</sup> LGS UFSAR Chapter 1.2.4.2.26  
<sup>142</sup> LGS UFSAR Chapter 7.6.1.8.2  
<sup>143</sup> LGS UFSAR Chapter 7.6.1.8.3.7  
<sup>144</sup> LGS UFSAR Chapter 7.6.1.8.3.6  
<sup>145</sup> LGS UFSAR Chapter 7.6.1.8.3  
<sup>146</sup> LGS UFSAR Chapter 7.6.1.2.3  
<sup>147</sup> LGS PPS SyDS WNA-DS-04899-GLIM, Revision 0, Attachment in PRIME  
<sup>148</sup> LGS PPS SyDS WNA-DS-04900-GLIM, Revision 0, Section 3.3.2  
<sup>149</sup> LGS PPS SyDS WNA-DS-04900-GLIM, Revision 0, Requirements PPS-SyDS-1115 - 1118  
<sup>150</sup> The description in this section is adapted from WCAP-17179-P, Revision 6



- 
- <sup>151</sup> CIM Technical Report, WCAP-17179-P, Revision 6, Section 2.5.1.1.1  
<sup>152</sup> CIM Technical Report, WCAP-17179-P, Revision 6, Section 3.2.2  
<sup>153</sup> LGS PPS SyDS WNA-DS-04900-GLIM, Revision 0, Section 3.8.1  
<sup>154</sup> LGS PPS SyDS WNA-DS-04900-GLIM, Revision 0, Requirement PPS-SyDS-39825  
<sup>155</sup> LGS PPS Section 9.2  
<sup>156</sup> PPS SyRS WNA-DS-04900-GLIM, Revision 0, Requirement PPS-SyDS-1023  
<sup>157</sup> PPS SyDS WNA-DS-04900-GLIM, Revision 0, Requirement PPS-SyDS-40330  
<sup>158</sup> LGS PPS SyDS WNA-DS-04900-GLIM, Revision 0, Section 5.6.1  
<sup>159</sup> PPS SyRS WNA-DS-04899-GLIM, Revision 0, PPS-SyRS-405, PPS-SyRS-3768, PPS-SyRS-3771  
<sup>160</sup> LGS PPS to DCS Interface Specification, WNA-DS-05091-GLIM, Revision 0, Figure 2.18  
<sup>161</sup> PPS SyRS WNA-DS-04899-GLIM, Revision 0, PPS-SyRS-405, PPS-SyRS-480  
<sup>162</sup> PPS to DCS Interface Specification, WNA-DS-05091-GLIM, Revision 0, Figure 2.1-4  
<sup>163</sup> CIM Technical Report, WCAP-17179-P, Revision 6, Section 2.1  
<sup>164</sup> PPS to DCS Interface Specification, Revision 0, Figure 2.1-5  
<sup>165</sup> PPS to DCS Interface Specification, Revision 0, Figure 2.1-9  
<sup>166</sup> PPS to DCS Interface Specification, Revision 0, Figure 2.1-3  
<sup>167</sup> PPS to DCS Interface Specification, Revision 0, Figure 2.1-9  
<sup>168</sup> LGS DMP PPS to DCS Interface Specification, WNA-DS-05091-GLIM, Rev. 0, Section 1.4 and requirements PPS-DCS-2.3-05  
<sup>169</sup> LGS DMP PPS to DCS Interface Specification, WNA-DS-05091-GLIM, Rev. 0, requirement PPS-DCS-2.3-03  
<sup>170</sup> PPS SyRS WNA-DS-04899-GLIM, Rev. 0, Requirement PPS-SyRS-366  
<sup>171</sup> Common Q Topical Report, Reference 3, Section 5.2.1.1.1  
<sup>172</sup> Common Q Topical Report, Reference 3, Section 5.2.1.2.2  
<sup>173</sup> Common Q Topical Report, Reference 3, Section 5.2.1.2.1, Base Software, Communication Section Software Description  
<sup>174</sup> CIM Technical Report, WCAP-17179, Revision 6, Section 3.2.1  
<sup>175</sup> PPS SyDS WNA-DS-04900-GLIM, Revision 0, Requirement PPS-SyDS-950 and Appendix D, CQTR-7 (SER 2.1) disposition.  
<sup>176</sup> The MTP and AC160 are two different computer systems and thus run asynchronously.  
<sup>177</sup> PPS SyDS WNA-DS-04900-GLIM, Revision 0, Requirement PPS-SyDS-40333.  
<sup>178</sup> PPS SyDS WNA-DS-04900-GLIM, Revision 0, Requirements PPS-SyDS-40332 and PPS-SyDS-1966  
<sup>179</sup> Software Design Description for the Common Q Generic Flat Panel Display Software, 00000-ICE-30157, Rev. 26, Section 5.6.7  
<sup>180</sup> Software Design Description for the Common Q Generic Flat Panel Display Software, 00000-ICE-30157, Rev. 26, Section 4.5.13  
<sup>181</sup> LGS PPS Failure Modes and Effects Analysis, WNA-AR-01050-GLIM, Revision 0  
<sup>182</sup> Common Q Topical Report, WCAP-16097-P-A, Revision 5, Section 5.2.1.3  
<sup>172-186</sup> Not used  
<sup>183</sup> See requirements for actuating divisions in PPS SyRS WNA-DS-04899-GLIM, Revision 0, Section 5 (e.g., Section 5.3.2.2 for ADS)  
<sup>184</sup> PPS SyRS WNA-DS-04899-GLIM, Revision 0, Requirements PPS-SyRS-3709  
<sup>185</sup> PPS SyRS WNA-DS-04899-GLIM, Revision 0, Section 5.1.1.3 and Requirements PPS-SyRS-3345, PPS-SyRS-8982, PPS-SyRS-9046, PPS-SyRS-9079, PPS-SyRS-9090  
<sup>186</sup> LGS PPS SyRS WNA-DS-04899-GLIM, Revision 0, Requirement PPS-SyRS-360  
<sup>187</sup> LGS PPS SyRS WNA-DS-04899-GLIM, Revision 0, Requirement PPS-SyRS-8982  
<sup>188</sup> LGS PPS SyRS WNA-DS-04899-GLIM, Revision 0, Requirement PPS-SyRS-9046  
<sup>189</sup> LGS UFSAR Chapter 7.3.2.15.6  
<sup>190</sup> The PPS SyRS WNA-DS-04899-GLIM, Revision 0, Requirements PPS-SyRS-3937, PPS-SyRS-3944, and PPS-SyRS-8818 define the operating temperature range for the AER  
<sup>191</sup> PPS SyRS WNA-DS-04899-GLIM, Revision 0, Requirement PPS-SyRS-10239  
<sup>192</sup> Plant Protection System (PPS) Performance Specification, NE-402, Section 6.4  
<sup>193</sup> PPS SyRS WNA-DS-04900-GLIM, Revision 0, Requirements PPS-SyDS-39560 and PPS-SyDS-39561  
<sup>194</sup> CIM Technical Report, WCAP-17179-P, DI&C-ISG-04 (Section 2, Position 10)
-



- 
- <sup>195</sup> PPS SyRS WNA-DS-04899-GLIM, Revision 0, Section 5.1.1.2  
<sup>196</sup> PPS SyRS WNA-DS-04899-GLIM, Revision 0, Section 5.2  
<sup>197</sup> PPS SyRS WNA-DS-04899-GLIM, Revision 0, Section 53  
<sup>198</sup> See the Equipment Qualification Summary Report (Reference 36)  
<sup>199</sup> See technical specification markups for the LAR for which this LTR is attached.  
<sup>200</sup> PPS SyRS WNA-DS-04899-GLIM, Revision 0, Requirement PPS-SyRS-3871  
<sup>201</sup> LGS PPS SyRS WNA-DS-04899-GLIM, Revision 0, Requirement PPS-SyRS-4052  
<sup>202</sup> LGS PPS SyRS WNA-DS-04899-GLIM, Revision 0, Requirement PPS-SyRS-10238  
<sup>203</sup> LGS PPS SyRS WNA-DS-04899-GLIM, Revision 0, Requirement PPS-SyRS-4052  
<sup>204</sup> Common Q Topical Report, Revision 5, DI&C-ISG-06, Position 10 (Section 5.6.10), PPS SyDS WNA-DS-04900-GLIM, Revision 0, Requirement PPS-SyDS-1860  
<sup>205</sup> LGS PPS SyRS WNA-DS-04900-GLIM, Revision 0, Requirement PPS-SyDS-1861  
<sup>206</sup> WCAP-16097-P-A, Section 5.6.10  
<sup>207</sup> WCAP-16097-P-A, Section 5.6.10  
<sup>208</sup> WCAP-16097-P-A, Section 5.6.10  
<sup>209</sup> WCAP-16097-P-A, Section 5.2.1.2.1 *Slow Background Task*, and 00000-ICE-3239 Section 3.2.24  
<sup>210</sup> LGS PPS SyRS WNA-DS-04899-GLIM, Revision 0, Requirement PPS-SyRS-3709  
<sup>211</sup> The LGS PPS SyDS WNA-DS-04900-GLIM, Revision 0, does not cite a requirement for an SLE keyswitch for the SD  
<sup>212</sup> The AI688 analog input module does not provide for or require manual calibration.  
<sup>213</sup> LGS PPS SyRS, WNA-DS-04899-GLIM, Revision 0, Sections 5.1.3.3, 5.3.4.4, 5.6  
<sup>214</sup> LGS PPS SyRS, WNA-DS-04899-GLIM, Revision 0, Section 5.5  
<sup>215</sup> LGS PPS SyRS, WNA-DS-04899-GLIM, Revision 0, Section 5.1.1.3  
<sup>216</sup> LGS PPS to DCS Interface Specification, WNA-DS-05091-GLIM, Revision 0  
<sup>217</sup> LGS PPS to DCS Interface Specification, WNA-DS-05091-GLIM, Revision 0  
<sup>218</sup> LGS PPS to DCS Interface Specification, WNA-DS-05091-GLIM, Revision 0  
<sup>219</sup> HARP Hardware Requirements Specification, WNA-DS-05100-GEN, Revision A  
<sup>220</sup> HARP Hardware Requirements Specification, WNA-DS-05100-GEN, Revision A  
<sup>221</sup> AP1000 I&C Data Communication and Manual Control of Safety Control of Safety System and Components, WCAP-16674-P, Revision 9 cited in Vogtle 3&4 UFSAR Table 1.6-1  
<sup>222</sup> LGS PPS to DCS Interface Specification, WNA-DS-05091-GLIM, Revision 0  
<sup>223</sup> LGS DMP Component Interface, WNA-DS-05110-GLIM, Revision 0  
<sup>224</sup> LGS DMP Component Interface, WNA-DS-05110-GLIM, Revision 0  
<sup>225</sup> LGS UFSAR Chapter 7.1.2.2.3.1.f and PPS SyDS WNA-DS-04900-GLIM, Revision 0, Requirement PPS-SyDS-991  
<sup>226</sup> PPS SyDS WNA-DS-04900-GLIM, Revision 0, Requirements PPS-SyDS-385 and PPS-SyDS-1107  
<sup>227</sup> LGS UFSAR Chapter 3, GDC 24 disposition  
<sup>228</sup> LGS SyRS WNA-DS-04899-GLIM, Revision 0, Requirement PPS-SyRS-10239  
<sup>229</sup> WCAP-16097-P-A, Section 5.2.1.1.1 Diagnostic Functions  
<sup>230</sup> LGS UFSAR Chapter 3, GDC 24 disposition  
<sup>231</sup> LGS SyRS WNA-DS-04899-GLIM, Revision 1, Requirements PPS-SyRS-840, PPS-SyRS-904, and PPS-SyRS-366 (Guidance)  
<sup>232</sup> LGS PPS Response Time Analysis, WNA-CN-00651-GLIM, Revision 0  
<sup>233</sup> The SD is a Common Q Flat Panel Display System described in the Common Q Topical Report  
<sup>234</sup> Licensing precedents include the Oconee RPS/ESFAS, the AP1000 Protection and Safety Monitoring System, and the APR1400 Safety System.  
<sup>235</sup> Avant Configuration for the Common Q Qualification Test, 00000-ICE-39165, Revision 1, Section 3  
<sup>236</sup> WNA-RM-00016-GLIM, LGS PPS Requirements Management Plan, Section 2.1. The engineering organization is delineated by system design, hardware design, and software design.  
<sup>237</sup> WCAP-16096-P-A SPM Section 4.6.2.2.1  
<sup>238</sup> WNA-PC-00071-GLIM  
<sup>239</sup> PPS SyRS WNA-DS-04899-GLIM, Revision 0, Appendix D and SyDS WNA-DS-04900-GLIM, Revision 0, Appendix F
-



- 
- <sup>240</sup> WCAP-16096-P-A SPM, Definition for RTM
- <sup>241</sup> WCAP-16096-P-A SPM, Section 4.6.2.1
- <sup>242</sup> WCAP-16096-P-A SPM, Exhibit 5-1
- <sup>243</sup> PPS LGS Software Development Plan, WNA-PD-00671-GLIM, Revision 0, Appendix A
- <sup>244</sup> WCAP-16096-P-A SPM, Exhibit 5-1
- <sup>245</sup> WCAP-16096-P-A SPM, Section 5.5.4.1 and 5.5.4.2
- <sup>246</sup> There are a multitude of Westinghouse internal work instructions. One example is WNA-WI-00053-GEN, Custom PC Element Compile and Link Work Instructions
- <sup>247</sup> Reference 25 in this document and Configuration Management Implementation Guideline WNA-IG-00109-GEN
- <sup>248</sup> WCAP-16096-P-A SPM, Sections 2.1.1.3 and 3.3.10
- <sup>249</sup> Westinghouse can provide an organization chart at time of review
- <sup>250</sup> Reference 3 in this document, PSAI 6.3
- <sup>251</sup> NRC ITAAC Review Status Report, ML21032A260
- <sup>252</sup> LGS PPS SyDS WNA-DS-04900-GLIM, Revision 0, Table D-4
- <sup>253</sup> The procedure number will be IC-11-05000 and Constellation Document services will hold it until the procedure is written. There will be multiple procedures in the IC-11-05000 series. 5000 will be administrative and general in nature when working with the Common Q PPS. An assignment in the LGS work tracking system (#4456632 04) establishes the requirement for procedure IC-11-05000 to be created to ensure setpoints are not changed while relying on its safety related function.
- <sup>254</sup> PPS SyDS WNA-DS-04900-GLIM, Revision 0, Requirement PPS-SyDS-39567
- <sup>255</sup> Each function described in the SyRS WNA-DS-04899-GLIM, Revision 0, Section 5, includes the requirements for soft control of those functions.
- <sup>256</sup> LGS UFSAR Chapter 15.0.3.2.1, “Transient evaluations have been judged against a criterion of one single active failure, or one single operator error, as the initiating event, with no additional single failure assumptions to the protective sequences, although a great majority of these protective sequences are utilized in safety systems that can accommodate single active failures aspects.” The D3 Analysis, WNA-AR-01074-GLIM marks each PPS automatic actuation that becomes disabled due to CCF. None of the sequences identify a manual PPS system level actuation.
- <sup>257</sup> LGS PPS SyDS WNA-DS-04900-GLIM, Revision 0, Section 11.3
- <sup>258</sup> LGS PPS SyDS WNA-DS-04900-GLIM, Requirement R-DS-04900-1885
- <sup>259</sup> Locked cabinet: PPS SyDS WNA-DS-04900-GLIM, Revision 0, Section 11.1; Secure location: AER and MCR are secured areas at LGS.
- <sup>260</sup> Section 3.2 in this document.
- <sup>261</sup> Section 3.2.21 in this document.
- <sup>262</sup> LGS PPS SyRS WNA-DS-04899-GLIM, Revision 0, Section 4.2
- <sup>263</sup> 10 CFR 50.62, “(3) Each boiling water reactor must have an alternate rod injection (ARI) system that is diverse (from the reactor trip system) from sensor output to the final actuation device. The ARI system must have redundant scram air header exhaust valves. The ARI must be designed to perform its function in a reliable manner and be independent (from the existing reactor trip system) from sensor output to the final actuation device.”
- <sup>264</sup> Safety to Non-Safety Interface Specification, WNA-DS-05091-GLIM, Section 2.2.3
- <sup>265</sup> WNA-AR-00039-GEN, Revision 3, Section Table 3.1-1.
- <sup>266</sup> See LAR Technical Specification Markups and justification for eliminating manual actuations from the technical specifications.
- <sup>267</sup> See LGS PPS SyRS WNA-DS-04899-GLIM, Revision 0, Requirement PPS-SyRS-8985
- <sup>268</sup> LGS DMP Component Interface Specification, WNA-DS-05110-GLIM, Section 3.1
- <sup>269</sup> High Amperage Replay Panel Assembly Hardware Requirements Specification , WNA-DS-05100-GEN, Revision A



\*\*This page was added to the quality record by the PRIME system upon its validation and shall not be considered in the page numbering of this document.\*\*

## Approval Information

Author Approval Odess Gillett Warren Jul-12-2022 06:40:31

Reviewer Approval Mocello Dominic M Jul-12-2022 08:28:25

Reviewer Approval Solmos Matthew Jul-12-2022 09:46:55

Reviewer Approval Seaman Stephen Jul-12-2022 20:28:14

Reviewer Approval Shakun Matthew A Jul-13-2022 12:11:58

Approver Approval Harper Zachary S Jul-13-2022 13:56:11

Files approved on Jul-13-2022

\*\*\* This record was final approved on 7/13/2022, 1:56:11 PM. (This statement was added by the PRIME system upon its validation)



**ATTACHMENT 6 TRANSMITTED HERewith CONTAINS PROPRIETARY INFORMATION –  
WITHHOLD UNDER 10 CFR 2.390**

**Attachment 6**

**Limerick Generating Station, Units 1 and 2  
Docket Nos. 50-352 and 50-353**

**Licensing Technical Report for the Limerick Generating Station Units 1&2  
Digital Modernization Project, WCAP-18598-P, Revision 0**