

ROUTING AND TRANSMITTAL SLIP

Date

5-24-94

TO: (Name, office symbol, room number, building, Agency/Post)

Initials

Date

BCS P1 37

PDR

2.

3.

4.

5.

Action	File	Note and Return
Approval	For Clearance	Per Conversation
As Requested	For Correction	Prepare Reply
Circulate	For Your Information	See Me
Comment	Investigate	Signature
Coordination	Justify	

REMARKS

This previous Central File material can now be made publicly available.

MATERIAL RELATED TO CRGR  
MEETING NO. 163

CC (LIST ONLY) JEAN RATAJE,  
PDR L STREET

DO NOT use this form as a RECORD of approvals, concurrences, disposals, clearances, and similar actions

FROM: (Name, org. symbol, Agency/Post)

Room No.—Bldg.

DENNIS ALLISON

Phone No.

24148

5041-102

OPTIONAL FORM 41 (Rev. 7-76)  
Prescribed by GSA  
FPMR (41 CFR) 101-11.206

☆ U.S. GPO: 1977-551-107 3324

310310

FORB  
1/1

9406070054 940524  
PDR REVP NRGRGR  
MEETING163 PDR

MATERIAL RELATED TO CRGR MEETING NO. 163  
TO BE MADE PUBLICLY AVAILABLE

1. MEMO FOR J. TAYLOR FROM E. JORDAN DATED 6-21-89  
SUBJECT: MINUTES OF CRGR MEETING NUMBER 163  
INCLUDING THE FOLLOWING ENCLOSURES WHICH WERE NOT  
PREVIOUSLY RELEASED:
  - a. ENCLOSURE 2  
A SUMMARY OF DISCUSSIONS OF A PROPOSED BL on the  
Emergency Response Data System
  - b. ENCLOSURE 3  
A SUMMARY OF DISCUSSIONS OF A PROPOSED Resolution  
of USI A-17 Systems Interactions in NPPs
  - c. ENCLOSURE 4  
A SUMMARY OF DISCUSSIONS OF A PROPOSED Resolution  
for GI-128
  - d. USI A-47 Safety Implications of Control System in LWP NPPs
2. MEMO FOR E. JORDAN FROM E. Bickford DATED 5-10-89  
FORWARDING REVIEW MATERIALS ON A PROPOSED Final  
Resolution of USI A-17 Systems Interactions in NPPs
3. MEMO FOR E. JORDAN FROM E. Bickford DATED 5-2-89  
FORWARDING REVIEW MATERIALS ON A PROPOSED Resolution  
of GI-128 Which includes: GI-48; GI-49 and GI A-30
4. MEMO FOR E. JORDAN FROM E. Bickford DATED 4-3-89  
FORWARDING REVIEW MATERIALS ON A PROPOSED Resolution of  
USI A-47, "Safety Implications of Control Systems  
in LWR NPPs"





UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
WASHINGTON, D. C. 20555

June 21, 1989

MEMORANDUM FOR: Victor Stello, Jr.  
Executive Director for Operations

FROM: Edward L. Jordan, Chairman  
Committee to Review Generic Requirements

SUBJECT: MINUTES OF CRGR MEETING NUMBER 163

The Committee to Review Generic Requirements (CRGR) met on Wednesday, May 24, 1988 from 1:00 - 5:00 p.m. A list of attendees for this meeting is attached (Enclosure 1). The following items were addressed at the meeting:

1. G. Zech (AECC) presented for CRGR review a proposed generic letter to provide information to licensees on the design and implementation policy for the Emergency Response Data System, and to request voluntary participation by licensees. The Committee recommended in favor of issuing the proposed generic letter. This matter is discussed in Enclosure 2.
2. R. Baer (RES) and D. Thatcher (RES) presented for CRGR review the proposed final resolution for Unresolved Safety Issue (USI) A-17, "Systems Interaction in Nuclear Power Plants." The Committee recommended in favor of approval of the proposed resolution, including issuance of a proposed implementing generic letter to licensees, subject to a number of minor modifications to the wording of the package (to be coordinated with the CRGR staff). These matters are discussed in Enclosure 3.
3. R. Baer (RES) and D. Thatcher (RES) presented for CRGR review the proposed resolution for integrated GI-128, which includes and combines GI A-30 (Adequacy of Safety-Related DC Power Supplies), GI-48 (LCOs for Class 1E Vital Instrument Buses), and GI-49 (Interlocks and LCOs for Class 1E Tie Breakers). The Committee recommended in favor of approval of the proposed resolution, including issuance of two 50.54(f) generic information request letters to licensees, subject to a number of minor modifications to the wording of the package (to be coordinated with the CRGR staff). This matter is discussed in Enclosure 4.
4. R. Baer (RES) and A. Szukiewicz (RES) presented for CRGR review the proposed final resolution for USI A-47, "Safety Implications of Control Systems in LWR Nuclear Power Plants." The Committee recommended in favor of approval of the proposed resolution, including issuance of a proposed implementing generic letter to licensees, subject to a number of changes to the wording of the package. The changes to the package are to be reviewed by the Committee prior to final issuance of the proposed resolution and implementing generic letter. This matter is discussed in Enclosure 5.

~~8907120264~~

As a general collateral recommendation related to the above items, the Committee recommended (a) that NRR issuance of the USI-related generic letters and their respective response dates be staggered since all three impact electrical and instrumentation engineering support, and (b) that NRR act to eliminate discrepancies between issuance date and mailing date for generic letters, since schedules specified for actions refer back to the issuance dates of the generic letter.

In accordance with the EDO's July 18, 1983 directive concerning "Feedback and Closure on CRGR reviews," a written response is required from the cognizant office to report agreement or disagreement with the CRGR recommendations in these minutes. The response, which is required within five working days after receipt of these minutes, is to be forwarded to the CRGR Chairman and if there is disagreement with CRGR recommendations, to the EDO for decisionmaking.

Questions concerning these meeting minutes should be referred to Jim Conran (492-9855).

Original Signed By  
E. L. Jordan

Edward L. Jordan, Chairman  
Committee to Review Generic  
Requirements

Enclosures:  
As stated

cc/w enclosures:  
Commission (5)  
SECY  
J. Lieberman  
P. Norry  
M. Malsch  
Regional Administrators  
CRGR Members

Distribution: (w/o enc.)  
Central File  
PDR (NRC/CRGR)  
S. Treby  
W. Little  
M. Lesar  
P. Kadambi (w/enc.)  
CRGR CF (w/enc.)  
CRGR SF (w/enc.)  
M. Taylor (w/enc.)  
L. Spessard (w/enc.)  
E. Rossi (w/enc.)  
W. Houston (w/enc.)  
G. Zech (w/enc.)  
R. Baer (w/enc.)  
E. Jordan (w/enc.)  
J. Heltemes (w/enc.)  
J. Conran (w/enc.)  
C. Sakenas (w/enc.)

OFC	: CRGR:AEOD	: AEOY:DD	: C/CRGR:AEOD		
NAME	: JConran:cg	: CJHeltemes	: EJordan		
DATE	: 6/2/89	: 6/2/89	: 6/2/89		

ATTENDANCE LIST  
FOR  
CRGR MEETING NO. 163

May 24, 1989

CRGR MEMBERS

E. Jordan  
C. Paperiello  
J. Goldberg  
R. Burnett (for R. Bernero)  
F. Gillespie (for J. Sniezek)

NRC STAFF

C. J. Heltemes  
J. Conran  
C. Sakenas  
K. Connaughton  
T. DiPalo  
M. Au  
M. Taylor  
G. Zech  
R. Priebe  
R. Baer  
W. Minners  
D. Thatcher  
A. Szukiewicz  
M. El-Zeftawy  
D. Houston

Enclosure 2 to the Minutes of CRGR Meeting No. 163  
Proposed Generic Letter on the Emergency Response Data System (ERDS)

May 24, 1989

TOPIC

G. Zech (AEOD) presented for CRGR review a proposed generic letter which provides information to licensees on the design and implementation policy for the ERDS, and requests voluntary participation by licensees.

BACKGROUND

The package submitted by the staff for CRGR review of this matter was transmitted by memorandum dated April 21, 1989, R. L. Spessard to E. L. Jordan, and included a draft of the generic letter and the background information required by the CRGR Charter.

CONCLUSIONS/RECOMMENDATIONS

As a result of their review of this matter, including discussions with the staff at this meeting, the Committee recommended in favor of issuing the proposed generic letter.

Enclosure 3 to the Minutes of CRGR Meeting No. 163  
Proposed Resolution of USI A-17, "Systems Interactions  
in Nuclear Power Plants"

May 24, 1989

TOPIC

R. Baer (RES) and D. Thatcher (RES) presented for CRGR review a proposed final resolution for Unresolved Safety Issue A-17, "Systems Interactions in Nuclear Power Plants." (The Committee considered the proposed draft resolution for this USI previously at Meeting Nos. 88 and 139.) Copies of the slides used by the staff to guide their presentation and the discussions with the Committee at this meeting are enclosed (Attachment 1).

BACKGROUND

1. The documents submitted for CRGR review in this matter were transmitted by memorandum dated May 10, 1989, E. S. Beckjord to E. L. Jordan; the review package included the following documents:
  - a. Draft Commission Paper (undated), "Unresolved Safety Issue A-17, 'Systems Interactions in Nuclear Power Plants,'" with three enclosures:
    - i. Enclosure 1 - Draft NUREG-1174 (undated), "Evaluation of Systems Interactions in Nuclear Power Plants"
    - ii. Enclosure 2 - Draft NUREG-1229 (undated), "Regulatory Analysis for Resolution of USI A-17"
    - iii. Enclosure 3 - Proposed Federal Register Notice and Summary Statement
  - b. Proposed Generic Letter (undated), "Resolution of Unresolved Safety Issue A-17, 'Systems Interactions in Nuclear Power Plants,'" with two attachments:
    - i. Attachment 1 - "Bases for Resolution of Unresolved Safety Issue A-17"
    - ii. Attachment 2 - "Summary Information for Use in Operating Experience Evaluations"
2. At the request of the CRGR staff, RES provided informally draft, updated SIMS sheets for USI A-17 for the information of the Committee (see Attachment 2).

CONCLUSIONS/RECOMMENDATIONS

As a result of their review of this matter, including the discussions with the staff at this meeting, the Committee recommended in favor of issuance of the

proposed final resolution for USI A-17, subject to a number of specific wording modifications discussed with the staff at this meeting, as follows:

1. Attachment 1 to the proposed Generic Letter:
  - a. At page 1, modify the second sentence of the second paragraph to read as follows:

"The staff has identified actions by licensees and the NRC that should acceptably reduce the risk from adverse systems interactions and resolve USI A-17."
  - b. At page 1, modify the sentence that comprises the third paragraph to read as follows:

"This resolution for USI A-17 is not based on the assertion that all ASIs have been identified, but rather that the A-17 actions plus other related activities by the licensees and NRC staff discussed further below provide reasonable assurance that the more risk significant ASIs will be identified and that appropriate corrective actions will be taken."
  - c. At page 1, under "Resolution," change the title of subsection (1) to "Ongoing Actions by Licensees."
  - d. At page 1, in the last sentence under subsection (1)(a), change the word "requires" to "calls for."
  - e. At the bottom of page 1 and top of page 2, delete the existing paragraph (1)(b), relabel existing paragraph (1)(c) as new paragraph (1)(b), and include in the new paragraph (1)(b) reference to Attachment 2 to this proposed Generic Letter as a kind of information (e.g., "other reports") disseminated by NRC that licensees would be expected to consider routinely in their ongoing operating experience reviews under Item I.C.5. of NUREG-0737.
  - f. At page 2, change the title of subsection (2) to "Actions by the NRC Related to Adverse Systems Interactions."
  - g. At page 3, under "Existing Plants" at the bottom of the page, change the wording of the first sentence to read as follows:

"The Severe Accident Policy, 50 FR 32128 (August 8, 1985), expresses the Commission's intent that all existing plants perform a plant-specific search for vulnerabilities."
2. In Attachment 2 to the proposed Generic Letter:
  - a. Change the title of this attachment to "SUMMARY INFORMATION RELEVANT TO OPERATING EXPERIENCE EVALUATIONS."
  - b. At page 1, in the line immediately following the second paragraph, change the word "document" to "attachment."



- c. At page 4, under subparagraph (10) near the top of the page, change the word "may" to "should."
- d. At page 4, in the last sentence under subparagraph (11), change the word "could" to "should."
- d. At page 4, at the beginning of the paragraph at the bottom of the page, change the wording to read as follows:

"...certain actions should be taken by NRC to resolve USI A-17. These actions are:"
- e. At page 4, change the wording of subparagraph (2) near the bottom of the page to read as follows:

"Consider the insights developed in the resolution of USI A-17 for flooding and water intrusion..."
- f. At page 5, change the title of section A to "Information Relevant to Operating Experience Evaluations."
- g. At page 5, change the last paragraph under section A to read as follows:

"Although no specific licensee actions are required, the staff concluded that it should communicate to the industry certain highlighted concerns identified in the A-17 studies. The insights gained from this information should be beneficial to industry in their ongoing evaluations of operating experience."
- h. At page 10, in the last sentence of the third paragraph, change the word "requirements" to "actions."

In addition to the specific changes above, the Committee recommended that the staff review carefully the wording of the other documents in the review package and make conforming changes as appropriate to ensure consistency throughout. All changes to the package are to be coordinated with the CRGR staff.

USI A-17  
"SYSTEMS INTERACTIONS"

PRESENTATION TO CRGR  
OF THE  
FINAL RESOLUTION OF USI A-17

MAY 24, 1989

D. F. THATCHER, TASK MANAGER  
R. L. BAER, BRANCH CHIEF  
R. W. HOUSTON, DIRECTOR  
DIVISION OF SAFETY ISSUE RESOLUTION  
OFFICE OF NUCLEAR REGULATORY RESEARCH

SLIDE 1

USI A-17 BACKGROUND

- o JUNE 1988 PROPOSED GENERIC LETTER
  - BASES FOR RESOLUTION
  - SUMMARY OF INFORMATION FOR USE IN EVALUATION OF OPERATING EXPERIENCE
  - REQUEST (PURSUANT TO 50.54(F)) FOR LICENSEES TO CERTIFY THAT THEY ANALYZED THEIR PLANT FOR FLOODING AND WATER INTRUSION
- o 50.54(F) REQUEST WAS PROPOSED TO BE A VERIFICATION OF LICENSEE COMPLIANCE WITH THE EXISTING LICENSING BASIS
- o CRGR AGREED WITH NEED FOR ACTION ON FLOODING AND WATER INTRUSION
- o CRGR RECOMMENDED MAKING A BACKFIT FINDING AND STATING THAT THE ACTIONS ARE CONSIDERED TO BE "NECESSARY FOR ADEQUATE ASSURANCE OF SAFETY"

INTERNAL FLOODING/WATER INTRUSION CONCERN

- o GENERIC LETTER 88-20 ON INDIVIDUAL PLANT EXAMINATIONS (IPEs) ISSUED NOVEMBER 1988
  - EXPLICITLY REQUESTED INTERNAL FLOODING TO BE INCLUDED
  
- o A-17 PROPOSES TO PROVIDE INSIGHTS TO THE IPE
  
- o IPE GUIDANCE TO REFERENCE A-17 TECHNICAL FINDINGS AND INSIGHTS ON FLOODING AND WATER INTRUSION (NUREG-1174 APPENDIX)

USI A-17 FINAL RESOLUTION

- o ISSUE GENERIC LETTER PROVIDING:
  - BASES FOR RESOLUTION OF A-17
  - SUMMARY OF INFORMATION FOR USE IN EVALUATION OF OPERATING EXPERIENCE
  
- o CONSIDER INTERNAL FLOODING AND WATER INTRUSION IN IPE
  
- o NO NEW REQUIREMENTS
  
- o NO PUBLIC COMMENTS TO BE SOLICITED
  
- o ISSUE:
  - COMMISSION PAPER
  - FEDERAL REGISTER NOTICE
  - NUREG-1229
  
- o INFORM CONGRESSIONAL COMMITTEES

## SAFETY ISSUE LEVEL INFORMATION

ISSUE NUMBER: A-17

TITLE: SYSTEM INTERACTIONS IN NUCLEAR POWER PLANTS

CONTACT: D. THATCHER

TYPE: USI

IDENTIFYING ORGANIZATION: NRR

STATUS:

SPONSORING OFFICE: RES

PRIORITY: U

TYPE OF REACTORS AFFECTED: ALL

OTHER:

DEPENDENT ISSUES: GI 77

## DESCRIPTION

NUCLEAR POWER PLANT IS COMPOSED OF NUMEROUS SYSTEMS, STRUCTURES AND COMPONENTS WHICH ARE DESIGNED AND ANALYZED BY MANY DIFFERENT ENGINEERING DISCIPLINES. THE DEGREE OF FUNCTIONAL AND PHYSICAL INTEGRATION OF ALL THESE SYSTEMS, COMPONENTS AND STRUCTURES INTO ANY SINGLE POWER PLANT MAY VARY CONSIDERABLY. CONCERNS HAVE BEEN RAISED WHICH QUESTION THE ADEQUACY OF THIS FUNCTIONAL AND PHYSICAL INTEGRATION/COORDINATION PROCESS. ALSO IT HAS BEEN POSTULATED THAT ADVERSE SYSTEMS INTERACTIONS (ASI'S) MAY BE INCORPORATED INTO PLANTS BY INADEQUACIES IN THE PROCESS. GIVEN THAT A NUCLEAR POWER PLANT INCLUDES SYSTEMS, COMPONENTS, AND STRUCTURES, INCLUDING SYSTEMS TO NORMALLY CONTROL THE PLANT, SYSTEMS TO RESPOND TO OFF NORMAL EVENTS, AND SYSTEMS WHICH SUPPORT (BOTH FUNCTIONALLY AND PHYSICALLY) OTHER SYSTEMS, IT IS REASONABLE TO SUSPECT THAT SUCH INTERACTIONS MAY EXIST. CURRENT REGULATORY REQUIREMENTS AND GUIDANCE DO NOT ADDRESS THIS AREA. THE USI A-17 PROGRAM WAS INITIATED TO INVESTIGATE THE AREA OF SYSTEMS INTERACTIONS AND CONSIDER VIABLE ALTERNATIVES FOR REGULATORY REQUIREMENTS (INCLUDING DO NOTHING) TO ASSURE THAT ADVERSE SYSTEMS INTERACTIONS HAVE BEEN OR WILL BE MINIMIZED AT OPERATING PLANTS AND NEW PLANTS.

## SOLUTION (NEAR AND LONG TERM)

THE A-17 PROGRAM INVOLVED TWO SIGNIFICANT EFFORTS WHICH PROCEEDED IN PARALLEL, EACH WITH A NUMBER OF TASKS. ONE EFFORT FOCUSED ON OPERATING EXPERIENCE, VARIOUS ACTIVITIES BY UTILITIES, AND NRC STUDIES. ITS OBJECTIVE WAS TO SEARCH FOR COMMON CAUSE EVENTS AND THEN EVALUATED THEM WITH EMPHASIS ON ADVERSE SYSTEMS INTERACTIONS. THE PARALLEL EFFORT FOCUSED ON A REVIEW OF THE METHODS THAT HAVE BEEN AND ARE BEING USED TO UNCOVER ADVERSE SYSTEMS INTERACTIONS. ITS OBJECTIVE WAS TO DETERMINE THE ATTRIBUTES OF THE METHODS SO THAT GUIDELINES CAN BE DEVELOPED FOR DEFINING AN ACCEPTABLE SEARCH PROGRAM IN THE EVENT THAT IT IS DETERMINED TO BE NECESSARY.

A-17 SUBSUMED GI 77.

The regulatory analysis (Reference 2) considered a number of alternatives for resolution, and based on that analysis, the staff has concluded that certain actions should be taken to resolve USI A-17. These actions are:

- (1) Send a generic letter to all plants outlining the resolution of USI A-17 and providing information developed during the resolution of A-17.
- (2) Consider flooding and water intrusion from internal sources in the Individual Plant Examinations (IPE).
- (3) Consider systems interactions involving the electrical power systems in the integrated program on electrical power reliability.
- (4) Provide information for use in future PRAs.

Attachment 2 to Enclosure

(plus next page)



- (5) Provide a framework for addressing those other concerns related to systems interactions which are not covered by the USI A-17 program.
- (6) Acknowledge that the resolution of USI A-46 addresses aspects of systems interaction.
- (7) Develop a standard review plan for future plants to address protection from internal flooding and water intrusion.

S A F E T Y I S S U E S M A N A G E M E N T S Y S T E M

S A F E T Y I S S U E L E V E L I N F O R M A T I O N

ISSUE NUMBER: A-17

TITLE: SYSTEM INTERACTIONS IN NUCLEAR POWER PLANTS

<u>NET CHANGE IN DOLLAR COST</u>	POINT ESTIMATE	<u>RANGE</u>	
		<u>LOW</u>	<u>HIGH</u>
NRC DEVELOPMENT. . . . .	*** NONE AVAILABLE ***		
NRC (IMPLEMENTATION/IMPOSITION). . . . .	*** NONE AVAILABLE ***		
NRC (ASSURE CONTINUED COMPLIANCE). . . . .	*** NONE AVAILABLE ***		
PUBLIC/INDUSTRY/OTHER (IMPLEMENTATION) . . . . .	*** NONE AVAILABLE ***		
PUBLIC/INDUSTRY/OTHER (CONTINUED COMPLIANCE)	*** NONE AVAILABLE ***		
 <u>NET CHANGES IN BENEFITS</u>			
PUBLIC EXPOSURE. . . . .	*** NONE AVAILABLE ***		
OCCUPATIONAL EXPOSURE. . . . .	*** NONE AVAILABLE ***		
CORE MELT FREQUENCY. . . . .	*** NONE AVAILABLE ***		

*not applicable -  
see resolution*

S A F E T Y I S S U E S M A N A G E M E N T S Y S T E M  
S A F E T Y I S S U E L E V E L I N F O R M A T I O N

ISSUE NUMBER: A-17

TITLE: SYSTEM INTERACTIONS IN NUCLEAR POWER PLANTS

ISSUE APPROVAL AND PLANNING:

ISSUE APPROVAL DATE: 01/79C

TECHNICAL RESOLUTION:

LEAD OFFICE: RES

SUPPORTING OFFICE(S): ~~N/A~~ NRR

INITIATION DATE: 86

INTER OFFICE REVIEW/COORDINATION COMPLETION DATE: 85C

PROPOSED SOLUTIONS/REQUIREMENTS APPROVAL BY OFFICE DIRECTOR DATE: 01/87C

REQUIREMENTS REVIEW AND APPROVAL:

INITIAL CRGR REVIEW DATE: <sup>6/28</sup> -12/87

RESOLVED WITH REQUIREMENTS: NO

RESOLUTION DATE: 09/89

R U L E M A K I N G

OTHER (SPECIFY)

FORM. . . . .	ANPR	PROPOSED	FINAL	GEN LETTER
OFFICE RESPONSIBLE. . . . .	*	*	*	RES
EDO APPROVAL TO PROCEED (YES/NO)	*	*	*	***
CRGR REVIEW DATE. . . . .	*	*	*	05 01/89
ACRS REVIEW DATE. . . . .	N	N	N	06/89 -12/87
EDO REVIEW DATE . . . . .	O	O	O	02/89 07/89
APPROVAL (YES/NO). . . . .	N	N	N	***
COMMISSION REVIEW DATE. . . . .	E	E	E	*****
APPROVAL (YES/NO). . . . .	*	*	*	***
PUBLIC COMMENT DATE . . . . .	*	*	*	***** Not Applicable
FINAL APPROVAL AND ISSUANCE DATE	*	*	*	04/89 09/89

REQUIREMENTS IMPOSITION NEEDED FOR VERIFICATION:

A. IMPOSITION - LICENSED PLANTS:

MULTIPLANT ACTION CODE: N/A

OTHER: A portion in IPE

APPROVAL OF LICENSEE PROPOSAL NEEDED (YES/NO): No

S A F E T Y I S S U E S M A N A G E M E N T S Y S T E M

S A F E T Y I S S U E L E V E L I N F O R M A T I O N

ISSUE NUMBER: A-17

TITLE: SYSTEM INTERACTIONS IN NUCLEAR POWER PLANTS

B. IMPOSITION - PLANTS NOT LICENSED: *No* SRP REVIEW PROCESS: *No* OTHER (SPECIFY):

C. IMPOSITION - ALL PLANTS: OFFICE RESPONSIBLE: *RES/NRR*

D. NEED FOR VERIFICATION: *No*

	NEEDED (YES/NO)	OFFICE RESPONSIBLE
VERIFICATION. . . . .	<i>No</i>	--

MPA VERIFICATION PRIORITY:

5. REQUIREMENTS IMPLEMENTATION BY LICENSEE AND VERIFICATION BY NRC:

	COMPLETION STATUS (PLANTS)	DATE OF LAST PLANT
IMPOSITION. . . . .	0 OF 0	*****
IMPLEMENTATION. . . . .	0 OF 0	*****
VERIFICATION. . . . .	0 OF 0	*****

6. REQUIREMENTS IMPLEMENTATION BY STAFF:

A. STAFF REQUIREMENTS -- N O N E

COMPLETION DATE: N/A OFFICE(S) RESPONSIBLE:

B. ROUTINE INSPECTION PROGRAM MODIFICATIONS: *No* MODIFICATIONS NEEDED (YES/NO): NO MODIFICATION COMPLETION DATE: \*\*\*\*\*

M O D I F I C A T I O N T E X T

-----  
\*\*\* NO MODIFICATION TEXT FOR ISSUE \*\*\*

S A F E T Y I S S U E S M A N A G E M E N T S Y S T E M  
P L A N T L E V E L I N F O R M A T I O N

ISSUE NUMBER: A-17

TITLE: SYSTEM INTERACTIONS IN NUCLEAR POWER PLANTS

<u>PLANT</u>	<u>DOCKET #</u>	<u>DOCKET</u> <u>PRIORITY</u>	<u>REACTOR</u> <u>TYPE</u>	<u>OL</u> <u>ISSUE</u>	<u>OL</u> <u>EXPIR</u>	<u>IMPOS</u> <u>MANAGE</u> <u>METHOD</u>	<u>IMPOS</u> <u>INIT</u>	<u>IMPOS</u> <u>COMPLET</u>	<u>IMPLEM</u> <u>COMPLET</u>	<u>VERIFY</u> <u>COMPLET</u>
--------------	-----------------	----------------------------------	-------------------------------	---------------------------	---------------------------	--	-----------------------------	--------------------------------	---------------------------------	---------------------------------

\*\*\* NO PLANT DATA FOR ISSUE \*\*\*

Enclosure 4 to the Minutes of CRGR Meeting No. 163  
Proposed Resolution for Generic Issue (GI) 128

May 24, 1989

TOPIC

R. Baer (RES) and D. Thatcher (RES) presented for CRGR review the proposed resolution for GI-128, which includes and combines GI-48 (LCOs for Class 1E Vital Instrument Buses), GI-49 (Interlocks and LCOs for Class 1E Tie Breakers), and GI A-30 (Adequacy of Safety-Related DC Power Supplies). The proposed resolution involves issuing to licensees two 50.54(f) generic information request letters regarding compliance with the single failure criterion in existing regulations. Copies of the briefing slides used by the staff to guide their presentation and the discussions of these matters with the Committee at this meeting are enclosed (Attachment 1).

BACKGROUND

1. The documents submitted by RES prior to the meeting for review by CRGR were transmitted by memorandum dated May 2, 1989, E. S. Beckjord to J. H. Sniezek; the review package included the following documents:
  - a. Enclosure 1 (undated) - "Evaluation and Resolution of GI 48 and 49"
  - b. Enclosure 2 (undated) - Draft Generic Letter, "Resolution of Generic Issues 48 and 49,..." and Attachment, "10 CFR 50.54(f) Request...GI-48...GI-49..."
  - c. Enclosure 3 - Technical Evaluation Report dated March 1989, EGG-NTA-7727, Revision 3, "Technical Findings for Proposed Integrated Resolution of Generic Issues 128 (Issue 48 & Issue 49)"
  - d. Enclosure 4 (undated) - "Evaluation and Resolution of GI A-30"
  - e. Enclosure 5 (undated) - Draft Generic Letter, "Resolution of GI A-30 "Adequacy of Safety-Related DC Power Supplies" and Attachment, "10 CFR 50.54(f) Request...GI A-30..."
  - f. Enclosure 6 - Technical Evaluation Report dated March 1989, EGG-NTA-8197, Revision 1, "Technical Findings for Generic Issue 128 (Issue A-30)..."
2. At the request of the CRGR staff, RES provided a revised SIMS sheet (draft) for tracking the status of these integrated generic issues; that item was distributed to CRGR members for information in their review of this matter.



3. At Meeting No. 163, RES provided directly to CRGR members revised versions, dated May 13, 1989, of the documents identified in item 1.b. above, reflecting additional interoffice review comments. For completeness of record, copies of those revised documents are enclosed with these minutes (Attachment 3).

#### CONCLUSIONS/RECOMMENDATION

As a result of their review of this matter, including the discussions with the staff at this meeting, the Committee recommended in favor of issuance of the proposed 50.54(f) generic information request letters, subject to the following caveats:

1. The Committee should review any generic criteria that the staff plans to use in making backfit determinations that might result from their review of 50.54(f) submittals by licensees related to GI A-30.
2. CRGR should review any model standard technical specifications (TS) proposed by the staff intended to be used in reviewing subsequent technical specification revisions by licensees as recommended by the staff in these proposed generic issue resolution packages.
3. The Committee agrees that the proposed response times for the two proposed information request letters (i.e., 180 days) are appropriate; but the issuance dates of the two letters should be staggered to distribute the associated licensee workload more evenly.
4. The staff should make the following clarifying changes to the package before final issuance of the proposed letters to licensees (all changes to be coordinated with the CRGR staff):
  - a. In Enclosure 1 of the review package, at page 5, delete the next to last paragraph on the page.
  - b. In Enclosure 1 of the review package, at page 5 under Schedule, delete the second sentence, and modify the first sentence to read as follows:

"The proposed schedule for resolution allows 180 days for licensee response."
  - c. In revised Enclosure 2 of the review package, at page 1 of the draft (GI-48/GI-49) Generic Letter, revise the third paragraph on the page to read as follows:

"We require pursuant to 10 CFR 50.54(f) and Section 182 of the Atomic Energy Act that you provide the NRC with certification within 180 days of the date of this letter that either appropriate procedures are in place or justification has been prepared demonstrating that such procedures are not needed. Guidance for procedures acceptable to the NRC staff is provided in the Attachment to this generic letter. The required certification shall be submitted to NRC, signed under oath and affirmation. Supporting documentation shall be retained by licensees in accordance with the document retention program at their respective facilities."

- d. In revised Enclosure 2 of the review package, at page 3 of the Attachment to the (GI-48/GI-49) Generic Letter, change the heading "REQUIREMENT" to "RECOMMENDED ACTIONS"; and delete the last sentence of the paragraph immediately preceding subsection 2 on that page.
- e. In revised Enclosure 2 of the review package, at page 4 of the Attachment to the (GI-48/GI-49) Generic Letter, delete the last sentence on the page.
- f. In Enclosure 5 of the review package, at page 1 of the draft (GI A-30) Generic Letter, change the fourth sentence of the first paragraph to read as follows:
- "As a result of their evaluation, the NRC staff believes that certain maintenance, surveillance and monitoring provisions are appropriate for safety-related systems."
- g. In Enclosure 5 of the review package, at page 1 of the draft (GI A-30) Generic Letter, change the first sentence of the second paragraph to read as follows:
- "In order to determine whether any further staff actions are necessary at your plant, we require, pursuant to 10 CFR 50.54(f) and Section 182 of the Atomic Energy Act, that you provide...."
- h. In Enclosure 5 of the review package, at page 1 of the Attachment to the (GI A-30) Generic Letter, delete the word "adequately" in the last sentence of the second paragraph, and replace the second sentence of the third paragraph with the following parenthetical insert:
- "(provide the indicated information for each unit at each site):
- Then delete the heading "Questions" and the sentence immediately following beginning "Licensees are requested..."
- i. In Enclosure 5 of the review package, at page 2 of the Attachment to the (GI A-30) Generic Letter, insert the following after Question 6.b.:
- "NOTE: If this facility has provisions for maintenance and surveillance equivalent to those found in the Westinghouse and Combustion Engineering Standard Technical Specifications, then Questions 7 and 8 may be skipped and a statement to that effect may be inserted here."

GI-128  
ELECTRICAL POWER RELIABILITY

PRESENTATION TO CRGR  
OF THE  
RESOLUTION OF GI-128

MAY 24, 1989

D. F. THATCHER, TASK MANAGER  
R. L. BAER, BRANCH CHIEF  
R. W. HOUSTON, DIRECTOR  
DIVISION OF SAFETY ISSUE RESOLUTION  
OFFICE OF NUCLEAR REGULATORY RESEARCH

## GI 128 INTRODUCTION

- o INTEGRATION OF EXISTING ISSUES RELATED TO ELECTRICAL POWER
  - GI 48 "LCOs FOR CLASS 1E VITAL INSTRUMENT BUSES IN OPERATING REACTORS"
  - GI 49 "INTERLOCKS AND LCOs FOR REDUNDANT CLASS 1E TIE BREAKERS"
  - GI A-30 "ADEQUACY OF SAFETY-RELATED DC SUPPLIES"
  
- o INTEGRATED PROGRAM BECAUSE OF INTERRELATIONSHIPS
  - VITAL AC INSTRUMENT BUSES (48) AND DC SUPPLIES (A-30) CAN USE TIE BREAKERS (49)
  - DC POWER SUPPLIES (A-30) FEED THE VITAL INSTRUMENT BUSES (48)
  
- o RELATIONSHIPS TO OTHER ISSUES
  - USI A-44
  - USI A-17
  - USI A-47

## GI 48 BACKGROUND

- o VITAL AC INSTRUMENT BUSES ARE DESIGNED TO SUPPLY CONTINUOUS AC POWER TO CRITICAL ELECTRICAL DEVICES SUCH AS:
  - CONTROL SYSTEMS
  - INSTRUMENTATION
  - SAFETY SYSTEM LOGIC
  
- o TYPICAL PLANTS INCLUDE MORE THAN ONE BUS TO MEET SINGLE FAILURE
  
- o POWER SOURCES TO THE BUSES INCLUDE:
  - INVERTERS (OR OTHER DEVICES) WHICH CONVERT ONSITE DC TO AC (USUALLY CONSIDERED THE PREFERRED SOURCE BECAUSE IT IS NOT SUBJECT TO INTERRUPTION ON PLANT TRIPS OR LOSS OF OFFSITE POWER)
  
  - REGULATED TRANSFORMERS FED FROM NORMAL AC POWER (OFFSITE AND HOUSE POWER)
  
- o WITH VITAL BUSES OR THEIR INVERTERS UNAVAILABLE, TRANSIENTS INVOLVING POWER LOSSES COULD LEAD TO SAFETY SIGNIFICANT EVENTS

### GI 49 BACKGROUND

- o ELECTRICAL BUSES (BOTH AC AND DC. MAY CONTAIN INTERCONNECTIONS (TIE BREAKERS) FOR SPECIAL OPERATING CONDITIONS
  
- o CROSSTIE CAPABILITY MAY EXIST BETWEEN REDUNDANT SAFETY-RELATED BUSES OR BETWEEN MULTIPLE UNITS AT ONE SITE
  
- o WHILE THESE CROSSTIES CAN PROVIDE FLEXIBILITY, THEY CAN COMPROMISE THE INDEPENDENCE OF SAFETY-RELATED ELECTRICAL DIVISIONS



GI 48 AND 49 SAFETY CONCERN

- o LOSS OF AC AND DC ELECTRICAL POWER CAN LEAD TO:
  - TRANSIENTS VIA CONTROL SYSTEMS
  - LOSS OF INFORMATION TO OPERATOR
  - LOSS OF REDUNDANCY IN SAFETY SYSTEMS
  
- o SOME PLANTS DO NOT HAVE TECHNICAL SPECIFICATION RESTRICTIONS ON CONTINUED PLANT OPERATION WITH VITAL AC POWER BUSES (OR THEIR SOURCES) UNAVAILABLE
  
- o SOME PLANTS DO NOT HAVE TECHNICAL SPECIFICATION RESTRICTIONS ON CONTINUED OPERATION WITH TIE BREAKERS CLOSED
  
- o WITHOUT ADEQUATE CONTROLS, PLANTS COULD BE OPERATING INDEFINITELY IN SITUATIONS WHICH COMPROMISE PRESUMED DIVISIONAL REDUNDANCY AND INDEPENDENCE

GI 48/49 RESOLUTION

- o TO PREVENT OPERATION IN SITUATIONS WHICH COULD DEGRADE THE INDEPENDENCE OF SAFETY RELATED ELECTRICAL EQUIPMENT, TECHNICAL SPECIFICATIONS AND SUPPORTING PROCEDURES SHOULD BE INCLUDED AT ALL PLANTS
  
- o TO CONFIRM COMPLIANCE WITH THESE EXISTING REQUIREMENTS A 50.54(F) REQUEST IS PROPOSED TO:
  - VERIFY THAT THE TECH SPECS INCLUDE APPROPRIATE PROVISIONS AND
  
  - VERIFY THAT PLANT PROCEDURES INCLUDE CORRESPONDING CONTROLS
  
- o BECAUSE ELECTRICAL DISTRIBUTION SYSTEMS ARE VERY PLANT SPECIFIC, A BASIS FOR NOT NEEDING SUCH PROVISIONS MAY BE JUSTIFIED AT SOME PLANTS.

MODIFICATION TO IMPLEMENTATION  
OF GI 48 AND 49

- o NO LONGER REQUIRE TECHNICAL SPECIFICATION ADDITIONS
  
- o REQUIRE PLANTS TO CERTIFY:
  - HAVE PROCEDURES, OR
  
  - HAVE ESTABLISHED BASES FOR NOT INCLUDING THEM
  
- o ONLY A CERTIFICATION, WITH POSSIBLE FUTURE NRC INSPECTION/AUDIT
  
- o NRC RESOURCES GOES DOWN FROM 100 MAN-WEEKS TO MINIMAL TIME

## GI A-30 BACKGROUND

- o SAFETY-RELATED DC POWER SUPPLIES ARE DESIGNED TO PROVIDE AN ONSITE SOURCE OF RELIABLE ELECTRICAL POWER FOR
  - FEED TO VITAL AC EQUIPMENT
  - ELECTRICAL BREAKER CONTROL
  - CONTROL SYSTEMS
  
- o TYPICAL PLANTS INCLUDE MORE THAN ONE SAFETY-RELATED DC SOURCE TO MEET SINGLE FAILURE
  
- o POWER SOURCES TO DC BUSES INCLUDE BATTERIES AND BATTERY CHARGER
  
- o ALTHOUGH SAFETY RELATED DC SYSTEMS ARE DESIGNED TO BE HIGHLY RELIABLE, SOME FAILURES HAVE BEEN IDENTIFIED
  
- o MOST FAILURES OF CONCERN INVOLVE COMMON CAUSE PROBLEMS AND FAILURE TO ADEQUATELY DETECT THE EXISTENCE OF BATTERY-RELATED PROBLEMS

### GI A-30 SAFETY CONCERN

- o LOSS OF DC SUPPLIES CAN LEAD TO
  - TRANSIENTS
  - LOSS OF INFORMATION TO OPERATORS
  - LOSS OF SAFETY SYSTEMS
  
- o SOME PLANTS MAY NOT INCLUDE RECOMMENDED PRACTICES IN AREAS OF TESTING, MAINTENANCE AND MONITORING
  
- o IMPROVEMENTS AT INDIVIDUAL PLANTS MAY BE NECESSARY

GI A-30 RESOLUTION

TO IMPROVE DC POWER SYSTEM PERFORMANCE THE STAFF DEVELOPED A NUMBER OF RECOMMENDATIONS FOR IMPROVEMENTS IN

- MAINTENANCE
- TESTING
- MONITORING

INDUSTRY (THROUGH INPO, NSAC, AND IEEE) HAS ALSO ADDRESSED IMPROVEMENTS IN THESE AREAS

TO GATHER INFORMATION TO CONFIRM THAT UTILITIES HAVE IMPLEMENTED THESE IMPROVEMENTS, A 50.54(F) REQUEST IS PROPOSED TO:

- QUESTION PLANTS ABOUT THESE IMPROVEMENTS
- IF IMPROVEMENTS HAVE NOT BEEN MADE, QUESTION THEIR BASES FOR NOT INCLUDING THEM



S A F E T Y I S S U E S M A N A G E M E N T S Y S T E M  
S A F E T Y I S S U E L E V E L I N F O R M A T I O N

ISSUE NUMBER: 128 TITLE: ELECTRICAL POWER RELIABILITY  
CONTACT: D. THATCHER TYPE: GSI IDENTIFYING ORGANIZATION: NRR STATUS: SPONSORING OFFICE: RES  
PRIORITY: H TYPE OF REACTORS AFFECTED: All OTHER:  
PENDENT ISSUES: 48, 49 and 50

DESCRIPTION

SOLUTION (NEAR AND LONG TERM)

\*\*\* NO DESCRIPTION TEXT FOR ISSUE \*\*\*

*See attached*

\*\*\* NO SOLUTION TEXT FOR ISSUE \*\*\*

*See attached*

NET CHANGE IN DOLLAR COST

POINT ESTIMATE      RANGE  
                            LOW      HIGH

NRC DEVELOPMENT. . . . .  
NRC (IMPLEMENTATION/IMPOSITION). . . . .  
NRC (ASSURE CONTINUED COMPLIANCE). . . . .  
PUBLIC/INDUSTRY/OTHER (IMPLEMENTATION) . . . . .  
PUBLIC/INDUSTRY/OTHER (CONTINUED COMPLIANCE)

\*\*\* NONE AVAILABLE \*\*\*  
\*\*\* NONE AVAILABLE \*\*\*  
\*\*\* NONE AVAILABLE \*\*\*  
\*\*\* NONE AVAILABLE \*\*\*  
\*\*\* NONE AVAILABLE \*\*\*

NET CHANGES IN BENEFITS

PUBLIC EXPOSURE. . . . .  
OCCUPATIONAL EXPOSURE. . . . .  
CORE MELT FREQUENCY. . . . .

\*\*\* NONE AVAILABLE \*\*\*  
\*\*\* NONE AVAILABLE \*\*\*  
\*\*\* NONE AVAILABLE \*\*\*

*Not applicable  
see resolution*

~~DISCONTINUED~~

A number of generic safety issues in the area of electric power systems have been identified ~~over a period of years~~. These ~~issues are listed and prioritized in NUREG-0933.~~<sup>1</sup> Three issues have been selected for ~~integrated action~~<sup>ign</sup> because they are interrelated. These are:

- Generic Issue A-30 "Adequacy of Safety-related DC Supplies"
- Generic Issue 48 "LCOs for Class 1E Vital Instrument Buses in Operating Reactors"
- Generic Issue 49 "Interlocks and LCOs for Redundant Class 1E Tie Breakers"

These three issues taken together are identified as Generic Issue 128.

GI 48 "LCOs for Class 1E Vital Instrument Buses" deals with a safety concern that some operating nuclear power plants do not have administrative controls or technical specifications governing operational restrictions for their Class 1E 120 Vac vital instrument buses and associated inverters.

Without such restrictions, the normal or alternate power sources for one or more VIBs could be out of service indefinitely. This could place certain safety systems in a situation where they could not meet the plant safety design basis, including the loss of off-site power or the single failure criterion.

GI 49 "Interlocks and LCOs for Class 1E Tie Breakers" involves a safety concern that independent, redundant Class 1E ac or dc buses can be interconnected via tie breakers which are left closed by mistake. When left closed, the tie breakers can compromise the independence of the redundant safety-related buses and, in some cases, may prevent loading of the emergency diesel generator.

GI A-30 "Adequacy of Safety Related DC Power Supplies" deals with a safety concern that some plants may not have adequate provisions for assuring that these power supplies are available and capable of performing their function.

Safety-related dc power is used for the overall operation of the safety-related portions of the electrical system including circuit breaker control for the ac power. It is typically also a source of vital ac power (via the vital inverters) for safety-related instrumentation and logic systems as well as operator indications. During normal operation, the battery chargers supply the load requirements and maintain the batteries fully charged to be available during loss of offsite power. For a loss of offsite power event, battery power is particularly important during the time period when the diesel generators are starting and immediately thereafter, because the circuit breaker control to sequence loads and the excitation of the generator field windings is entirely dependent on dc power.

SOLUTION

is proposing

~~SPUDUUCU~~  
For GI 48 and 49

The staff ~~proposes~~ to submit an Information Request to all licensees to identify plants that should develop additional administrative control to avoid operating under conditions that are in violation of the single failure criterion. The licensee's responses are expected to identify plants in which further action may be necessary. In most cases it is expected that licensees will voluntarily take appropriate actions without specific direction from the staff.

The proposed resolution of GI A-30 involves a number of recommended provisions for tests and maintenance and a number of provisions for monitoring the dc power supply status. Many of these provisions may have already been implemented at a large number of plants.

is proposing

The staff ~~believes~~ that the most cost-effective approach to resolve the A-30 issue is for the staff to request certain information from all plants (pursuant to 10 CFR 50.54(f)) in order that the NRC can establish that adequate measures have been or will be taken at all facilities. ~~Only a portion of the measures would be reflected in a plant's technical specifications.~~ The responses may indicate that in some cases improvements in dc system surveillance, maintenance and procedures are necessary.

S A F E T Y I S S U E S M A N A G E M E N T S Y S T E M  
 SAFETY ISSUE LEVEL INFORMATION

ISSUE NUMBER: 128

TITLE: ELECTRICAL POWER RELIABILITY

1. ISSUE APPROVAL AND PLANNING:

ISSUE APPROVAL DATE: \*\*\*\*\*

2. TECHNICAL RESOLUTION:

LEAD OFFICE: RES SUPPORTING OFFICE(S):

INITIATION DATE: \*\*\*\*\*

INTER OFFICE REVIEW/COORDINATION COMPLETION DATE: \*\*\*\*\*

PROPOSED SOLUTIONS/REQUIREMENTS APPROVAL BY OFFICE DIRECTOR DATE: \*\*\*\*\*

3. REQUIREMENTS REVIEW AND APPROVAL:

INITIAL CRGR REVIEW DATE: \*\*\*\*\*

RESOLVED WITH REQUIREMENTS:

RESOLUTION DATE: 12/89

FORM. . . . .	<u>R U L E M A K I N G</u>			<u>OTHER (SPECIFY)</u>
	ANPR	PROPOSED	FINAL	
OFFICE RESPONSIBLE. . . . .	*	*	*	TBD Generic Letters
EDO APPROVAL TO PROCEED (YES/NO)	*	*	*	RES
CRGR REVIEW DATE. . . . .	*	*	*	*** NO 05/89 <del>09/88</del> 06/89 <del>09/88</del>
ACRS REVIEW DATE. . . . .	N	N	N	10/89
EDO REVIEW DATE . . . . .	O	O	O	***
APPROVAL (YES/NO). . . . .	N	N	N	*****
COMMISSION REVIEW DATE. . . . .	E	E	E	***
APPROVAL (YES/NO). . . . .	*	*	*	*****
PUBLIC COMMENT DATE . . . . .	*	*	*	*****
FINAL APPROVAL AND ISSUANCE DATE	*	*	*	12/89

4. REQUIREMENTS IMPOSITION NEEDED FOR VERIFICATION:

A. IMPOSITION - LICENSED PLANTS:

MULTIPLANT ACTION CODE: TBD after generic letter issued

OTHER:

APPROVAL OF LICENSEE PROPOSAL NEEDED (YES/NO): yes, for Tech. Spec. changes

SAFETY ISSUES MANAGEMENT SYSTEM

SAFETY ISSUE LEVEL INFORMATION

ISSUE NUMBER: 128

TITLE: ELECTRICAL POWER RELIABILITY

B. IMPOSITION - PLANTS NOT LICENSED: SRP REVIEW PROCESS: jc OTHER (SPECIFY):

C. IMPOSITION - ALL PLANTS: jc OFFICE RESPONSIBLE: NRR

D. NEED FOR VERIFICATION:

NEEDED (YES/NO) OFFICE RESPONSIBLE
VERIFICATION. . . . . - yes --NRR

MPA VERIFICATION PRIORITY:

5. REQUIREMENTS IMPLEMENTATION BY LICENSEE AND VERIFICATION BY NRC:

Table with 3 columns: Requirement, Completion Status (Plants), Date of Last Plant. Rows include IMPOSITION, IMPLEMENTATION, and VERIFICATION, all showing 0 of 0 and \*\*\*\*\*.

REQUIREMENTS IMPLEMENTATION BY STAFF:

A. STAFF REQUIREMENTS -- N O N E

COMPLETION DATE: \*\*\*\*\* OFFICE(S) RESPONSIBLE:

B. ROUTINE INSPECTION PROGRAM MODIFICATIONS: jc MODIFICATIONS NEEDED (YES/NO): MODIFICATION COMPLETION DATE: \*\*\*\*\*

MODIFICATION TEXT

\*\*\* NO MODIFICATION TEXT FOR ISSUE \*\*\*

S A F E T Y I S S U E S M A N A G E M E N T S Y S T E M  
P L A N T L E V E L I N F O R M A T I O N

ISSUE NUMBER: 128

TITLE: ELECTRICAL POWER RELIABILITY

PLANT	DOCKET #	DOCKET PRIORITY	REACTOR TYPE	OL ISSUE	OL EXPIR	IMPOS MANAGE METHOD	IMPOS INIT	IMPOS COMPLET	IMPLEM COMPLET	VERIFY COMPLET
-------	----------	--------------------	-----------------	-------------	-------------	---------------------------	---------------	------------------	-------------------	-------------------

\*\*\* NO PLANT DATA FOR ISSUE \*\*\*



ENCLOSURE 2 (Revision 5/23/89)

Enclosure

DRAFT GENERIC LETTER

To: ALL HOLDERS OF OPERATING LICENSES

SUBJECT: RESOLUTION OF GENERIC ISSUES GI-48, "LCOS FOR CLASS 1E VITAL INSTRUMENT BUSES," AND GI-49, "INTERLOCKS AND LCOS FOR CLASS 1E TIE BREAKERS"

The NRC staff has completed the evaluation of Generic Issues GI-48 and GI-49, which focus on vital ac buses and tie breakers between redundant, safety-related buses. Attachment 1 provides a brief description and history of each of these GIs. Additional details are provided in reference 1.

As a result of our evaluation, the staff concludes that all licensees should include appropriate ~~Limiting-Conditions-for-Operation-(LCOs)-in-their-Technical-Specifications-and-have-proper-administrative-controls-to-implement-these-Technical-Specifications~~ procedures to limit the length of time that a plant is in potential violation of the single failure criterion with regard to the Class 1E vital instrument buses and tie breakers unless there is adequate justification why such provisions are not needed at their specific facilities.

~~In-order-to-determine-whether-any-further-staff-actions-are-necessary-to-assure-implementation-of-recommended-corrective-measures,~~ We request pursuant to 10 CFR 50.54(f) and Section 182 of the Atomic Energy Act that you provide the NRC with certification, within 90 days of the date of this letter, that either the appropriate procedures (in accordance with the enclosed requirements in the attachment to this generic letter) are in place or justification has been prepared demonstrating that such procedures are not needed. This certification should be submitted to NRC, signed under oath and affirmation. The procedures may be subject to future NRC inspection. Any justifications for not including such procedures should be retained onsite for possible future NRC audit. ~~a-response-to-the-questions-in-the-attachment-within-180-days-of-the-date-of-this-letter.--This-information-should-be-submitted-to-NRC, signed-under-oath-and-affirmation.--The-information-will-enable-the-Commission-to-determine-whether-any-further-action-should-be-taken-on-your-license.~~

This request is covered by Office of Management and Budget Clearance Number 3150-0011, which expires December 31, 1989. The estimated average burden hours is 100 man-hours per licensee response, including assessment of the recommendations, searching data sources, gathering and analyzing the data, and preparing the required responses certifications. These estimated average burden hours pertain only to these identified response related matters and do not include time for actual implementation of any related actions. Comments on the accuracy of this estimate and suggestions to reduce the burden may be directed to the Office of Management and Budget, Room 3208, New Executive Office Building, Washington, D.C. 20503, and to the U. S. Nuclear Regulatory Commission, Records and Reports Management Branch, Office of Administration and Resources Management, Washington, D.C. 20555.

If you have any questions, please contact your project manager.

Sincerely,

Attachment: 10 CFR 50.54(f) Request - GI-48, "LCOs for Class 1E Vital Instrument Buses," GI-49, "Interlocks and LCOs for Class 1E Tie Breakers"

Reference: EGG-NTA-7727 Revision 3  
"Technical Findings for Proposed Integrated Resolution of Generic Issue 128 (Issue 48 and Issue 49)

10 CFR 50.54(f) Request  
GI-48, "LCOs for Class 1E Vital Instrument Buses"  
GI-49, "Interlocks and LCOs for Class 1E Tie Breakers"

INTRODUCTION

The designation "Vital Instrument Bus" may be interpreted differently for different plants. In this document, the term "Vital Instrument Buses" refers to the ac buses that provide power for the Instrumentation and Controls of the Engineered Safety Features (ESF) Systems and the Reactor Protection System (RPS) and are designed to provide continuous power during postulated events including the loss of normal offsite power. Tie breakers are devices used to cross connect either redundant class 1E buses in one unit or Class 1E buses in different units at the same site.

The NRC staff has evaluated the concerns of generic issue GI-48, "LCOs for Class 1E Vital Instrument Buses," and GI-49, "Interlocks and LCOs for Class 1E Tie Breakers." The staff has concluded that these concerns can be generally resolved by the verification or implementation of appropriate ~~limiting-conditions-of-operations-(LCOs)-in-the-plant-technical-specifications-and-by-inclusion-of~~ associated administrative controls in plant procedures for the Class 1E buses and tie breakers. For both issues, the primary objective is to verify that plants are not being operated in violation of the design criteria of 10 CFR 50 Appendix A, for example, GDC 17, 21, 34, and 35. Conditions identified by the staff evaluation suggested a strong possibility that the single failure criterion may be violated for substantial time periods in some plants. These plants, therefore, may not meet the requirements of the design basis events considered in the plant safety analysis report.

BACKGROUND

The primary concern of GI-48 was identified when it was found that some operating nuclear power plants do not have any administrative controls or technical specifications governing operational restrictions for their Class 1E 120V ac Vital Instrument Buses (VIBs) and associated inverters. Without such restrictions, the normal or alternate power sources for one or more VIBs could be out of service indefinitely. This could place certain safety systems in a situation where they could not meet the plant design basis, including loss of off-site power or the single failure criterion.

Specifically, the VIBs may be subjected to power failure modes that may not have been considered during the safety analysis of the plant. For example, this situation could occur as a result of removing one or more of the normal or alternate power sources for the VIBs from service for repair or maintenance. Without some type of restrictions, more than one VIB could be connected to an offsite alternate power source. The loss of the alternate power source would then cause the simultaneous loss of more than one VIB, at least until the diesel generators pick up the loads.

The concerns of GI-49 were raised by an incident that occurred at the Point Beach Unit 2 plant. On June 9, 1980 it was discovered that a tie breaker between

the safeguards buses at the plant was improperly left closed after a plant shutdown. The improper electrical lineup probably occurred after a loss of ac power test that was conducted on May 2, 1980 and was attributed to personnel error.

This concern is limited to manually actuated tie breakers that have the capability of connecting either nominally independent, redundant Class 1E ac or dc buses at one unit or Class 1E buses in different units at the same site. These tie breakers permit convenient maintenance of supply buses and equipment without de-energizing plant equipment. The maintenance is normally conducted when the plant is not in operation. These tie breakers require special consideration, because, when closed, they can compromise the independence of the redundant safety-related buses and, in some cases, may prevent loading of the emergency diesel generator. It is also recognized that the tie breakers could be beneficial under very special conditions (such as loss of off-site power coincident with loss of a diesel or batteries) to provide flexibility to supply power across division boundaries.

Approximately 5 weeks elapsed before the improper closure at the Point Beach plant was discovered. With the two breakers closed, the two redundant buses were connected; and, consequently, the independence of the buses was lost. If there had been a loss of off-site ac power with the tie breaker closed, interlocks would have prevented automatic closure of the diesel generator output breakers.

The event at Point Beach was subsequently evaluated by the NRC staff, resulting in the identification of the generic concerns of GI-49 regarding procedural controls to reduce human error of the type that occurred at Point Beach. The staff also noted that the tie breaker interlocks to prevent manual paralleling of standby power sources, which are a provision of Regulatory Guide (RG) 1.6, Item 4(d), had not been implemented at the Point Beach plant.

It should be noted that the proposed resolution does not include a recommendation regarding the verification of tie breaker interlocks. The interlocks raised as a concern were to help protect against the potential for an operator committing an error and inadvertently closing a tie breaker between either:

- (1) two operating diesel generators which are potentially out-of-phase, or
- (2) an operating diesel generator and an incoming feeder line which are potentially out-of-phase.

Although such interlocks can provide an additional degree of assurance for some infrequent situations, we believe that such interlocks can also have a potential negative impact on safety. For example, in some emergency situations (such as loss of offsite power and failure or nonavailability of a divisional diesel generator, or a station blackout) an operator may need to cross connect power (via tie breakers) to an opposite division. In such instances, a failure in the interlocking circuits could inhibit the operator from taking such action. PRA analyses have shown that cross connecting can allow for options that can prove to be beneficial.



In addition, there is some protection provided for inadvertent out-of-phase connections by the normal protective relaying and breaker coordination. If the protective relaying actuates, equipment would be protected and normal restart could be undertaken. Therefore, the staff concluded that if proper administrative controls are placed on the operation of the tie breakers and normal protective relaying is present, then the addition of these interlocks would not be cost beneficial.

The GI-48 and GI-49 concerns have been resolved in recently licensed plants by implementation of Standard Technical Specifications and current licensing practice.

#### QUESTIONS REQUIREMENT

1.---Do your plant Technical Specifications include Limiting Conditions for Operations (LCOs)

Ensure that your plant procedures include time limitations and surveillance requirements for:

- a. Vital instrument buses (typically 120V ac buses),
- b. Inverters or other onsite power sources to the vital instrument buses, and
- c. Tie breakers which can connect redundant Class 1E buses (ac or dc) at one unit or which can connect Class 1E buses between units at the same site.

If such provisions are not included for any of the above items (a, b, or c), ensure that you have established the bases for such a position. This information should be retained onsite for possible future NRC audit.

2.---Do your plant procedures include appropriate corresponding administrative controls to implement these technical specification requirements?

If the answer to any of the previous questions is no, then provide an explanation of the basis for your belief that your plant will not be operated indefinitely in violation of the single failure criterion regarding the Class 1E vital instrument buses and the closure of tie breakers connecting Class 1E ac or dc buses.---This may be accomplished by either:--(a) providing information and supporting analyses, or (b) submitting an amendment request proposing that appropriate LCOs be incorporated in the plant technical specifications on the above items.

The information to be provided should demonstrate that adequate consideration has been given to loss of off-site power in conjunction with a worst case additional single failure. In conjunction with these postulations, the analysis should consider the time delay for the emergency generators to pick up load, since in typical plants, if an inverter serving a vital instrument bus is out of service, a loss of off-site power will cause numerous actuations due to the



delay time while the diesels are starting. The analysis should, therefore, also consider malfunctions that do not always have a preferred failure mode (e.g., instrumentation or controls that initiate a switch of emergency core cooling from injection to recirculation or initiate isolation of the steam generators). If the alternate power sources for the vital buses are not backed up by the diesel generators, then this should be stated.

NOTE: As part of future upgrades to Technical Specifications, licensees should consider including appropriate Limiting Conditions for Operation (LCOs) and Surveillance Requirements in future Technical Specification improvements.

An example of ~~acceptable~~ LCO and surveillance requirements (from the Westinghouse Standard Technical Specifications) is included for guidance. The staff plans to upgrade all Standard Technical Specifications to include these provisions.

Enclosure 5 to the Minutes of CRGR Meeting No. 163  
USI A-47, "Safety Implications of Control Systems  
in LWR Nuclear Power Plants"

May 24, 1989

TOPIC

R. Baer (RES) and A. Szukiewicz (RES) presented for CRGR review a proposed resolution of Unresolved Safety Issue A-47, "Safety Implications of Control Systems in LWR Nuclear Power Plants." Copies of the briefing slides used by the staff to guide their presentation and discussions with the Committee at this meeting are attached.

BACKGROUND

The package submitted by the staff was transmitted by memorandum dated April 3, 1989, E. S. Beckjord to E. L. Jordan and contained the following:

1. A proposed generic letter
2. NUREG-1217, "Safety Implications of Control Systems in LWR Nuclear Power Plants, Technical Findings Related to Unresolved Safety Issue A-47"
3. NUREG-1218, "Regulatory Analysis for Resolution of USI A-47"
4. Model SER
5. Revised STS for B&W and CE plants

CONCLUSIONS/RECOMMENDATIONS

As a result of their review of this matter, including discussions with the staff at this meeting, the Committee recommended in favor of issuing the proposed generic letter, subject to the recommendations listed below:

1. The four actions specified in the generic letter are difficult to follow in Enclosure 2 since the enclosure is oriented toward a specific reactor type; it is not clear which actions apply to which reactor type. A clarifying statement should be included in the generic letter to eliminate this potential confusion.
2. Language on page 1 of Enclosure 2 should be revised to clarify the basis for this letter, that it is a safety enhancement and has not been determined to be needed for adequate protection.
3. The generic letter needs to provide a caution against the potential for inadvertent trips in making design changes which would provide overfill protection.

4. The language on page 2 of the generic letter needs to be revised to conform with the requirements of 10 CFR 50.54f. Enclosure 2 should be identified as guidance which licensees are requested to follow. The letter should state they are required to inform the NRC of their plans. Any records to be maintained by the licensee should be in accordance with existing records retention requirements.
5. The implementation schedule should be reviewed and sufficient flexibility added to not cause an unnecessary burden on licensees. In addition, the date for licensee response to the generic letter should be extended to 180 days and adjusted to reflect due dates of other generic letters which may be issued at the same time (in particular, the other USIs reviewed at this CRGR meeting).
6. In Enclosure 2 to the generic letter, language should be made consistent regarding the actions recommended of licensees. Two phrases are currently used, recommended and requested, only one should be used.
7. Language in Enclosure 2 which discusses changes to technical specifications should be made clear that changes are not required in response to this generic letter, and that licensees will only be encouraged to revise their tech specs.

As a collateral recommendation, the Committee recommended that NRR act to improve the mailing of generic letters to eliminate unnecessary delays in licensees' receipt of generic letters. This was prompted by information of up to a six-week transit time for the SPDS generic letter, and statements by licensees that three weeks is the standard delay between issuance and receipt.

USI A-47  
SAFETY IMPLICATIONS OF CONTROL SYSTEMS

PRESENTATION TO CRGR  
OF THE  
FINAL RESOLUTION OF USI A-47

MAY 24, 1989

A. J. SZUKIEWICZ, TASK MANAGER  
R. L. BAER, BRANCH CHIEF  
R. W. HOUSTON, DIRECTOR  
DIVISION OF SAFETY ISSUE RESOLUTION  
OFFICE OF NUCLEAR REGULATORY RESEARCH

ATTACHMENT  
TO ENCLOSURE

USI A-47  
MILESTONES

COMMENTS ON DRAFT PROPOSED RESOLUTION  
BY CRGR DECEMBER 1987

CRGR RECOMMENDED PUBLICATION OF DRAFT  
RESOLUTION MAY 1988

DRAFT RESOLUTION PACKAGE ISSUED  
FOR PUBLIC COMMENT MAY 1988

PUBLIC COMMENT PERIOD JUNE-SEPT, 1988

FINAL RESOLUTION PACKAGE ISSUED FOR  
REVIEW DECEMBER 1988

OTHER OFFICES CONCUR WITH FINAL  
PACKAGE MARCH 1989

FINAL PACKAGE SUBMITTED TO CRGR APRIL 1989

FINAL PACKAGE SUBMITTED TO ACRS APRIL 1989

ISSUE FINAL PACKAGE AUGUST 1989

## PUBLIC COMMENTS

- o 37 PUBLIC COMMENTS RECEIVED
- o RESPONSES TO COMMENTS PROVIDED IN NUREG-1217 APPENDIX C
- o MOST COMMENTS RESULTED IN EDITORIAL CHANGES - PROVIDING CLARIFICATION
- o SOME UTILITIES OBJECT TO HAVING PERIODIC VERIFICATION OF OVERFILL PROTECTION INCLUDED IN THE TECH. SPECS.
- o CALVERT CLIFFS INDICATED THAT THE STAFF'S COST ESTIMATES WERE LOW BY FACTOR OF 2



## SUMMARY OF FINAL RESOLUTION

LIMITED NUMBER OF REQUESTED ACTIONS PER 10CFR50.54(F)

- o PROVIDE ALL LICENSEES WITH RESULTS OF ANALYSIS CONDUCTED BY STAFF - FOR INFORMATION
- o REQUEST OVERFILL PROTECTION (ALL PLANTS)
- o REQUEST PERIODIC VERIFICATION OF OVERFILL PROTECTION (TECH SPECS)
- o IMPROVE AUTOMATIC INITIATION OF EFW ON LOSS OF POWER TO CONTROL SYSTEMS (OCONEE ONLY)
- o IMPROVE EMERGENCY PROCEDURES FOR SBLOCA (CE PLANTS WITH LOW HEAD PUMPS)

MODIFICATIONS TO THE  
PROPOSED RESOLUTION

- o FINAL RESOLUTION ESSENTIALLY THE SAME AS PROPOSED IN THE DRAFT (FOR COMMENT) PACKAGE
  
- o ALTERNATIVE CORRECTIVE ACTIONS TO AVOID STEAM GENERATOR DRYOUT ON LOSS OF POWER TO CONTROL SYSTEMS HAVE BEEN ADDED TO THE GENERIC LETTER - FOR OCONEE PLANTS
  
- o REQUESTS TO SUBMIT PLANT DESIGN MODIFICATIONS FOR NRC REVIEW WERE DELETED. LICENSEES ARE NOW REQUESTED TO RETAIN ON SITE, THE DOCUMENTATION ASSOCIATED WITH THE REQUESTED ACTIONS FOR POSSIBLE FUTURE INSPECTION (EXCEPT FOR TECH. SPEC. MODIFICATIONS)



UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
WASHINGTON, D. C. 20555

MAY 10 1989

MEMORANDUM FOR: Edward L. Jordan, Chairman  
Committee to Review Generic Requirements

FROM: Eric S. Beckjord, Director  
Office of Nuclear Regulatory Research

SUBJECT: CRGR REVIEW OF THE FINAL RESOLUTION OF USI A-17, "SYSTEMS  
INTERACTIONS IN NUCLEAR POWER PLANTS"

Attached is the final resolution of USI A-17 for your consideration.

The previous version of the A-17 resolution was forwarded to you on September 2, 1988. That resolution addressed your comments from the "Minutes of CRGR Meeting 139" regarding internal flooding and water intrusion. You recommended approval of those changes in your memorandum of October 20, 1988. On November 23, 1988, the staff issued Generic Letter 88-20 on Individual Plant Examinations (IPE), which directed licensees to include flooding from internal water sources in their analyses.

Guidance to licensees on the content of IPE submittals is now being completed. The insights on flooding and water intrusion from internal plant sources developed as part of A-17 will be provided for licensees' use. No additional work by licensees is intended outside the scope of the planned IPE effort. With this action, the internal flooding and water intrusion portion of USI A-17 is considered resolved.

We plan to issue a generic letter to inform licensees and applicants of the resolution of A-17 and to provide the information which form the basis for the resolution. We do not plan to seek public comment. Rather, we are (1) proposing to inform the Commissioners via the enclosed Commission Paper; (2) publishing NUREG-1174 and NUREG-1229; (3) publishing the Federal Register Notice in the Federal Register; (4) informing the various Congressional committees and (5) having NRR issue the generic letter for information only.

NRR and AEOD have concurred in these changes. OGC has no legal objection.

We would appreciate your prompt consideration of this matter. Please inform us if the CRGR wishes to have another meeting to discuss the changes we made to the resolution.

A handwritten signature in dark ink, appearing to read "Eric S. Beckjord".

Eric S. Beckjord, Director  
Office of Nuclear Regulatory Research

Enclosures: See following page

~~9004120024~~

Edward L. Jordan

2

Enclosures:

1. Draft Commission Paper with 3 enclosures:
  - (1) NUREG-1174
  - (2) NUREG-1229
  - (3) Federal Register Notice and Summary Statement
2. Proposed Generic Letter with 2 attachments

cc: T. Murley  
F. Gillespie  
S. Lewis  
J. Conran

DRAFT COMMISSION PAPER

For: The Commissioners

From: Victor Stello, Jr.  
Executive Director for Operations

Subject: UNRESOLVED SAFETY ISSUE A-17, "SYSTEMS INTERACTIONS IN NUCLEAR POWER PLANTS"

Purpose: To inform the Commissioners of the staff plans for the final resolution of USI A-17

Summary: The staff has completed its technical work on USI A-17 and has developed a proposed resolution. The technical findings and proposed resolution are documented in NUREG-1174, "Evaluation of Systems Interactions in Nuclear Power Plants - Technical Findings Related to USI A-17" (Enclosure 1), and NUREG-1229, "Regulatory Analysis for Proposed Resolution of USI A-17: (Enclosure 2). The staff concluded from its A-17 investigations that certain actions should be taken by the NRC and licensees.

These actions include guidance to the staff for use in severe accident policy implementation and probabilistic risk assessment (PRA) review and development, and general insights and lessons learned for licensees' use in evaluating operating experience. The resolution also includes more specific insights regarding flooding (including water intrusion) vulnerabilities from plant internal sources. It is expected that these insights will be considered by licensees in performing the Individual Plant Examinations (IPEs).

The staff concluded that certain older plants should perform seismic system interaction reviews. However, these reviews are required to be performed as a part of the USI A-46 implementation; therefore, a separate action under USI A-17 is not proposed.

Discussion: Nuclear power plants contain many structures, systems, and components (SSCs), some of which are safety-related. Certain SSCs are designed to interact to perform their intended functions.

Contact:  
D. Thatcher, RES  
492-3935

These "systems interactions" are usually well recognized and therefore accounted for in the evaluation of plant safety by the designers and by those who assess plant safety.

A number of significant, plant-specific events have involved unintended or unrecognized dependencies among the SSCs. Some of these events have involved subtle dependencies between safety-related SSCs and other SSCs. Some events have also involved subtle dependencies between redundant safety-related SSCs that were believed to be independent.

Therefore, the purpose of USI A-17 was to investigate the potential that unrecognized, subtle dependencies among SSCs have remained hidden and that they could lead to safety-significant events. The term used to describe these unrecognized, subtle dependencies is adverse systems interactions (ASIs).

NUREG-1174, "Evaluation of Systems Interactions in Nuclear Power Plants: Technical Findings Related to Unresolved Safety Issue A-17," summarizes the technical work supporting the resolution of USI A-17. NUREG-1229, "Regulatory Analysis for Resolution of USI A-17: Systems Interactions in Nuclear Power Plants," provides a discussion of the alternatives considered and the deterministic and probabilistic arguments that led to the resolution. The resolution is not recommending that licensees conduct further broad searches specifically to identify all ASIs, because such searches have not proved to be cost effective in the past, and there is no guarantee after such a study that all ASIs have been uncovered. Rather, in its study of A-17, the staff has concluded that certain more specific actions, together with other ongoing activities, could reduce the risk from adverse systems interactions.

The staff has concluded from its A-17 investigations that the following actions should be taken:

- (1) Issuance of a generic letter that includes:
  - (a) the bases for resolution of USI A-17,
  - (b) a summary of information for use in ongoing operating experience reviews.
- (2) Recognition that Individual Plant Examinations (IPE) already include evaluation of internal flooding and the A-17 insights will be referenced in the IPE guidance documents.
- (3) Recognition that the USI A-46 implementation will address seismically induced systems interactions to



verify that components and systems needed to safely shut down the plant are protected, given loss of offsite power. (New plants, not covered by A-46, have been reviewed to current requirements that address seismically induced systems interactions.)

- (4) Communication of information regarding ASIs for staff review of PRAs and for staff evaluation of electric power supplies as part of GI-128, "Electric Power Reliability."
- (5) Identification and definition of concerns related to A-17 and other programs that have not been specifically addressed in this or in other generic issues. (RES has established the Multiple System Responses Program at Oak Ridge National Laboratory. The objective of this program is to define the concerns with sufficient specificity to permit them to be prioritized as potential generic safety issues.)
- (6) Development of a Standard Review Plan for future plants that would include guidance regarding protection from internal flooding and water intrusion events. (This would be done by NRR at a future time.)

The Advisory Committee on Reactor Safeguards (ACRS) has taken an active interest in this USI since its beginning. In fact, the ACRS raised the first concern with "systems interactions" in about 1974 with regard to the concept of standardized plants. The staff has had many discussions with ACRS, and the committee has written a number of letters on the subject. The ACRS provided the Commission with their latest comments on the proposed resolution to USI A-17 in a letter to Chairman Zech, dated August 16, 1988. The ACRS acknowledged that, since the systems interactions issue is so comprehensive, it is unlikely that it will ever be "resolved" in the sense that all ASIs will be found and corrected. They concluded that the proposed resolution of USI A-17 would represent a useful step in the direction of reducing plant risk due to ASIs and recommended that the proposed resolution be issued for public comment.

That proposed resolution was concurred in by NRR, OGC, and AEOD and discussed at Meeting Nos. 88 and 139 of the Committee to Review Generic Requirements (CRGR). At the conclusion of the later meeting, CRGR recommended that the staff make a number of modifications to the package related to the flooding and water intrusion actions and provide the revised package to the CRGR staff. By memorandum dated October 20, 1988, the CRGR agreed that the comments had been adequately addressed and the resolution could be issued for public comment.



Subsequently, however, the staff has concluded that a different method of implementation of the proposed resolution would be more efficient for licensees to evaluate the safety concerns associated with flooding and water intrusion from internal plant sources. Since such vulnerabilities are already to be addressed in the IPE program, the staff concluded that it was appropriate to include the A-17 insights in the IPE program. No additional work by licensees is intended outside the scope of the planned IPE effort. RES, NRR, ACRS and CRGR agreed with this decision. OGC has no legal objection.

It should be noted that as part of the staff's integration of generic issues, the A-17 proposed action on flooding and water intrusion is addressing the concerns of GI 77, "Flooding of Safety Equipment Compartments by Back-Flow Through Floor Drains," which is a directly related issue. As a result, if the A-17 action regarding flooding and water intrusion is implemented as proposed, there would be no further action on GI 77, and GI 77 would be considered subsumed by A-17.

Another related issue, GI 57, "Effects of Fire Protection System Actuation on Safety-Related Equipment," although related, has not been subsumed by the A-17 resolution. The GI 57 scope includes consideration of the effects of more than just inadvertent actuation of a fire suppression system which uses water. It also is considering systems which use gas as a suppressant, and it is considering multiple simultaneous actuations of the suppression systems (including water) due to common causes such as earthquakes or smoke. Therefore, if the A-17 action regarding flooding and water intrusion is implemented as proposed, GI 57 will still have other potential safety significance associated with it. Further action may be proposed on GI 57 based on that safety significance.

The staff plans to issue the two enclosed NUREG reports and the generic letter to all licensees. A Federal Register Notice has been prepared and is enclosed.

Victor Stello, Jr.  
Executive Director  
for Operations

Enclosures:  
See following page

The Commissioners

- 5 -

Enclosures:

1. NUREG-1174
2. NUREG-1229
3. Federal Register Notice and  
Summary Statement

Enclosures:

- 1. NUREG-1174
- 2. NUREG-1229
- 3. Federal Register Notice and Summary Statement

[REVISED COMMISSION PAPER A17]

\*SEE PREVIOUS CONCURRENCE

EIB:DSIR	EIB:DSIR	DD:DSIR	D:DSIR	DD:GI:RES	D:RES
DThatcher/b	RBaer	WMinners	WHouston	TSpeis	EBeckjord
03/17/89*	03/17/89*	03/17/89*	03/22/89*	03/23/89*	05/10/89

OGC	AEOD	NRR	EDO
SLewis*	EJordan*	FGillespie	VStello
05/03/89	05/01/89	04/ /89*	/ /89

(by verbal)

by Verbal

"No Legal

Objection

OFFICIAL RECORD COPY

*Handwritten mark and date: 5/1/89*

the A-17 action regarding flooding and water intrusion is implemented as proposed, there would be no further action on GI 77, and GI 77 would be considered subsumed by A-17. Another directly related issue, GI 57, "Effects of Fire Protection System Actuation on Safety-Related Equipment," although directly related, has not been subsumed by the A-17 resolution. The GI 57 scope includes consideration of the effects of more than just fire suppression systems which use water. It also is considering systems which use gas as a suppressant. Therefore, if the A-17 action regarding flooding and water intrusion is implemented as proposed, GI 57 will still have other potential safety benefits associated with it. Further action may be proposed on GI 57 based on this remaining safety benefit.

The staff plans to issue the two enclosed NUREG reports and the generic letter to all licensees. A Federal Register Notice has been prepared and is enclosed.

Victor Stello, Jr.  
Executive Director  
for Operations

Enclosures:

1. NUREG-1174
2. NUREG-1229
3. Federal Register Notice and Summary Statement

DISTRIBUTION

Commissioners	T. Lewis
RES Chron	E. Beckjord
RES Circ	T. Speis
EIB r/f	W. Houston
V. Stello	W. Minners
T. Murley	R. Baer
E. Jordan	D. Thatcher

REVISED COMMISSION PAPER A17]

\*SEE PREVIOUS CONCURRENCE

B:DSIR	EIB:DSIR	DD:DSIR	D:DSIR	DD:GI:RES	D:RES	OGC	AEOD	
Thatcher/b	RBaer	WMinners	WHouston	TSpeis	EBeckjord	SLewis	EJordan	<del>MRR</del> FGillespie
/17/89*	03/17/89*	03/17/89*	03/22/89*	03/23/89*	03/ /89	/ /89	/ /89	4/7/89

0  
tello  
/ /89

the A-17 action regarding flooding and water intrusion is implemented as proposed, there would be no further action on GI 77, and GI 77 would be considered subsumed by A-17. Another directly related issue, GI 57, "Effects of Fire Protection System Actuation on Safety-Related Equipment," although directly related, has not been subsumed by the A-17 resolution. The GI 57 scope includes consideration of the effects of more than just fire suppression systems which use water. It also is considering systems which use gas as a suppressant. Therefore, if the A-17 action regarding flooding and water intrusion is implemented as proposed, GI 57 will still have other potential safety benefits associated with it. Further action may be proposed on GI 57 based on this remaining safety benefit.

The staff plans to issue the two enclosed NUREG reports and the generic letter to all licensees. A Federal Register Notice has been prepared and is enclosed.

Victor Stello, Jr.  
Executive Director  
for Operations

Enclosures:

1. NUREG-1174
2. NUREG-1229
3. Federal Register Notice and Summary Statement

DISTRIBUTION

Commissioners	T. Lewis
RES Chron	E. Beckjord
RES Circ	T. Speis
EIB r/f	W. Houston
V. Stello	W. Minners
T. Murley	R. Baer
E. Jordan	D. Thatcher

REVISED COMMISSION PAPER A17]

\*SEE PREVIOUS CONCURRENCE

IB:DSIR	EIB:DSIR	DD:DSIR	<del>D:DSIR</del>	DD:GI:RES	D:RES	OGC	AEOD	NRR
thatcher/b	RBaer	WMinners	<del>WHouston</del>	<del>TSpeis</del>	EBeckjord	SLewis	EJordan	TMurley
3/17/89*	03/17/89*	03/17/89*	03/24/89	03/23/89	03/ /89	/ /89	/ /89	/ /89

DO  
Stello  
/ /89

the A-17 action regarding flooding and water intrusion is implemented as proposed, there would be no further action on GI 77, and GI 77 would be considered subsumed by A-17. Another directly related issue, GI 57, "Effects of Fire Protection System Actuation on Safety-Related Equipment," although directly related, has not been subsumed by the A-17 resolution. The GI 57 scope includes consideration of the effects of more than just fire suppression systems which use water. It also is considering systems which use gas as a suppressant. Therefore, if the A-17 action regarding flooding and water intrusion is implemented as proposed, GI 57 will still have other potential safety benefits associated with it. Further action may be proposed on GI 57 based on this remaining safety benefit.

The staff plans to issue the two enclosed NUREG reports and the generic letter to all licensees. A Federal Register Notice has been prepared and is enclosed.

Victor Stello, Jr.  
Executive Director  
for Operations

Enclosures:

1. NUREG-1174
2. NUREG-1229
3. Federal Register Notice and Summary Statement

DISTRIBUTION

Commissioners	T. Lewis
RES Chron	E. Beckjord
RES Circ	T. Speis
EIB r/f	W. Houston
V. Stello	W. Minners
T. Murley	R. Baer
E. Jordan	D. Thatcher

REVISED COMMISSION PAPER A17]

IB:DSIR thatcher/b 1/17/89	EIB:DSIR RBaer 3/17/89	DD:DSIR WMinners 3/17/89	D:DSIR WHouston / /89	DD:GI:RES TSpeis / /89	D:RES EBeckjord / /89	OGC SLewis / /89	AEOD EJordan / /89	NRR TMurley / /90
----------------------------------	------------------------------	--------------------------------	-----------------------------	------------------------------	-----------------------------	------------------------	--------------------------	-------------------------

DO  
Stello  
/ /

Distribution

RES Chron

RES Circ

EIB r/f

V. Stello

T. Murley

E. Jordan

T. Lewis

E. Beckjord

T. Speis

W. Houston

W. Minners

R. Baer

D. Thatcher



---

---

# Evaluation of Systems Interactions in Nuclear Power Plants:

Technical Findings Related to  
Unresolved Safety Issue A-17

---

---

**U.S. Nuclear Regulatory  
Commission**

Office of Nuclear Regulatory Research

Dale Thatcher



NUREG-1174

---

---

# Evaluation of Systems Interactions in Nuclear Power Plants:

Technical Findings Related to  
Unresolved Safety Issue A-17

---

---

Manuscript Completed:

Date Published:

Dale Thatcher

Office of Nuclear Regulatory Research  
U.S. Nuclear Regulatory Commission  
Washington, DC 20555



*camera ready*

Document Name:  
NUREG-1174 TC

Requestor's ID:  
PROCTOR

Author's Name:  
THATCHER/SANDERS

Document Comments:  
PH ECS 11/22/88 Final KEEP THIS SHEET WITH DOCUMENT

*PH ECS 11/22/88*

## ABSTRACT

This report presents a summary of the activities related to Unresolved Safety Issue (USI) A-17, "Systems Interactions in Nuclear Power Plants," and also includes the NRC staff's conclusions based on those activities. The staff's technical findings provide the framework for the final resolution of this unresolved safety issue. The final resolution will be published later as NUREG-1229.

TABLE OF CONTENTS (Continued)

	<u>Page</u>
4.5 Oak Ridge National Laboratory's Conclusions and Recommendations .....	20
4.6 Staff Conclusions .....	21
5 DESCRIPTION OF RESULTS AND STAFF CONCLUSIONS .....	21
5.1 Utility Studies of Systems Interactions .....	21
5.1.1 Zion Nuclear Plant Study .....	21
5.1.2 Diablo Canyon Nuclear Power Plant Seismically Induced Systems Interaction Program .....	23
5.1.3 Indian Point Station Unit 3 Utility Study .....	24
5.1.4 Midland Nuclear Power Plant Units 1 and 2 Program ...	25
5.1.5 Staff Conclusions .....	25
5.2 Other Related Studies, Programs, and Issues.....	26
5.2.1 Sandia Laboratory Study of Watts Bar Nuclear Plant ..	26
5.2.2 Systems Interactions State-of-the-Art Reviews .....	27
5.2.3 Advisory Committee on Reactor Safeguards Concerns ...	28
5.2.4 Post-TMI-2 Actions, Including Human Factors Issues ..	31
5.2.5 NRC Office for Analysis and Evaluation of Operational Data Activities .....	31
5.2.6 Office of Inspection and Enforcement Activities.....	31
5.2.7 Other Generic Issues.....	32
5.2.8 Other Unresolved Safety Issues .....	33
5.2.9 Systematic Evaluation Program .....	34
5.2.10 Standard Review Plan .....	34
5.2.11 NRC's Policy Statement on Severe Reactor Accidents Regarding Future Designs and Existing Plants .....	35
5.2.12 Electric Power Research Institute's "Systems Interaction Identification Procedures" .....	36
5.3 Indian Point Station Unit 3 Laboratory Demonstration Study .....	36
5.4 Search for Common-Cause Events in Operating Experience .....	38
5.4.1 Functionally Coupled Type .....	40
5.4.2 Spatially Coupled Type .....	43
5.4.3 Induced-Human-Intervention-Coupled Type .....	43
5.4.4 Adequacy of Ongoing Evaluations of Operating Experience .....	44
5.4.5 Undesirable Results of Systems Interaction Events ...	44
5.5 Probabilistic Risk Assessments .....	45
5.5.1 PRA Methods .....	46
5.5.2 ASIs Identified From Review of PRA Results .....	48

TABLE OF CONTENTS (Continued)

	<u>Page</u>
5.6 Study of Seismic/Spatially Coupled Systems Interactions ....	49
5.6.1 Target Scope .....	49
5.6.2 Initiating Events .....	49
5.6.3 Source Failures .....	50
5.6.4 Documentation .....	50
5.6.5 Analysis of Spatially Coupled Systems Interactions ..	50
5.6.6 Staff Conclusions .....	51
6 SUMMARY OF STAFF CONCLUSIONS .....	52
7 REFERENCES .....	54

APPENDIX: INTERNAL FLOODING AND WATER INTRUSION INSIGHTS

## ABBREVIATIONS

ACRS	Advisory Committee on Reactor Safeguards
ADS	automatic depressurization system
AEC	Atomic Energy Commission
AEOD	Office for Analysis and Evaluation of Operational Data
AFW	auxiliary feedwater
ANS	American Nuclear Society
ASI	adverse systems interaction
ATWS	anticipated transient without scram
BNL	Brookhaven National Laboratory
BTP	branch technical position
BWR	boiling-water reactor
CCC	common cause candidate
CCW	component cooling water
CFR	<u>Code of Federal Regulations</u>
CPCo	<u>Consumers Power Company</u>
DMA	digraph matrix analysis
ECCS	emergency core cooling system
EPRI	Electric Power Research Institute
ESF	engineered safety features
FMEA	failure modes and effects analysis
FSAR	Final Safety Analysis Report
GDC	general design criterion/criteria
GI	generic issue
HELB	high energy line break
HPSI	high pressure safety injection
HVAC	heating, ventilation, and air conditioning
I&C	instrumentation and control
I&E	Office of Inspection and Enforcement, NRC
IEEE	Institute of Electrical and Electronics Engineers
INPO	Institute of Nuclear Power Operations
IP3	Indian Point Station, Unit 3
IREP	Interim Reliability Evaluation Program
LER	licensee event report
LLNL	Lawrence Livermore National Laboratory
LOCA	loss-of-coolant accident
MSLB	main steamline break



NPRDS	Nuclear Plant Reliability Data System
NRC	U.S. Nuclear Regulatory Commission
NSSS	nuclear steam supply system
NYP&A	New York Power Authority
ORNL	Oak Ridge National Laboratory
PASNY	Power Authority of the State of New York
PG&E	Pacific Gas & Electric Co.
PRA	probabilistic risk assessment
PWR	pressurized-water reactor
RCPB	reactor coolant pressure boundary
RHR	residual heat removal
RSS	Reactor Safety Study
RSSMAP	Reactor Safety Study Methodology Applications Program
RTS	reactor trip system
SEP	Systematic Evaluation Program
SETS	Set Equation Transformation Systems
SI	systems interaction
SISIP	Seismically Induced Systems Interaction Program
SRP	Standard Review Plan
TAP	Task Action Plan
TMI	Three Mile Island Nuclear Station
TMI-2	Three Mile Island Nuclear Station, Unit 2
USI	unresolved safety issue

## EXECUTIVE SUMMARY

The U.S. Nuclear Regulatory Commission (NRC) has concluded its technical evaluation of Unresolved Safety Issue (USI) A-17, "Systems Interactions in Nuclear Power Plants." This report summarizes the results of the technical activities used by the NRC staff to formulate the final resolution of USI A-17. The regulatory analysis for the proposed resolution of USI A-17 will be published later as NUREG-1229.

Because of the complex, interdependent network of systems, structures, and components that constitute a nuclear power plant, the scenario of almost any significant event can be characterized as a systems interaction. As a result, the staff determined that if the term "systems interaction" were interpreted in a very broad sense, it became an unmanageable safety issue. To begin to address perceived safety concerns within this potentially broad subject area requires some focusing. One way to focus such an effort is to develop a working set of definitions based on the perceived safety concerns. It is recognized that by the very nature of such a focusing effort, all concerns that one may characterize as systems interactions may not be addressed. It is therefore extremely important that the scope and boundary of the focused program be as clearly defined and understood as possible. Then, if other concerns still exist after completion of the program, they can be addressed as part of other efforts as deemed necessary.

The technical findings and conclusions presented in this document are based on the following definitions.

### (1) Systems Interaction (SI)

An action or inaction (not necessarily a failure) of various systems (sub-systems, divisions, trains), components, or structures resulting from a single credible failure within one system, component, or structure and propagation to other systems, components, or structures by inconspicuous or unanticipated interdependencies. The major difference between an SI and a classic single-failure event is in those hidden or unanticipated aspects of the initiating failure and/or its propagation.

### (2) Adverse Systems Interaction (ASI)

A systems interaction that produces an undesirable result.

### (3) Undesirable Result (Produced by SIs)

This was defined by a list of the types of events that were to be considered in USI A-17:

- Degradation of redundant portions of a safety system, including consideration of all auxiliary support functions. Redundant portions are those considered to be independent in the design and analysis (Chapter 15) of the Final Safety Analysis Report (FSAR) of the plant. (Note: This would violate the single-failure criterion.)

- Degradation of a safety system by a system that is not safety related. (Note: This result would demonstrate a breakdown in presumed "isolation.")
- Initiation of an "accident" [e.g., loss-of-coolant accident (LOCA), main steamline break (MSLB)] and (a) the degradation of at least one redundant portion of any one of the safety systems required to mitigate that event (Chapter 15, FSAR analyses) or (b) degradation of critical operator information sufficient to cause the operator to perform unanalyzed, unassumed, or incorrect action.  
  
(Note: This includes failure to perform correct actions because of incorrect information.)
- Initiation of a "transient" (including reactor trip) and (a) the degradation of at least one redundant portion of any one of the safety systems required to mitigate the event (Chapter 15, FSAR analyses) or (b) sufficient degradation of critical operator information to cause the operator to perform unanalyzed, unassumed, or incorrect action.  
  
(Note: This includes failure to perform correct actions because of incorrect information.)
- Initiation of an event that requires plant operators to act in areas outside the control room (perhaps because the control room is being evacuated or the plant is being shut down) and disruption of the access to these areas (for example, by disruption of the security system or isolation of an area when fire doors are closed or a suppression system is actuated).

The intersystem dependencies (or systems interactions) have been divided into three classes based on the way they propagate:

(1) Functionally Coupled

Those SIs that result from sharing of common systems/components; or physical connections between systems, including electrical, hydraulic, pneumatic, or mechanical.

(2) Spatially Coupled

Those SIs that result from sharing or proximity of structures/locations, equipment, or components or by spatial inter-ties such as heating, ventilation, and air conditioning (HVAC) and drain systems.

(3) Induced Human-Intervention Coupled

Those SIs in which a plant malfunction (such as failed indication) inappropriately induces an operator action, or a malfunction inhibits an operator's ability to respond. As analyzed in A-17, these SIs are considered another example of functionally coupled ASIs.

(Note: Random human errors and acts of sabotage are excluded.)

As a result of the staff's studies of ASIs undertaken as part of its search for a solution to the USI A-17 safety issue, the staff has concluded the following:

- (1) To address a subject area such as "systems interactions" in its broadest sense tends to be an unmanageable task and therefore incapable of resolution. Some bounds and limitations are crucial to proceeding toward a resolution. Considering this, the A-17 program utilized a set of working definitions to limit the issue. It is recognized that such an approach may leave some concerns unaddressed.
- (2) The occurrence of an actual ASI or the existence of a potential ASI is very much a function of an individual plant's design and operational features (such as its detailed design and layout, allowed operating modes, procedures, and test and maintenance practices). Furthermore, the potential overall safety impact (such as loss of all cooling, loss of all electric power, or core melt) is similarly a function of those plant features that remain unaffected by the ASI. In other words, the results of an ASI depend on the availability of other independent equipment and the operator's response capabilities.
- (3) Although each ASI (and its safety impact) is unique to an individual plant, there appear to be some characteristics common to a number of the ASIs.
- (4) Methods are available (and some are under development) for searching out SIs on a plant-specific basis. Studies conducted by utilities and national laboratories indicate that a full-scope plant search takes considerable time and money. Even then, there is not a high degree of assurance all, or even most, ASIs will be discovered.
- (5) Functionally coupled ASIs have occurred at a number of plants, but improved operator information and training (instituted since the accident at Three Mile Island) should greatly aid in recovery actions during future events.
- (6) Induced human-intervention-coupled interactions as defined in A-17 are a subset of the broader class of functionally coupled SIs. As stated for functionally coupled SIs, improvements in both operator information and operator training will greatly improve recovery from such events.
- (7) As a class, spatially coupled SIs may be the most significant because of the potential for the loss of equipment which is damaged beyond repair. In many cases these ASIs are less likely to occur because of the lower probability of initiating failure (e.g., earthquake, pipe rupture) and the less-than-certain coupling mechanisms involved. However, past operating experience highlighted a number of flooding and water intrusion events and more recent operating experience indicates that these types of events are continuing to occur.
- (8) Probabilistic risk assessments or other systematic plant-specific reviews can provide a framework for identifying and addressing ASIs.

- (9) Because of the nature of ASIs (they are introduced into plants by design errors and/or by overlooking subtle or hidden dependencies), they will probably continue to happen. In their evaluations of operating experience, NRC and the nuclear power industry can provide an effective method for addressing ASIs.
- (10) For existing plants, a properly focused, systematic plant search for certain types of spatially coupled ASIs and functionally coupled ASIs (and correction of the deficiencies found) may improve safety.
- (11) The area of electric power, and particularly instrumentation and control power supplies, was highlighted as being vulnerable to relatively significant ASIs. Further investigation showed that this area remains the subject of a number of separate issues and studies. A concentrated effort to coordinate these activities and to include power supply interactions could provide a more effective approach in this area.
- (12) For future plants, additional guidance regarding ASIs could benefit safety.
- (13) The concerns raised by the Advisory Committee on Reactor Safeguards (ACRS) on A-17, but which have not been addressed in the staff's study of A-17, should be considered as candidate generic issues, separate from USI A-17.



*in  
ready*

Document Name:  
NUREG-1174 TEXT

Requestor's ID:  
BONNIE

Author's Name:  
Thatcher/Sanders

Document Comments:  
PH-ECS 05/1/88 Final KEEP THIS SHEET WITH DOCUMENT

## UNRESOLVED SAFETY ISSUE A-17: SYSTEMS INTERACTIONS IN NUCLEAR POWER PLANTS

### 1 INTRODUCTION

In 1978, the NRC identified the area of systems interactions as an unresolved safety issue (USI) and designated it as USI A-17, "Systems Interactions in Nuclear Power Plants."

The origins of the concerns with systems interactions go back to 1974 when the Advisory Committee on Reactor Safeguards (ACRS, Nov. 8, 1974) expressed its belief that the staff should give "attention to the evaluation of safety systems and associated equipment from a multi-disciplinary point of view to identify potentially undesirable interactions between systems."

It should be noted that the original concerns were raised in the context of standard plants (ACRS, Nov. 8, 1974). It was felt that with the prospect of many "identical" plants, significant additional efforts should be focused on uncovering potential problems that may arise because a nuclear power plant is designed by groups of engineers and scientists who belong to separate engineering and scientific disciplines. It was recognized that some interdisciplinary reviews were performed to ensure the compatibility of the plant's structures, systems, and components; however, there remained some question regarding the adequacy of these reviews. For standardized plants, it was believed that the additional effort could provide significant benefits. In addition to the original ACRS concern, some potentially significant events at operating nuclear power plants have been traced to, or have been postulated to be the result of, a single common cause (as opposed to multiple independent causes). As a result, the required independence among the plant safety systems and the independence of the safety systems from the systems not related to safety have been questioned. Because of the original ACRS concern and because some significant operating events took place as a result of unexpected interdependencies among the various plant systems, components, and structures, USI A-17 was developed to address the area of systems interactions. (Note: The program designed to address systems interactions will not address all events resulting from a single common cause.) For further clarification, see Sections 2 and 3 of this report.

In 1979, an accident at the Three Mile Island Nuclear Station, Unit 2 (TMI-2) led to issuance of NUREG-0660, "NRC Action Plan Developed As a Result of the TMI-2 Accident," which identified TMI Action Plan Item II.C.3, "Systems Interaction," for the purpose of coordinating and expanding the staff's work on systems interaction (USI A-17) and to incorporate that work into an integrated plan for addressing the broader question of systems reliability in conjunction with IREP (Interim Reliability Evaluation Program) and other efforts. The TMI-2 Action Plan also stated: "As these programs go forward, there will be a conscious effort to coordinate these activities, including possible combination of resources, to eliminate unnecessary duplication." As stated in the Task Action Plan (TAP) for USI A-17 (NUREG-0649), the resolution of USI A-17 has considered the activities described in Item II.C.3.



The A-17 program has been designed to establish whether or not there are significant generic safety concerns in the area of systems interactions, and then if there are such concerns, to develop ways to identify these concerns and address them.

## 2 BACKGROUND

The term "systems interaction" has never been precisely defined, and, as a result, the investigation into the concern has suffered from a lack of a clear focus. At times, A-17 was becoming a "catch all" category for almost all significant events that occurred at operating reactors. The term has often been used interchangeably with other terms such as "dependent failures," "propagating failures," "common-cause failures," and "common-mode failures." To address what was perceived to be the original concern, and to address some of the significant types of events that have occurred, the A-17 program has been provided with a set of working definitions (see Section 3, "Definitions and Scope").

The definitions attempt to clarify the specific types of phenomena or events that are of interest in A-17 and to separately classify other phenomena or events considered outside the scope of A-17.

## 3 DEFINITIONS AND SCOPE

One of the largest efforts in focusing all of the various tasks related to systems interactions was in the development of a workable set of definitions. The definitions, and associated clarifications, were drawn from the large amount of information previously developed in A-17 (before 1983). The definitions attempt to clarify the specific types of phenomena or events that are of interest, i.e., those that represent unanticipated, adverse interactions among "systems" where systems can be structures, systems, or components. The definitions also attempt to separately classify other types of events which, although they may be significant, are not addressed in A-17. Table 1 is included to summarize the scope and bases of the USI A-17 issue.

The definitions presented here parallel those in the NRC Task Action Plan (NUREG-0649); however, the term "common-mode failure" has been dropped and further clarifications have been added. In developing the definitions, the main objective was to acknowledge that a great amount of concern exists regarding events in which a scenario progresses to an undesirable set of circumstances and the cause can be traced to a single common cause (common-cause events), involving an equipment malfunction or failure and its propagation.

After tracing the origins of the systems interaction concern as expressed by the ACRS and then also considering the changes that have been taking place in the nuclear industry over the last 10 years, it was decided that a classification needed to be created to make the problem of "systems interactions" more tractable and also to take credit for other activities which will cover areas that one might argue should be included in A-17. Some of the changes that have been acknowledged include

- (1) greater attention to human factors or the man/machine interface in all aspects of nuclear power plant design and operation

Table 1 Scope of USI A-17, "Systems Interactions": General subject area involves system failures which are due to system dependencies

Concerns	Covered by	Clarification
(1) Recognized/analyzed single failures directly propagate to other equipment/systems within the same safety division	Existing regulations • Single failure defined in the GDC	Not analyzed in A-17
(2) Single failures subtly propagate to cause plant transients/accidents and/or degrade the required safety systems. Includes: • Subtle spatial interties • Subtle functional interties	USI A-17 definition of adverse systems interactions	
(3) Common failure of redundant safety systems due to commonalities such as: • Same manufacturing defect • Same testing error • Same maintenance error	Improvements in maintenance and test procedures, ATWS rule, A-44 proposed rule	Not analyzed in A-17
(4) Operator errors that disable redundant safety systems	Improvements in operator training	Not analyzed in A-17
(5) Events that could cause multiple plant problems simultaneously: • Particularly earthquakes • Also fire and pipe break/flooding	USI A-46 plus current licensing requirements cover earthquakes  Appendix R deals with fire  Equipment qualification rule (10 CFR 50.49) deals with design-basis pipe breaks  None of these programs deals with multiple, simultaneous events. Therefore, this area is to be further evaluated under the Multiple System Responses Program.	Not analyzed in A-17, except for internal flooding/water intrusion events occurring one at a time

- (2) use of probabilistic risk assessments (PRAs) in safety analysis
- (3) increased attention to operating events.

The resulting classification scheme outlines a number of different types of common-cause events, only one set of which was defined to involve "adverse systems interactions." The other single-cause events involve mostly common characteristics of the equipment (e.g., single manufacturer, common maintenance practices and personnel, common testing practices and personnel).

### 3.1 Systems Interactions

The definition used here is: Actions or inactions (not necessarily failures) of various systems (subsystems, divisions, trains), components, or structures resulting from a single credible failure within one system, component, or structure and propagation to other systems, components, or structures by inconspicuous or unanticipated interdependencies. The major difference between this type of event and a class single-failure event is in those aspects of the initiating failure and/or its propagation that are not obvious (that are hidden or unanticipated).

Systems interactions (SIs) also can involve systems related to safety and systems not related to safety. A large part of the problem in addressing SIs stems from the fact that, in any nuclear power plant, many systems are intended to interact and are so designed. For example, one division of the safety-related component cooling water system is designed to interact with (that is, cool) a number of other safety-related systems in that division as well as possibly some systems not related to safety. Similarly, one division of the Class 1E electric power system is designed to interact with a number of safety-related systems in that same division as well as possibly with some equipment not related to safety. If these support-type systems do fail, the supported system will also most likely fail or at least will operate improperly.

Although these examples involve interaction of systems and even could be considered adverse systems interactions, they are not the kinds of interactions of concern in USI A-17, because this type of interaction is expected and the potential for such failure propagation is within the typical analysis and assumptions for a single failure. To differentiate among all the potential "systems interactions," the A-17 Task Action Plan added the aspect of "adverse" to further pinpoint the issue.

### 3.2 Adverse Systems Interactions

The definition used here is: A systems interaction that produces an undesirable result, as defined by a list of the types of events to be considered in the A-17 program (see below).

The list was created on the basis of perceived safety concerns in the broad area of systems interactions for the purpose of capturing potential adverse systems interactions, and therefore terms such as "undesirable" instead of "unacceptable" and "degradation" instead of "failure" were used.

- (1) Degradation of redundant portions of a safety system, including consideration of all auxiliary support functions. Redundant portions are those considered to be independent in the design and accident analysis (Chapter 15, FSAR analyses) of the plant.

(Note: This would violate the single-failure criterion.)

- (2) Degradation of a safety system by a system not related to safety.

(Note: This result would demonstrate a breakdown in presumed "isolation.")

- (3) Initiation of an "accident" [e.g., loss-of-coolant accident (LOCA), main steamline break (MSLB)] and (a) the degradation of at least one redundant portion of any one of the safety systems required to mitigate that event (Chapter 15, FSAR analyses) or (b) degradation of critical operator information sufficient to cause the operator to perform unanalyzed, unassumed, or incorrect actions.

(Note: This includes failure to perform correct actions because of incorrect information.)

- (4) Initiation of a "transient" (including reactor trip) and (a) the degradation of at least one redundant portion of any one of the safety systems required to mitigate the event (Chapter 15, FSAR analyses) or (b) degradation of critical operator information sufficient to cause the operator to perform unanalyzed, unassumed, or incorrect actions.

(Note: This includes failure to perform correct actions because of incorrect information.)

(Note: Undesirable results 3 and 4 are included because of the concerns regarding possible breakdowns in defense-in-depth principles. If a link is found between the initiation of an event and the systems designed to mitigate that event, then the probability of an event sequence progressing to core melt may be greater than originally believed.)

- (5) Initiation of an event that requires plant operators to act in areas outside the control room area (perhaps because the control room is being evacuated or the plant is being shut down) and disruption of the access to these areas (for example, by disruption of the security system or isolation of an area when fire doors are closed or a suppression system is actuated).

The intersystem dependencies (or systems interactions) have been divided into three classes, based on the way they propagate:

- (1) Functionally Coupled

Those SIs that result from sharing of common systems/components; or physical connections between systems, including electrical, hydraulic, pneumatic, or mechanical.



## (2) Spatially Coupled

Those SIs that result from sharing or proximity of structures/locations, equipment, or components, or by spatial inter-ties such as heating, ventilation, and air conditioning (HVAC) and drain systems.

## (3) Induced Human-Intervention Coupled

Those SIs that result when a plant malfunction (such as failed indication) inappropriately induces an operator action, or when a malfunction inhibits an operator's ability to respond. As analyzed in the study of USI A-17, these SIs are considered another example of functionally coupled ASIs.

(Note: Random human errors and acts of sabotage are excluded.)

### 3.3 Other Common-Cause Events

Multiple failures resulting from a single common cause and typically characterized by the failure of identical components in redundant safety systems will not be addressed in the A-17 study. Such multiple failures can be traced to external events; manufacturing and installation errors; or to operation, testing, and maintenance errors.

The usual design practice for safety systems is to satisfy the single-failure criterion by providing identical, redundant safety systems which are subjected to common environmental events and made, installed, operated, tested, and maintained in common. Therefore, the potential for these types of "failures" results from a recognized compromise in independence (see 10 CFR 50, Appendix A, "Introduction to the General Design Criteria") and is addressed in a number of ways, and in some cases without specific identification. Some of the ways in which this other class of failures/errors is addressed are discussed in the four paragraphs that follow.

To obtain protection from possible failures induced by a component's environment, including failures resulting from external events, the components of the safety systems are designed, qualified, and installed to be immune to such anticipated challenges.

To obtain immunity to failures, including failures resulting from manufacturing and installation errors, the safety-related systems, structures, and components are subjected to various quality control and quality assurance programs which include comprehensive testing requirements at all phases of construction and pre-operation. Major improvements in the area of quality assurance have been made at the utilities.

Protection from failures attributed to errors by operators, technicians, and maintenance personnel can be obtained through adequate training and good procedures for all aspects of operation, testing, and maintenance. The staff is instituting major programs to address all of these areas (see NUREG-0985).

Other provisions may be utilized for protection against these types of common-cause failures. One design technique which is utilized is diversity. An example of such an application by the staff is a portion of the requirements which resulted from the Salem anticipated transient without scram (ATWS) event (NUREG-1000). As part of the resolution, it was concluded that consideration

should be given to providing a diverse breaker trip scheme. Although such cases have been addressed on an individual basis, the concept of diversity is cited in the regulations (e.g., General Design Criterion (GDC) 22).

### 3.4 Clarifications

Some additional clarifications are included here to address the areas that tend to be the hardest to classify. First, events induced by operator error will be discussed and then events involving external phenomena and other major plant-wide events will be discussed. Classic single failures vs. adverse systems interactions will be discussed. Also, the concept of frontline and support systems will be presented.

#### 3.4.1 Operator Error

For purposes of studying USI A-17, plant operators and their procedures were assumed to be perfect. This assumption allowed the staff to focus on only the area of the adequacy of the information presented to the operator by the plant display systems, as outlined in induced human-intervention-coupled SIs. Therefore, the operator was treated as a hardwired link that performed perfectly. As stated earlier, other programs involving human factors were considered more suited to addressing the possibility of operator error, test and maintenance errors, and procedure deficiencies (see NUREG-0985).

#### 3.4.2 External Events

One of the most difficult areas to classify for purposes of studying USI A-17 is external events. In general, external events such as tornadoes and earthquakes are not addressed in the A-17 program. It is recognized that external events could initiate other common-cause failures, as stated in Section 3.3 above.

It is also recognized that, with respect to non-seismically qualified or non-safety-related equipment, an external event such as an earthquake could be the cause of the single initiating failure in an adverse systems interaction sequence. In that limited sense, external events were considered. The group engaged in the A-17 program did not consider the potential for an external event to cause simultaneous multiple initiating failures and systems responses. For more discussion of major plantwide events and the potential for multiple systems responses, see Section 3.4.3 which follows.

#### 3.4.3 Major Plantwide Events and the Potential for Unanalyzed, Nonconservative, Multiple Systems Responses

During discussions with the ACRS, some disagreements over the scope of the A-17 program were noted (ACRS, May 13, 1986).

In later discussions with the ACRS, the concerns were developed further. The analysis for plant events (such as earthquakes, fires, LOCAs, and floods) involve a number of assumptions. These assumptions often include certain aspects which the ACRS believes may not be conservative. The first aspect involves the assumptions that the events themselves are not linked, that is

an earthquake does not start a fire, a fire does not cause a LOCA, etc. The ACRS is concerned that such assumptions are neither realistic nor conservative.

The second aspect involves the assumption that if a component is not specifically required to function for the mitigation of an event, then it is assumed to be disabled or inoperable. Again, the ACRS is concerned that such assumptions are not conservative because if the specific failure modes of the component are considered, the component could spuriously perform some detrimental action which could affect the ability to mitigate the event and/or to achieve safe shutdown.

The above concern involving specific failure modes includes the added aspect that systems and components are generally assumed to be either fully operable or totally inoperable, as if only two possible states existed. As a result, ACRS believes that there is also the potential that partial failures, which do not result in total loss of function could lead to some unanalyzed systems action which in turn may adversely affect the event mitigation and/or the ability to achieve safe shutdown. The ACRS believes that failures or partial failures could occur simultaneously in multiple systems, if the initiating event is of a sufficiently broad nature, such as an earthquake, fire, or flood.

The staff studying USI A-17 has not addressed the potential for major events causing other events nor has it addressed the multiple failure concerns expressed by the ACRS. It is recommended that these issues be addressed as separate potential generic issues.

#### 3.4.4 Single Failures vs. ASIs

An important aspect of the A-17 group's definition of SIs and ASIs is the unanticipated or hidden nature of the dependency. It is acknowledged (and therefore not "unanticipated") that certain design features do not have redundancy. Examples are the reactor vessel itself and the refueling water storage tank at some pressurized-water reactors (PWRs). Clearly, a failure of these could lead to an undesirable result; however, A-17 does not intend to deal with these common causes because they are not hidden or "unanticipated." The other important aspect involves a similar problem area. A problem arose because once an ASI is identified, it looks like a classic single failure and one could then argue that it is, therefore, not an ASI, just a single failure. This aspect was very critical in the operating experience search. That part of the program relied heavily on the consensus of a number of people familiar with operating events and plant design and, therefore, keenly attentive to "surprises" such as unanticipated couplings or dependencies. This "judgment" aspect has led to at least one noted disagreement involving power sources and the results that one would anticipate or expect from a single failure in a Class 1E power source. An analyst or engineer familiar with nuclear power plant systems, and particularly with the instrumentation and control power systems and electric power systems, may expect one set of results (which would meet all other aspects of the ASI definition); another analyst or engineer may find the results unexpected. Therefore, some events involving loss of instrumentation and control power supplies may not have been captured during the initial screening of the licensee event report (LER) data base. Because of its possible importance, as outlined in related Generic Issue (GI) 76 (NUREG-0933, Rev. 2) and as stated by the NRC staff (NRC memorandum, September 18, 1984), further specific work was undertaken in this area (see Section 5.4 below).



### 3.4.5 Frontline and Support Systems

During the review and evaluation of systems interactions, the group studying USI A-17 acknowledged that there may be a difference in the way the frontline systems, such as emergency core cooling and reactor protection systems, are treated and the way the support systems, such as component cooling water and heating and ventilating systems, are treated. The frontline systems usually receive thorough scrutiny in the licensing process because of the number of specific criteria which are clearly applicable and also because these areas of the plant tend to be more standardized among plants (at least regarding any specific nuclear steam system supplier).

The support systems, on the other hand, are often less standardized and in many cases are more complex and pervasive, so that they not only interface with multiple frontline safety systems and other safety-related support systems, but also may interface with functions not related to safety. As a result, support systems may require greater scrutiny for adverse systems interactions.

### 3.5 Summary and Conclusions

The resolution of USI A-17 involves those types of common cause events which are classified as adverse systems interactions subject to the above definitions and classifications.

On the basis of all work that has been and is being performed in the resolution of A-17 and with the objective of resolving A-17 in a defined time frame, the staff concluded that a working set of definitions was crucial to the A-17 program. Therefore, the staff focused its A-17 task on certain types of phenomena and scenarios and left other areas to other programs and issues.

## 4 AVAILABLE METHODS FOR IDENTIFYING SYSTEMS INTERACTIONS

As a related effort to the investigation of the nature and potential safety significance of adverse systems interactions, the group engaged in the A-17 program explored a number of methods that appeared to offer the potential for finding ASIs. The purpose of this part of the program was to determine the effectiveness and the resource requirements of potential ASI search methods and to make recommendations regarding possible search methods if it was concluded that a search was necessary.

Some of the information on methods is reported in other sections of this report (e.g., digraph matrix analyses, Section 5.3; interactive fault tree and failure modes and effects analyses, Section 5.3; operating experience search, Sections 5.1.1, 5.2.3, 5.2.5, 5.2.6, and 5.4; onsite inspections, Sections 5.1 and 5.6; and PRAs, Section 5.5). This section of the report also addresses some of these methods, combinations of these methods, and other methods, and then draws some general conclusions.

ORNL (NRC, NUREG/CR-4261) reviewed and identified four classes of qualitative analyses techniques that can be used to identify possible systems interactions. Each class of techniques would be appropriate for different aspects of a systems interaction search (see Table 2). In addition, there are distinct advantages and disadvantages in performing each class of techniques. The four basic classes are

Table 2 Analysis methodologies available to identify types of systems interactions

Analysis methodologies available to identify systems interactions	Types of systems interactions identified by methodologies		
	Functional	Spatial	Induced human-intervention-coupled
Operating experience review	X	X	X
Plant walkthrough		X	
Preoperational testing	X		
Failure modes and effects analysis	X	X	X
Design review	X	X	X
Decision table	X		X
System state enumeration	X		
Binary matrix	X	X	
Digraph matrix	X	X	X
Event tree analysis	X		
Fault tree analysis	X	X	X
GO methodology	X	X	
Sneak-circuit analysis	X		
Generic analysis	X	X	

- (1) operating experience reviews
- (2) onsite inspections
- (3) analysis by parts
- (4) graph-based analyses

Each class of techniques is composed of one or more different analysis methodologies. Each class of techniques is discussed below, and information is provided about the individual methodologies in the class. (For a list of some associated references for each technique, see NUREG/CR-4261.)

Some combination of these analysis techniques could be used to perform a systems interaction study or could be incorporated into a systematic study such as a probabilistic risk assessment (PRA) to identify functional, spatial, or induced human-intervention-coupled systems interactions.

#### 4.1 Operating Experience Reviews

The NRC staff currently requires operating experience review "programs" for each nuclear power plant licensee (TMI Action Plan Item I.C.5). The NRC and industry also sponsor their own reviews of operating experience (see Section 5.4). The objective of all of these programs is to learn from events that have already occurred, or have the potential to occur, at operating nuclear power plants. The history of events at plants under construction is also reviewed. The potential benefit of operating experience reviews is to eliminate recurring problems. For systems interaction purposes, this may allow previously unanticipated dependencies to be identified before any serious safety consequences occur.

To benefit from the review of operating experience, reliable sources of data on events must be available. For a specific plant, this includes both onsite sources (deficiency reports, operating logs, work orders, etc.) and documents prepared for submittal to outside agencies (licensee event reports (LERs), significant event reports, Nuclear Plant Reliability Data System (NPRDS) failure reports, etc.) The data sources that contain information on events from many plants include the NRC's LER files, Institute of Nuclear Power Operations (INPO) operating experience systems, and various other industry working groups (vendors, technical societies, etc.).

Once a source of operating experience is chosen, proper review requires the services of experienced personnel. The reviewers need to be familiar with the facility for which the review is conducted; reviewers also need to be cognizant of the similarities and differences between that facility and those facilities at which the events occurred. This knowledge is essential in determining whether the events apply to the plant for which the review is being performed.

A key to performing effective operating experience reviews is to carry the evaluation beyond simply asking, "What would happen in our plant if the exact same conditions occurred?" It requires the personnel to consider two other questions:

- (1) Can this systems interaction occur at our facility under any conditions?
- (2) If such an event occurred at our facility, are the consequences unacceptable?

If the answer to both these questions is "yes," then further evaluation (and subsequent resolution) of the potential problem is required.

Operating experience reviews can examine the potential for certain systems interactions (i.e., those interactions that have occurred previously). Since the NRC requires ongoing operating experience reviews, it would be simple and inexpensive to include the identification of systems interactions as one of the objectives of the reviews. The recognized shortcomings of operating experience reviews are that the reviews (1) are not fully predictive and (2) are very dependent on the experience and training of the review staff. Operating experience reviews can provide insights into functional, spatial, and induced human-intervention-coupled systems interactions.

#### 4.2 Onsite Inspections

Onsite inspections are used to identify differences between the as-built conditions and the design conditions. They can also examine undesirable situations (i.e., proximity, seismic interaction, etc.) that may not be apparent from design documentation. This class of techniques incorporates the experience and knowledge of plant personnel into the analysis. Onsite inspections can also be used to identify areas in which the environmental conditions within the plant are hazardous to equipment or in which adverse changes have been made in the plant's equipment configuration (because of maintenance or upgrading). Two types of onsite inspection methodologies were identified: plant walkthroughs and preoperational testing.

#### 4.2.1 Plant Walkthroughs

Plant walkthroughs are used to identify potential spatial systems interactions and to visually inspect safety-related components and systems in their as-built configuration. Consequently, walkthroughs are used to identify those systems interactions that were overlooked during plant design or that were generated during plant construction.

Consumers Power Company developed a plant walkthrough program at its Midland Nuclear Power Plant, Units 1 and 2 (Consumers Power Company, June 1983) to determine the potential for spatial systems interactions. The program consisted of: (1) combined proximity for seismic Category I and II components, systems, and structures, (2) high-energy line break hazards, (3) internal missiles, and (4) flooding. The function and team composition for each of these walkthroughs were varied to be appropriate for each specific type of systems interaction. Consumers Power Company also developed a supplemental walkthrough program that addressed (1) fire protection, (2) stress, (3) thermal growth, (4) system or area turnover walkthroughs, and (5) potential concerns discovered during pre-operational testing of systems.

Plant walkthroughs to identify potential systems interactions have also been performed at Diablo Canyon Nuclear Power Plant; San Onofre Nuclear Generating Station, Units 2 and 3; Zion Nuclear Plant; and Indian Point Station, Unit 3. These walkthroughs were structured to identify spatial systems interactions.

The advantages of plant walkthroughs include: (1) They can focus on bad design, construction errors, maintenance errors, and conditions for common failure and (2) They utilize the knowledge of experienced plant personnel.

#### 4.2.2 Preoperational Testing

Preoperational testing is used to demonstrate the operability of the nuclear steam supply systems, the auxiliary systems, and related secondary systems. All licensees are required to successfully complete a preoperational testing program before a full-power license can be issued. This testing program demonstrates the capability of items of equipment (and systems) to meet their design performance and safety criteria. However, preoperational tests can specifically test how systems interact (in some cases existing tests already do this). For example, a diesel generator operability test should include sequencing the diesel generators onto the emergency power buses. There are many cases in which a test specifically designed to test for systems interactions could confirm the absence of unacceptable interactions during specific operating modes.

The advantages of preoperational testing include: (1) The tests can provide a baseline of operating data from which future operational anomalies may be identified, (2) They provide further confidence in the analytical results and functional capabilities of the systems, and (3) They have the potential to identify functional interactions.

A disadvantage is that they cannot typically identify spatially coupled interactions.



### 4.3 Analysis by Parts

The third class of techniques available for identifying systems interactions is analysis by parts. Analysis-by-parts techniques are more analytically oriented than the previously discussed classes of techniques, but they are also less comprehensive than the graph-based analyses discussed in Section 4.4. Five methodologies were identified as analysis-by-parts techniques:

- (1) failure modes and effects
- (2) design reviews
- (3) decision tables
- (4) system state enumeration
- (5) binary matrix

Analysis by parts requires the analyst to examine the causes of a given event or to develop credible conditions under which an undesirable event could occur. Consequently, a problem is not evaluated from a total system perspective. Instead, direct causes of subsystem or component failures are identified and the consequences of these failures are examined. Since these techniques are used to look for direct causes, they are not exhaustive in that regard.

Several advantages of this class of techniques are: (1) They require less effort to perform than the graph-based analyses (at the price of less complete coverage), (2) They are relatively simple to perform, (3) They are useful for detecting local effects, and (4) They require the analyst to look systematically at the failure of each component. Disadvantages of this class include: (1) They usually capture only local effects, (2) They depend on the creativity of the analyst, (3) They have a limited amount of predictive strength, and (4) They are generally used in support of other classes and frequently address the same type of systems interactions as the graph-based methods. Each of the methodologies is discussed below.

#### 4.3.1 Failure Modes and Effects Analysis

Failure modes and effects analysis (FMEA) is an inductive analysis method that is generally applied at the component level. As such, it examines a component to determine how it would fail (mode) and what would result (effect). An FMEA generally does not examine the causes of the failure extensively but may be employed to identify failure modes whose effects are severe enough to warrant further analysis.

The FMEA identifies failure modes for components of concern and traces their effects on other components, subsystems, and systems. Emphasis is placed on identifying the problems that result from hardware failures, operator errors, etc. Typically, a column format is employed in an FMEA. Specific entries for the columns include descriptions of the component, its failure modes, possible failure causes, possible effects, and actions to reduce the failures and their consequences. By further examining the causes of the failures, possible common-cause mechanisms may be identified.

An FMEA is traditionally developed at the component level. However, an FMEA can also be applied at the subsystem or system level to trace interactions and their effects on plant safety functions and, eventually, on plant safety itself. In addition, the effects of the failure modes (whether at the component or

system level) must be considered for all plant operational modes and the analyst must also consider the possibility of other components undergoing test and maintenance.

#### 4.3.2 Design Reviews

Design reviews are performed to ensure that the safety system independence and functional design criteria have been met or exceeded. The procedures for performing them vary, and are specific to the design organization. Design reviews are generally performed by a diversified group of experienced designers called a design review team. Using the design criteria or specifications for the systems, the team reviews available documentation such as control schematics, layout drawings, as-built drawings, and piping and instrumentation diagrams. The team then identifies design deficiencies, including potential systems interactions. The team also recommends actions or design changes that may correct the design deficiencies and eliminate potential systems interactions. An advantage of using design reviews to identify potential systems interactions is that they can provide early identification. One disadvantage is that as-built drawings are frequently not available or are not up to date. Also, it is difficult to ensure the comprehensiveness of design reviews.

#### 4.3.3 Decision Tables

Decision tables are used to describe each possible output state of a component. The output states are a function of the inputs and internal states (operational or failed states) of the components. Decision tables can handle binary and nonbinary logic (i.e., components with two or more states).

To construct a decision table, the analyst divides the system into levels of components or subsystems. Once the system has been divided into levels, the analyst needs to perform three basic steps:

- Step 1 The analyst constructs the decision tables beginning with the components of the lowest levels (i.e., the simpler components of the system).
- Step 2 The outputs of the tables from Step 1 constitute the inputs of the decision tables for the next higher level.
- Step 3 Step 2 is repeated for each higher level until the decision table of the system is formed.

This methodology can be used to identify common-cause failures, since they are the inputs that are carried through several levels.

One advantage of constructing decision tables is that they not only model hardware failures, but model human actions and interactions as well. However, decision tables are not a stand-alone method and are generally used to aid in constructing fault trees.

#### 4.3.4 System State Enumeration

In a system state enumeration analysis, all of the system states are generated and recorded in a table format by considering all possible combinations of

component states. After this is completed, each system state is individually examined for dependencies between component states. From a qualitative point of view, this analysis is equivalent to an event tree analysis.

An advantage of system state enumeration is that it is a fairly complete qualitative method. However, a complete qualitative system analysis would include an FMEA for each state. Also, for complex systems, enumerating all potential component states can be an overwhelming task.

#### 4.3.5 Binary Matrices

Binary matrices use hierarchies to portray the dependencies between components. A binary entry in each intersection of the matrix indicates whether or not the components are dependent upon each other. The binary entry indicates that the component on the left of the matrix (row) is dependent upon (receives support from) the component listed at the top (column). The matrix is not limited to components. The entity of interest could be maintenance, a physical location, a system train, etc. A set of binary matrices that represent more than one independent system is used to generate digraph matrices.

One advantage of binary matrices is that the analyst need only supply direct relationships between individual items (components, subsystems, etc.). A computer code can then be used to deduce subsequent relationships. A second advantage of binary matrices is that the components can be listed in any order in the matrix. In addition, the use of binary matrices forces the analyst to identify all supporting systems or components. This aids the analyst in developing fault trees, digraph matrices, etc.

#### 4.4 Graph-Based Analyses

The last class of analysis techniques is graph-based analyses. Graph-based analyses are comprehensive within a given set of boundary conditions and are used to represent the logical relationship among those components (or systems) whose failure can lead to a specific undesired event. These relationships are captured in the graphic model. All of the potential failure modes (within the scope of the analysis) are then identified by using computers to generate the combinations of component and human failures that contribute to the undesired event.

Advantages of this class of techniques include: (1) the ability to cover low-frequency events systematically, (2) the ability to deal with complex systems, (3) the ability to evaluate shared support systems, and (4) the ability to identify common-cause failures. Disadvantages of these techniques include: (1) their limited ability to analyze human interface, (2) their complexity, and (3) their expense when performed at a detailed level (probably the level needed for an ASI study).

Six methodologies were identified as graph-based analysis techniques:

- (1) digraph matrix
- (2) event tree
- (3) fault tree
- (4) GO methodology
- (5) sneak circuit
- (6) generic analysis



#### 4.4.1 Digraph Matrix Analysis

Digraph matrix analysis (DMA) utilizes a success tree that includes all systems and/or components (elements) involved in an accident sequence. This success tree includes subsystems and support systems as elements. A binary matrix (known as an adjacency matrix) is produced from the success tree that contains information about the relationship between these elements. This binary matrix is then converted to a dual-digraph matrix by changing all "or" gates to "and" gates and "and" gates to "or" gates. Cutsets or failure combinations are then obtained from the dual digraph. The cutsets are then evaluated for systems interactions. The steps involved in performing a DMA are:

First, the analyst selects the combinations of systems of interest for a detailed evaluation. (This is equivalent to the PRA event tree analysis designed to find accident sequences.)

Next, the analyst constructs a single-digraph model for each accident sequence. This is a graph approach that allows the analyst to develop a binary matrix (adjacency matrix) of elements that have direct influence on an element of higher order.

The analyst can then partition digraph models into independent subdigraphs to find the cutsets. Computer codes are available that identify the cutsets.

Finally, the analyst can evaluate cutsets on the basis of probability and display answers for both top event and cutset probabilities.

Some advantages of a digraph matrix analysis include:

- (1) The construction of the logic model is performed directly from plant schematics (piping and instrumentation diagrams, electrical schematics, safety logic diagrams, etc.). The resulting model can be overlaid on the plant schematics; thus, the model can be readily understood, reviewed, and corrected.
- (2) The digraph can represent physical situations that are cyclic.
- (3) DMA computer codes can process very large models. An entire accident sequence consisting of several safety systems and their support systems is modeled as a single digraph.
- (4) The binary matrix indicates all levels of subordination, but only direct first-level relationships must be provided. Computer codes deduce any consequent levels of subordination.
- (5) An element of the matrix can be any entity of interest (e.g., an entire system, a system function, component, or maintenance crew). Elements of any level of detail can be intermixed.

Disadvantages of a digraph matrix analysis include:

- (1) There are few trained analysts and few available computer codes that can be used to develop and subsequently apply the analysis.

- (2) For certain types of logic diagrams, the analyst's attempt to be more complete can lead to computer limitations.

#### 4.4.2 Event Tree Analysis

Because nuclear power plant systems are so complex, it is not feasible to write down by inspection a listing of important accident sequences. Therefore, a systematic and orderly approach is required to properly understand and identify the many factors that could influence the course of potential accidents. This approach involves developing an event tree. An event tree is an inductive logic model that sequentially models the progression of events (both failure and success) from some initiating event to a series of logic consequences. An event tree begins with an initiating failure, and it maps out a sequence of events of the system level that forms a set of branches. Each of the branches represents a specific accident sequence. A complete event tree analysis requires the identification of all possible initiating events and the development of an event tree for each event.

Event trees are normally used to model events having binary failure states. These events usually correspond to total success or failure of a system. Event tree analysis is a useful tool for systems interaction analysis when used with other techniques such as fault tree analysis.

#### 4.4.3 Fault Tree Analysis

Fault tree analysis is a deductive failure analysis that focuses on an undesired event and provides a method for determining causes of this event. The undesired event constitutes the top event in a fault tree diagram. Careful choice of the top event is important to the success of the analysis. A fault tree analysis describes an undesired state of the plant or system (usually an undesired state that is critical from a safety viewpoint) and analyzes the plant or system to find all credible ways in which the undesired event can occur. The fault tree is a graphic model of the combinations of faults that will result in the occurrence of the undesired event. The faults can depict hardware failure, human error, system failures, external events (e.g., earthquakes or internal fires), or other events that can lead to the undesired event.

A fault tree is not a model of all possible plant or system failures or all possible causes for failure. A fault tree is tailored to its top event and includes only those faults that contribute to the top event. The fault tree is not quantitative; however, the results can be evaluated quantitatively. In fact, the fault tree is a convenient model to quantify and, along with event trees, has formed the structure for almost all of the PRA studies performed for the nuclear industry. As a result, a large number of people in the nuclear industry are experienced in developing and/or using fault trees.

A formalized combination of event trees and fault tree analyses is called a cause-consequence analysis. The event trees are used to determine the sequence of events that can lead to the consequences of interest. Event trees are developed for several different initiating events (usually LOCAs and transients). The fault trees are then used to model the causes of the event sequences. The

causes of the event sequence failures can be modeled as system failures or component failures. However, if failure data are lacking on the system level, the causes would be modeled on the component level where such data are usually available. Hence, the results of a cause-consequence analysis are both qualitative and quantitative.

Two advantages of performing a cause-consequence analysis are: (1) the method is better suited for identifying potential system dependencies on the component level than is the event tree alone and (2) for fault trees alone, the dependencies are shown on separate trees. However, the consequence diagram includes all of them within a single logic structure.

#### 4.4.4 GO Methodology

The GO methodology is a success-oriented technique that is generally used for quantitative analyses. However, this methodology can be used to identify component failure combinations that can lead to system failure, and to construct event trees. Completed GO models resemble system schematic or process flow charts and tend to be more compact than equivalent fault tree models (albeit with correspondingly less failure mode information). Seventeen logical operators are used to model a process. From these models, functional, spatial, and induced human-system interactions can be identified.

Specific advantages of the GO methodology include: (1) The system models follow the normal process flow (as does a digraph matrix analysis), (2) Modeling of most component and system interactions and dependencies is explicit, (3) Models are compact and easy to validate, (4) Model evaluations can represent both success and failure states of systems, and (5) It is uniquely adaptable to analyses in which many levels of system availability are to be considered since it has the ability to handle multiple system states (i.e., partial failure or degraded conditions can be modeled).

Disadvantages of the GO methodology include: (1) Fewer analysts are familiar with the GO methodology than with fault tree/event tree analyses and (2) The GO methodology has been used extensively for probabilistic studies of individual systems but has not been employed to any great extent as the primary technique for a full-scope PRA.

#### 4.4.5 Sneak-Circuit Analysis

Sneak-circuit analyses are normally applied to electrical systems and were originally designed to identify unplanned modes of operation, unexplained problems, and unrepeatably anomalies. However, this type of analysis can also be applied to fluid systems since fluid systems can be represented by electrical system analogs.

A sneak-circuit analysis will identify latent signal paths or circuit conditions in systems that may cause undesired events to occur, or may inhibit the occurrence of a desired function. The problems identified in the analysis are called sneak circuits and are characterized by their ability to escape detection during most standardized tests. In addition, sneak circuits are not dependent on component failures, although many erroneous responses of system failures occur because of component failures. Sneak circuits can be subdivided into four types:

- (1) sneak paths, which cause current or energy to flow along unexpected paths
- (2) sneak timing, which may cause or prevent the flow of current of energy to activate or inhibit a function at an unexpected time
- (3) sneak indications, which may cause an ambiguous or false display of system operating conditions
- (4) sneak labels, which may cause incorrect stimuli to be initiated through operator error

An advantage of sneak-circuit analyses is that problems caused by latent signal paths that are not contingent on component failures can be identified. These signal paths can cause undesired events to occur, or inhibit a desired function from occurring. The main disadvantages of sneak-circuit analyses are the lack of documentation explaining the methodology. Additionally, only one company was found that had experienced and qualified analysts able to perform such analyses.

#### 4.4.6 Generic Analysis

A generic analysis reviews the basic events in each minimal cutset for susceptibilities to generic causes (dependencies). The minimal cutsets can be determined from fault tree analysis or similar analyses. When a generic cause is common to all members of a minimal cutset, and the location of the minimal cutset components offers no protection from that generic cause of failure, the minimal cutset is called a common-cause candidate (CCC). Generic causes for failure that are often considered in such analyses are:

- (1) mechanical/thermal generic causes
  - impact
  - vibration
  - pressure
  - grit
  - moisture
  - stress
  - temperature
  - freezing
- (2) electrical/radiation generic causes
  - electromagnetic interference
  - radiation damage
  - conducting medium
  - out-of-tolerance voltage
  - out-of-tolerance current
- (3) chemical/miscellaneous generic causes
  - corrosion (acid)
  - corrosion (oxidation)
  - other chemical reactions
  - carbonization biological



(4) other common links

- energy source
- calibration
- installations
- maintenance
- operator or operation
- proximity
- test procedure
- energy flow paths

Although a major portion of this technique is qualitative, it follows an analysis procedure such as fault trees rather than preceding it, as other qualitative methods usually do. This approach differs from most common-cause analyses because it deals directly with the minimal cutsets instead of adding secondary failures to the logic model. Thus, only component failures that result in system failure are considered.

A generic analysis is a helpful methodical way to identify spatial systems interactions. It has been implemented in a number of computer programs and is extensively used in dependent-failure analyses in the nuclear industry.

#### 4.5 Oak Ridge National Laboratory's Conclusions and Recommendations

Oak Ridge National Laboratory (ORNL) concluded (NRC, NUREG/CR-4261) that there are many different and varied methodologies available that can identify systems interactions. However, no one methodology by itself can adequately identify functional, spatial, and induced human-intervention-coupled systems interactions. Therefore, several different analysis techniques should be used simultaneously.

Determining the most appropriate combination of analysis techniques for identifying systems interactions requires consideration of several factors - time, scope, costs, benefits, etc. However, a review of the methodologies available made several insights apparent. First, any systems interaction program should utilize operating experience reviews, design reviews, and preoperational testing. These three methodologies are already required to be performed, and minimal modifications to the existing programs could be required to identify all three types of systems interactions. Second, expanding the scope of PRAs to include the identification of systems interactions should simplify the problem (with respect to starting an independent evaluation), since the analysts would already be familiar with the systems and their responses. Last, the resulting combination of methodologies must be able to adequately identify all three types of systems interactions - spatial, functional, and induced human-intervention coupled.

The manpower required to perform a PRA that includes a systems interaction analysis should be within the bounds provided in the "PRA Procedures Guide" (NRC, NUREG/CR-2300). The "PRA Procedures Guide" indicates that 19 to 38 man-months are required for sequence and system modeling, with another 18 to 24 man-months required for external event analysis. It is not possible to separate the amount of modeling required for independent and dependent failure modes. However, it should be recognized that to do an adequate job of analyzing systems interactions requires experienced analysts and adequate time to examine and incorporate all the potential dependencies that can arise from

systems interactions. For this reason, the upper estimates provided in the guide may be more appropriate to ensure that adequate analysis of systems interactions can be included.

In summary, the methodologies discussed in this report can be applied to identify systems interactions. However, the problem in conducting a systems interaction analysis is not a problem with methodology as much as it is a problem with scope and level of detail.

#### 4.6 Staff Conclusions

All methods appear to have some advantages and disadvantages. The major conclusions based on the above review are:

- (1) The global application of any method or combination of methods is costly.
- (2) The choice of method may not be as important as the scope and depth of the study performed.
- (3) It is, therefore, probably most cost effective to limit studies to specific areas and to increase the level of detail in modeling and analysis in those areas.

### 5 DESCRIPTION OF RESULTS AND STAFF CONCLUSIONS

NRC defined a number of tasks in the revised Task Action Plan for USI A-17 (NUREG-0649) to address the area of systems interactions. Although all the tasks defined in the TAP were completed, this section of the report is not organized into the same set of tasks. Rather, this report is organized around the task results and recommendations which were then used as input for the technical resolution of USI A-17.

The tasks outlined for studying the A-17 issue were developed to utilize a combination of existing information, ongoing work, and new work with the objective of focusing the various efforts to resolve the generic issue as defined in the revised TAP scope and definitions.

#### 5.1 Utility Studies of Systems Interactions

A number of utilities performed systems interaction studies of their own plant(s) as part of the operating license review process. The staff has considered some of these programs in the resolution of A-17.

##### 5.1.1 Zion Nuclear Plant Study

In a June 17, 1977 letter, the NRC Advisory Committee on Reactor Safeguards (ACRS, June 1977) recommended that Commonwealth Edison conduct a study of possible systems interactions related to the Zion Nuclear Plant's shutdown heat removal capability. The ACRS also referenced additional guidance contained in its letter of November 8, 1974. Possible approaches to a systems interaction study were discussed with a number of consultants and with the NRC staff.

As a followup to these discussions, Commonwealth Edison performed an experience survey utilizing LERs (Commonwealth Edison Company, June 1978). The study was



divided into three phases. Phase 1 consisted of a review of more than 9000 LERs which were generated in the operation of U.S. commercial nuclear power plants between 1969 and 1977.

The LERs were used to identify events that have occurred at operating power plants that involve systems interactions which had a potential for reducing the effectiveness of shutdown cooling systems under nonaccident conditions. The review covered not only four-loop PWRs but all pressurized-water, boiling-water, and gas-cooled reactor LERs.

The Zion screening criteria as quoted from the report were formulated to include the following types of events:

- Events which demonstrated that the action of any system degraded or resulted in loss of the effectiveness of any of the following systems:

reactor coolant	instrumentation power
residual heat removal	chemical and volume control
component cooling	auxiliary feedwater
service water	portions of main steam
auxiliary power	

- The action which initiated the event could have been a normal control function, a malfunction, or operator induced. The single-failure criterion was not extended; however, a detailed review was made to determine its applicability.
- As an example, the failure of an RHR [residual heat removal] pump to start due to an electrical fault in the motor would not have been considered a systems interaction. However, if the motor failure was due to excessive humidity and temperature in the RHR cubicle, it was considered an undesirable systems interaction.
- It was noted that personnel action can result in maintenance errors or operator errors which will have a direct effect on a system or piece of equipment, but this was not considered to be an interaction between systems. For example, the loss of an instrument bus due to placing a grounded test instrument on the bus results in the loss of a large amount of equipment, as expected. If, alternatively, the load from the bus was not correctly shed from the electrical system and resulted in faults in other parts of the electrical system, it would be considered an undesirable interaction.

The second phase of the study, which was conducted by Fluor Pioneer, Inc., involved detailed analysis and investigations of each identified event to determine how and why the event occurred and its effect on the originating plant.

For the third phase, an assessment was made of the possibility of the occurrence of an identical or similar event at the Zion plant. If it was found that a similar event could occur at the Zion plant, corrective action options were evaluated. The evaluation criteria included consideration of safety, constructability, operability, maintainability, and cost. While the range of possible

corrective options was being review and analyzed, the utility assessed the benefits of the options.

On the basis of the evaluation criteria and the benefits assessment, the utility concluded that for Zion, the generic studies requested by the NRC and the implementation of conclusions and recommendations involving such items as fire protection, pipe break, and low-temperature primary system overpressure have resulted in modifications which substantially reduce the possibility of the occurrence of a majority of the events studied. In addition, about five specific investigations and/or plant modifications were recommended in the study.

It should be noted that there is not a good correlation between the LERs highlighted by Commonwealth Edison and the LERs contained in the Oak Ridge National Laboratory's (ORNL's) review of operating experience (see Section 5.4, below). To some degree, this occurred because of differences in definitions of what constitutes an adverse systems interaction event. Nevertheless, the Zion study was reviewed by ORNL as part of the review of operating experience (see Section 5.4, below) for possible SI events which met the definition offered in the current A-17 Task Action Plan.

#### 5.1.2 Diablo Canyon Nuclear Power Plant Seismically Induced Systems Interaction Program

Pacific Gas and Electric Co. (PG&E) established a systems interaction program (PG&E, May 1984) which was intended to establish confidence that if a seismic event of the severity of the postulated Hosgri event\* occurred, structures and equipment important to safety will not be prevented from fulfilling their safety functions because of seismically induced failure or motion of structures or equipment not related to safety. Also, the Seismically Induced Systems Interaction Program (SISIP) was instituted to establish confidence that safety-related systems will not fail to meet the single-failure criterion because of seismically induced interactions.

PG&E defined the following two terms to clarify its postulation of potential systems interactions:

- (1) Targets are (a) structures and equipment needed to take the plant to safe shutdown and maintain it at safe shutdown; (b) certain accident-mitigating systems such as containment isolation, main steam isolation, and containment spray; and (c) the manual fire suppression equipment.
- (2) Sources are any other equipment whose seismically induced failure or motion could interact with a target and prevent or inhibit a target from accomplishing its safety function.

On the basis of these definitions, a large number of potential interactions were postulated. PG&E utilized four ways to resolve postulated interactions. These were: (1) resolution by field inspection in which the interaction team could by inspection or simple field analysis show that either the source would

---

\*The Diablo Canyon seismic design basis was upgraded after the potential for severe earthquakes originating from the Hosgri Fault (a branch of the San Andreas Fault) was reappraised.

not fail, the occurrence of the interaction was not credible, or the consequences of the interaction, if it occurred, would not adversely affect target operations; (2) resolution by engineering analysis in which PG&E could show either that the interactions would not occur or, if they did occur, that the consequences would not affect target operations; (3) resolution by an expedient modification in which PG&E decided it was more cost effective to resolve the interaction by modifying the plant than to justify the configuration by analysis; and (4) resolution by necessary modification in which further analysis showed that plant modification is the only means for resolving the interaction. Because the last two involved plant modification, PG&E combined resolutions 3 and 4 and only reported three resolution groups.

The problem in assessing the Diablo Canyon program comes from the fact that the safety significance of the modifications (both expedient and necessary) cannot be readily established.

Information developed as a result of this program has been utilized in the A-17 program (see Section 5.6 of this report).

### 5.1.3 Indian Point Station Unit 3 Utility Study

The Indian Point Station Unit 3 (IP3) systems interaction report was prepared by the Power Authority of the State of New York (PASNY, June 1983) in conjunction with Ebasco Services Inc. and consists of 25 volumes. The objectives of this study were (1) to develop a methodology and evaluation criteria to be used to identify and evaluate systems interactions and (2) to apply these criteria to a systems interaction review of 23 identified systems.

For purposes of this study, the utility decided to define systems interactions as those events that affect the safety of the plant by one system acting on one or more other systems in a manner not intended by design, with emphasis on interactions in which systems not related to safety (non-safety systems) act on safety-related systems.

The analysis then involved (1) the systematic search for hidden or inadequately analyzed interconnections or couplings that link safety and non-safety systems in the reactor plant and (2) the evaluation of the effects of a non-safety system failure (or maloperation) propagated into the safety system by such interconnections/couplings.

(Note: It was assumed for purposes of that study that the safety systems satisfied the single-failure criterion and that redundant safety systems do not possess dependencies so that one malfunction cannot disable redundant safety systems.)

On the basis of these premises, a number of potentially adverse interactions between non-safety systems and safety systems were identified through a series of dependency tables, logic diagrams, failure mode and effect analysis, event trees/fault trees, review of previous reports, and walkthroughs (onsite reviews). Only one of these resulted in a reportable condition (LER) as determined by the licensee. This involved a nonseismic pipe connection to a seismic system with inadequate isolation. The resolution involved maintaining a manual isolation valve in a closed position.

A number of potential adverse systems interactions were identified and resolved. The utility concluded that the program increased the level of safety for Indian Point 3; however, the contribution to core damage probability from the postulated non-connected seismically initiated systems interactions was less than 4% of the overall core-melt frequency at the design-basis earthquake level (Atomic Industrial Forum, Inc., October 1985). Information developed as a result of this program has been utilized in the A-17 program (see Section 5.6 of this report).

#### 5.1.4 Midland Nuclear Power Plant Units 1 and 2 Program

In January 1983, Consumers Power Company (CPCo) initiated a program to address systems interactions (CPCo, June 1983). The program consisted of three parts to address the three classes of systems interaction: functional, spatial, and induced human-intervention-coupled.

The functional interaction portion of the program was to rely heavily on existing plant procedures for design control and preoperational checkout and testing. The design control task involved an interdisciplinary review of plant design to ensure that potential interactions generated by the interface between activities of the various engineering groups were identified and corrected. The program was to include preoperational testing to demonstrate the capability of required safety systems to meet design performance and safety criteria. Additional methods for use in identifying and evaluating functional dependencies included probabilistic risk assessment (PRA), control systems failure evaluation, and licensing department reviews of industry operating experience through nuclear steam supply system (NSSS) vendor reports, Institute of Nuclear Power Operations (INPO) reports, and licensee event reports (LERs).

Onsite reviews (walkthroughs) of safety-related structures, systems, and components were employed to address spatially coupled SIs. These onsite reviews identified potential interactions arising from proximity, location of non-seismically qualified equipment over safety equipment, high-energy line break (HELB), internal missiles, and flooding. Additional reviews also addressed the areas of pipe stress, fire protection, and thermal growth for potential spatial interactions. CPCo was incorporating many inplace programs into the spatial SI studies to avoid unnecessary duplication of efforts. For example, a program had been in place to address the seismic "Class II over Class I" issue per Regulatory Guide 1.29 requirements.

To address the induced human-intervention-coupled class of ASIs, the CPCo SI program incorporated design reviews and other tasks implemented to improve operator response to plant events. Other tasks included a human factors review of control room design and procedures, review of control room operating experience, and increased operator training, including the use of simulators.

Although the Midland project has been terminated, the available results, particularly with regard to the seismically induced systems interactions have been utilized in the A-17 program (see Section 5.6 of this report).

#### 5.1.5 Staff Conclusions

Although the licensee programs discussed above contributed to an increase in safety, the utilities did not perceive the amount of increase to be significant. What was clear was that each program cost the utility millions of dollars.



On the basis of these preliminary conclusions, the staff defined a task to examine the three utility studies (Diablo Canyon, Indian Point Unit 3, and Midland) in greater detail to attempt to better optimize the cost/benefit ratio.

For the results and conclusions of this additional work, refer to Section 5.6.

## 5.2 Other Related Studies, Programs, and Issues

As part of earlier NRC programs to address the issue of systems interaction, national laboratories did a number of studies. In addition, many other ongoing NRC programs are directly related to the work on A-17.

### 5.2.1 Sandia Laboratory Study of Watts Bar Nuclear Plant

From 1973 through 1980, NRC contracted with Sandia Laboratory to utilize a method of reviewing nuclear power plant systems for potential interactions that was different from the review process being used by NRC in its Standard Review Plan (SRP) ( NUREG-0800).

The method was the fault tree method using the Set Equation Transformation Systems (SETS) computer code for evaluating the fault trees to identify the potentially interactive cutsets. The resulting report (NRC, NUREG/CR-1321), also assessed the SRP to show where the potential interactions revealed by this independent method may not be specifically discussed in the SRP sections on review, review procedures, or acceptance criteria.

The scope of the study was restricted to allow the methodology to be developed and demonstrated in a timely fashion. The interactions addressed were limited to those arising from physical connections and common locations.

Three plant functions were included: decay heat removal, reactor subcriticality, and reactor coolant pressure boundary integrity. The range of environmental conditions, plant modes, and plant occurrences was also restricted.

The first step of the study was to develop a methodology for reviewing the SRP that could also be used to evaluate specific facilities. The underlying premise of the methodology is that potential interactions can effectively be found by identifying the commonalities between systems.

The methodology uses fault trees to model plant functions from which the analysis is performed. The SETS computer code and subsequent analysis identifies and highlights the important commonalities based on input plant information. Commonalities found between components whose unavailability could lead to loss or significant degradation of an important plant function are pursued in greater detail.

The principal product of this study was to be the development of a systematic and disciplined methodology for the identification and evaluation of a range of potential systems interactions.

The methodology was applied to a facility that had recently gone through the licensing process (Watts Bar) to achieve two goals: (1) to provide a basis for comparison to the SRP-type review and (2) to demonstrate the methodology itself. In general, it was concluded that application of the methodology should

not be limited to those systems explicitly identified in the SRP as safety related. In addition to this general conclusion, several weaknesses were identified in the SRP. These met all of the following criteria: (1) A potential cause of an interaction could be identified, (2) If an interaction occurred, it would increase the likelihood of core damage, and (3) The potential cause of an interaction was not explicitly covered in the SRP.

The weakness identified was the absence of explicit assurances in the SRP or its supporting documents that (1) the reactor coolant pressure boundary integrity will not be lost as a result of interactions stemming from a common location or common actuation of the pressurizer power-operated relief valves and their isolation valves, (2) the decay heat removal function will not be lost as a result of interactions stemming from a common location or common cooling between trains of the auxiliary feedwater system, (3) positive pressure control will not be lost as a result of interactions stemming from common power sources between pressurizer heater channels, and (4) the inventory makeup necessary to maintain decay heat removal will not be lost as a result of interactions stemming from the common location of the refueling water storage tank output valves.

Although the Sandia work was considered a major portion (Phase I) of the NRC program to address systems interactions, subsequent revision to the A-17 Task Action Plan somewhat deemphasized this work by Sandia because ongoing PRA work (see Section 5.5) and the Brookhaven application on Indian Point 3 (see Section 5.3) were similar to the Sandia work.

The staff concluded that fault trees and other PRA techniques could be used in the investigation of systems interactions. For more on PRA and its relationship to systems interactions see Section 5.5.

#### 5.2.2 Systems Interactions State-of-the-Art Reviews

The NRC requested three national laboratories to conduct a review of the state of the art in the area of systems interactions in 1980.

Each laboratory produced a report as follows:

- NUREG/CR-1859, "Systems Interaction: State-of-the-Art Review and Methods Evaluation," prepared for NRC by Lawrence Livermore National Laboratory, dated January 1981
- NUREG/CR-1896, "Review of Systems Interactions Methodologies," prepared for NRC by Battelle Columbus Laboratories, dated January 1981
- NUREG/CR-1901, "Review and Evaluation of Systems Interaction Methods," prepared for NRC by Brookhaven National Laboratory, dated January 1981

The broad objective of these reports was to develop methods that held the best potential for further development and near-term use by industry and NRC on systems interaction evaluations for future as well as operating plants. More specifically, the objectives of the work were to include:

- (1) development of a definition of systems interaction and corresponding safety failure criteria



- (2) review and assessment of current systematic methods that have been used, or are considered feasible for use, on any complex system comparable to a light-water reactor plant
- (3) provision of an inventory of a range of systems interaction scenarios with emphasis on actual operating experience to
  - (a) better focus on the definition of systems interaction
  - (b) serve as a basis for evaluating the ability of the various methodologies to predict these examples
- (4) recommendation of a methodology or alternatives that have the best potential for further development and near-term use by industry and the NRC on systems interaction evaluations
- (5) application of candidate methodologies to actual occurrences to demonstrate their ability to predict systems interactions effects

The staff concluded that the recommendations of the three studies would be considered as part of the A-17 resolution if a study was required of all utilities. For more on state of the art see Section 4, on methods.

### 5.2.3 Advisory Committee on Reactor Safeguards Concerns

As stated in the introduction to this report (Section 1), the ACRS was credited with identifying the original concerns. In addition to the original identification, the ACRS has also been instrumental in subsequent investigations in the area of systems interactions. The utility studies at Zion, Indian Point, and Diablo Canyon were all the subject of ACRS discussions (see Sections 5.1.1, 5.1.2, and 5.1.3, respectively).

In addition, in September 1979, ACRS consultants completed NUREG-0572, "Review of Licensee Event Reports (1976-1978)," in which they identified a class of events as "systems interaction." The report concluded that a number of LERs reveal unusual and often unpredicted interactions among various plant systems. The report went on to state that it is not surprising that interactions exist, since a nuclear power plant is an extensive and complex facility; however, the nature of these interactions is often quite unexpected. When interactions involve degraded performance of systems required for vital functions, such as shutdown heat removal, there can be significant safety implications. The ACRS acknowledged that the NRC staff is studying systems interactions through Generic Task No. A-17.

Regarding the use of the LERs the report stated:

Redundancy and defense in depth are widely used in essential reactor systems to assure their availability. Implicit in such usage is the assumption that a high degree of independence exists between the redundant elements (or the various echelons of defense in depth). Occasionally an LER discloses an unintentional or previously unrecognized interdependence between such elements. In such cases, interdependence reflects one type of systems interaction problem. Although

there are few LERs that directly reveal such problems, there are many that hint at deficiencies of this nature. Because of the potentially serious implications of such situations, more attention needs to be directed to seeking them out. Careful review of LERs can uncover such design errors, if they are consciously sought out.

Reference is then made to three sections of the Appendix that include some examples. The first section is entitled "Systems Interactions" and describes three separate events, all of which involve the plant electrical systems. These specific events do not meet the definition and screening criteria of the current TAP for A-17 and therefore were not included in the ORNL list. However, it should be noted that the ORNL LER study (see Section 5.4) does highlight the area of electrical systems as a potentially significant area from the viewpoint of adverse systems interactions.

The second section is entitled "Failures That Indicate Interdependence of Redundant Elements" and describes four separate events.

- The first of these events involves redundant battery chargers for a fire pump and would not meet the TAP definition of systems interaction because (1) the fire system is not typically a system needed to achieve and maintain safe shutdown and (2) the chargers were not truly redundant in the same sense of engineered safety features (ESF) Trains A and B equipment.
- The second event involves the loss of both makeup pumps at Davis-Besse Nuclear Power Station. It is the staff's understanding that the makeup pumps at Davis-Besse are not considered safety related and therefore such an event does not meet the TAP definition which includes degradation of safety-related equipment.
- The third event involves a boron dilution event at Surry Power Station, Unit 2. Although this event involved some unexpected interaction between systems and temporarily blinded the operator, none of the systems involved were safety related and the consequences were very minimal. The consequences were limited by the inherent design of the system because the system could only deliver a maximum of 150 gpm which could not reduce the boron concentration below acceptable levels between the required sampling intervals.
- The fourth event occurred at Three Mile Island Nuclear Station Unit 1 (TMI-1) and involves a miscalibration of all four power range flux monitors as a result of a faulty test pressure transmitter. Although this event does demonstrate a common-cause effect or dependency, it is not an adverse systems interaction but rather fits in the class of other common-cause failures according to the TAP definitions.

The third section of the Appendix is entitled "Adverse Interactions of Safety System and the Influence of Human Errors" and involves one event at Arkansas Nuclear One Units 1 and 2. The event involved a number of adverse systems interaction aspects and has also been included in the list of events compiled by ORNL. It was noted that the ACRS report and the ORNL report both seem to indicate the potential for adverse systems interactions in the highly complicated electrical power supply and its control systems.

Some other ACRS questions and concerns were documented in the form of recommendations to the staff and, in at least three cited utility studies, in the form of guidance to the utilities. Of particular note is the guidance in the ACRS October 12, 1979 letter on Indian Point Station Unit 3. This guidance was issued in response to questions about what constitutes "reasonably appropriate study of systems interactions at Indian Point 3." In that letter, the ACRS expressed specific concerns in two separate areas. One area involved "possibility of systems interactions within an interconnected electrical and mechanical complex." The ACRS expressed concerns with the consideration of other than usually assumed failures, i.e., partly failed or other than normally assumed failed states. The ACRS was also concerned that this type of failure would probably not be revealed by LERs and that a failure mode and effects analysis (FMEA) was required. The second area involved "possibility of interactions between non-connected systems due to the physical arrangement or disposition of equipment." Again, ACRS expressed its belief that LERs would not reveal these unique interactions and recommended a physical inspection of the plant and the "formation of a small but competent interdisciplinary team."

Over the years, ACRS has stated its belief that the staff should require all utilities to do a systems interaction type of analysis and that because such an analysis could be done with little NRC guidance, the requirement should be issued without further investigations and delay. Over the same time period, the NRC staff took the position that such a general requirement would not resolve the issue because of the lack of any consensus about what, if anything, needed to be done. The staff continued to pursue an approach for resolution, searching for an overall cure in the form of what "acceptable" methods should be applied. At this time and on the basis of further review, the staff has concluded that the concerns expressed by the ACRS in the October 12, 1979 letter are some of the central issues that need to be addressed by the resolution of USI A-17.

Regarding the ACRS report (NRC, NUREG-0572), the staff concluded that although many of the events cited there were not "adverse systems interactions" as defined in the present A-17 TAP, the overall conclusions of the report regarding power systems and their control remain valid. In addition, the general type of concerns expressed in the report regarding compromise in redundancy and/or levels of defense in depth also remain valid and have been explored further in the work on A-17 (see Sections 3, 5.4, and 5.6).

On the basis of further review, the staff concludes that (1) walkthroughs similar to walkthroughs suggested by ACRS but with much narrower focus could achieve a cost-effective safety improvement at some plants and (2) although the pursuit of so-called partial failures (leading to functionally coupled ASIs) may uncover uniquely plant-specific scenarios, there is not sufficient evidence to show that they are safety significant enough to justify the type of analyses required to uncover them. In addition, with respect to the failure modes of control systems, USI A-47 (NUREG-0649) is also addressing this area. The staff will provide information to the utilities regarding the types of problems uncovered in the electrical power systems (one area that was highlighted for partial failure investigation), and other types of problems regarding failure modes (see Section 5.4). The ACRS has also expressed concern (ACRS, May 1986) over the scope of the A-17 program. This was discussed previously in Sections 3.4.2 and 3.4.3.

#### 5.2.4 Post-TMI-2 Actions, Including Human Factors Issues

After the accident at TMI-2, a significant amount of attention was focused on the operators and on so-called human factors issues. The USI A-17 TAP (NRC, NUREG-0649) recognizes all the activity in this area and attempts to limit the overlap of concerns between the systems interaction issue and those other efforts. As a result, the A-17 studies focused on the hardware or hardwired aspects of the operators' indication systems and left the human engineering and, specifically operator error, to NUREG-0985, "Human Factors Program Plan."

The A-17 area of concern was, therefore, limited to the possibility of misleading an operator by means of malfunction (that was not readily detectable) in a plant indication system during an event. This was the induced human-intervention-coupled adverse systems interaction referred to in Section 3. After the accident at TMI-2, a significant amount of attention was focused on this aspect of plant indications. Specifically, requirements were implemented through NUREG-0737, Supplement 1, which improved monitoring information (Regulatory Guide 1.97, "Instrumentation for Light-Water-Cooled Nuclear Power Plants To Assess Plant and Environs Conditions During and Following an Accident," and added operator aids such as the safety parameter display system.

The staff engaged in the A-17 program concluded that plant personnel (operators, maintenance personnel, test technicians, etc.) can have a significant impact on plant response, both negative and positive; however, events initiated by personnel error should not be classified as systems interactions. The potential for indication systems misleading the operator has been reduced by other actions mentioned above. Furthermore, the actions in the area of operator information and training should improve response to and recovery from ASI-type events.

#### 5.2.5 NRC Office for Analysis and Evaluation of Operational Data Activities

As a result of the TMI-2 accident, the NRC formed the Office for Analysis and Evaluation of Operational Data (AEOD) with the intent to pay closer attention to current operating experience and to learn from past experience. AEOD has reported on a number of events that meet the TAP definition of systems interaction, although the events may not have been labeled "systems interactions." In some cases, the staff has formulated new generic issues based on the AEOD reports (see Section 5.2.7 of this report). As part of the resolution of A-17, the staff took a separate look at operating experience. The AEOD reports were one of the reference sources for this work (see NRC's NUREG/CR-3922 and Section 5.4 of this report for more information on operating events).

The staff has concluded that since the formation of AEOD, operating events at plants receive much greater scrutiny than at the time when the systems interaction issue first surfaced. It should be recognized that the implementation by NRC and the industry, through organizations such as INPO, of such scrutinizing analyses addresses some concerns that could be called SIs and as such contributes to a reduction in concerns with systems interaction.

#### 5.2.6 Office of Inspection and Enforcement Activities

The former NRC Office of Inspection and Enforcement (I&E) had the responsibility for notifying all utilities about significant operating events through a system of bulletins and information notices. Several of the events that were screened



from the operating experience, by the work on A-17, were the subject of an IE bulletin or notice. In those cases, this information was included as a reference source (see NUREG/CR-3922 for more information). In addition, as part of the decisionmaking process to possibly implement new requirements, those regulatory actions already required by I&E were considered (for more information see Section 5.4 of this report).

Over the years, I&E has notified the industry about significant operating occurrences. In some cases, the occurrences involve systems interactions. As was concluded for AEOD, the staff concludes that the I&E mechanisms of bulletins and notices addressed significant experience, including systems interactions.

#### 5.2.7 Other Generic Issues

In November 1983, the NRC published NUREG-0933, "A Prioritization of Generic Safety Issues." The report presents the priority rankings for a number of generic safety issues related to nuclear power plants. The purpose of these rankings is to assist in the timely and efficient allocation of NRC resources for the resolution of those safety issues that have a significant potential for reducing risk.

The prioritized issues include TMI Action Plan items under development; previously proposed issues covered by task action plans, except issues designated as unresolved safety issues (USIs) which had already been assigned high priority; and newly proposed issues.

The safety priorities, ranked as high, medium, low, and drop, have been assigned on the basis of risk significance estimates, the ratio of risk to costs, and other impacts estimated to result if resolution of the safety issues were implemented.

A number of the issues identified in NUREG-0933 can be called adverse systems interactions and, therefore, there is significant overlap between some issues listed there and the general categories resulting from the ORNL experience search (Section 5.4). This could be expected since the NUREG-0933 issues often arise from the same sources that ORNL used (e.g., LERs and AEOD reports). In some cases, a potential area of concern highlighted from an A-17 systems interaction perspective will have been cited, and possibly addressed, but on a more specific basis.

The resolution of A-17 has considered the safety priority ranking given to the corresponding issues (when available). The A-17 resolution then also recommends further action if necessary (for more information see Section 5.4 of this report).

Three issues included in NUREG-0933 warrant special discussion: Issue II.C.3, "Systems Interactions"; Issue C-13, "Non-random Failures"; and Generic Issue 77, "Flooding of Safety Equipment Compartments by Backflow Through Floor Drains." As stated in the TMI Action Plan, the purpose of Issue II.C.3 was "to coordinate and expand ongoing staff work on systems interaction (USI A-17) so as to incorporate it into an integrated plan for addressing the broader question of system reliability in conjunction with IREP [Interim Reliability Evaluation Program] and other efforts."

When the A-17 Task Action Plan was revised in January 1984, it was decided to include in issue A-17 the activities described under Issue II.C.3.

Issue C-13, "Non-random Failures," is an issue that was credited to ACRS in NUREG-0471. Although this issue was formerly referred to as "common mode failure of identical components exposed to identical or nearly identical conditions or environments" (as evidenced by reference to issues such as A-9, A-30, A-35, B-56, and B-57) it was expanded to include other types of failures and, as a result, a reference to USI A-17 is made in NUREG-0933. It should, therefore, be kept clear that the term "non-random failures" can include more than "systems interactions" and that a resolution of A-17 does not resolve all non-random failures (for additional information see Section 3).

GI-77 was given a high priority and was also qualified insofar as the lack of plant-specific details. In this regard, the group studying the resolution of USI A-17 considered these in its resolution.

The mechanism in place for identifying and prioritizing generic safety issues provides an avenue for handling all types of issues, including systems interaction type issues. On the basis of the treatment of a general type of issue such as C-13, that is by handling it as a class and dealing with individual identified parts, the staff concludes that this is the best mechanism for dealing with any remaining or future SI concerns after the resolution of A-17. This is consistent with the need to clearly define any proposed safety issue in order to prioritize it.

#### 5.2.8 Other Unresolved Safety Issues

The Task Action Plan for USI A-17 acknowledges that a relationship can exist with USI A-47, "Safety Implications of Control Systems" (NUREG-0649). This is primarily based on the understanding that control systems do interact with many plant systems and, therefore, if the control systems interactions lead to possible degradations in safety systems, such a concern could also be labeled an adverse systems interaction.

As the resolution of A-17 progressed, a close relationship between A-46 (NUREG-0649) and part of A-17 was acknowledged. Part of A-17 deals with possible seismic-induced spatial interactions between the non-seismic structures, systems, and components and the seismic structures, systems, and components. A-46 deals with the seismic qualification of certain equipment in older plants. The resolution of A-17 reflects this relationship.

Although USI A-45, "Shutdown Decay Heat Removal Requirements" (NUREG-0649) is not directly related to A-17, it is recognized that if the resolution of A-45 were to be an independent shutdown system, then such a resolution could substantially reduce the safety benefit of pursuing some ASIs.

As the resolution of A-17 has progressed to the point of focusing on certain areas, the relationships to other unresolved safety issues have been considered. The proposed resolution of A-17 acknowledges relationships with USI A-45, USI A-46, and USI A-47.



### 5.2.9 Systematic Evaluation Program

The Systematic Evaluation Program (SEP) was initiated by the NRC to review the designs of older operating nuclear reactor plants to reconfirm and document their safety. The review provided (1) an assessment of the significance of differences between current technical positions on safety issues and those that existed when a particular plant was licensed, (2) a basis for deciding how these differences should be resolved in an integrated plant review, and (3) a documented evaluation of plant safety.

The review focused on 137 different "topic" areas (NUREG-0824). Although topics that were being reviewed under other programs, such as unresolved safety issues, were generally deleted from consideration in the SEP, some topics that were evaluated under the SEP are related to USI A-17. Therefore, the information developed in these topic areas was used in the A-17 study.

Of specific applicability were topics that were related to potential spatially coupled interactions.

These topics included:

- III-4.C Internally Generated Missiles
- III-5.A Effects of Pipe Break on Structures, Systems, and Components Inside Containment
- III-5.B Pipe Break Outside Containment

On the basis of its review of the general SEP findings on these topics (NRC, SECY-84-133), the staff concluded that:

- (1) Plants typically provide significant protection against internally generated missiles.
- (2) The flooding reviews performed in response to the Atomic Energy Commission (AEC) generic letter of September 26, 1972, may not have adequately covered some significant areas of concern.

This information was used to develop the focus of spatially coupled ASIs (see Section 5.6).

### 5.2.10 Standard Review Plan

The Commission's Standard Review Plan (SRP) (NUREG-0800) is the document that defines the acceptance criteria and review guidance used in the licensing process. The SRP has evolved over a number of years and has typically addressed areas of concern that can be considered adverse systems interactions.

One alternative considered in the A-17 program was the possibility of revising the SRP or related guidance documents such as regulatory guides to improve the evaluation of ASIs for future plant reviews. Some of the SRP sections that already address systems interaction concerns are listed in Table 3.

Table 3 SRP sections that deal with spatially and functionally coupled ASIs

Source	SRP Section(s) (NUREG-0800)
<u>Spatially coupled ASIs</u>	
Earthquake	3.6.2, 3.7.3, 3.9.2, 3.10, 3.11, 6.7, 9.1.3, 9.2.1-9.2.3, 9.2.6, 9.3.1, 9.3.3, 9.3.5, 9.4.1-9.4.5, 10.3, 10.4.7, 10.4.9
Internal flood	3.4.1, 3.6.1, 9.3.3, 10.4.5
Internal fire	9.5.1
High-energy line break	3.6.1
Internal missiles	3.5.1.1-3.5.1.3, 9.1.4, 9.1.5
<u>Functionally coupled ASIs</u>	
Reactor protection/engineered safety features	7.2, 7.3
Safe shutdown	7.4
Control system	7.7
Station service water	9.2.2
Electric power systems	8.2, 8.3

#### 5.2.11 NRC's Policy Statement on Severe Reactor Accidents Regarding Future Designs and Existing Plants

The NRC has published a policy to resolve safety issues related to reactor accidents more severe than design-basis accidents (NUREG-1070). Its main focus is on the criteria and procedures the Commission intends to use to certify new standard designs for nuclear power plants; however, it also provides guidance on decision and analytical procedures for the resolution of severe accident issues for other classes of future plants and for existing plants (operating reactors and plants under construction which have applied for operating licenses). Severe nuclear accidents are those during which substantial damage is done to the reactor core, whether or not there are serious offsite consequences. Specifically the policy states:

The Commission plans to formulate an integrated systematic approach to an examination of each nuclear power plant now operating or under construction for possible risk contributors (sometimes called "outliers") that might be plant specific and might be missed absent a systematic search.

The investigation into USI A-17, "Systems Interactions," highlighted a number of nuclear power plant systems or areas that appear to be the ones that are most likely to contain potential adverse systems interactions.

ASIs (both functionally coupled and spatially coupled) are most often caused by a design feature and/or a set of operating conditions peculiar to a particular plant; the consequences of an ASI are similarly determined by features peculiar to a particular plant and by the operator's response. Therefore, the resolution of A-17 can add to the formulation of any systematic evaluation of plants by providing aid in focusing the search for "outliers."

The areas of concern should include aspects that are discussed in the review of operating experience (see Section 5.4) and the review of seismic/spatially coupled SI programs (see Section 5.6). These are:

- Functionally Coupled ASIs

- (1) electric power systems
- (2) support systems
- (3) overreliance on "fail-safe" design principles
- (4) automatic actions with no preferred failure mode for all stations
- (5) instrumentation and control power supplies

- Spatially Coupled ASIs

- (1) non-seismically qualified equipment effects on seismically qualified equipment
- (2) internal plant flooding of safety-related equipment

#### 5.2.12 Electric Power Research Institute's "Systems Interaction Identification Procedures"

As the technical resolution of USI A-17 was proceeding, the Electric Power Research Institute (EPRI) published EPRI NP-3834, Volumes 1-5, "Systems Interaction Identification Procedures." The staff asked Oak Ridge National Laboratory to review and assess the report's impact on the proposed resolution of USI A-17.

ORNL prepared a draft letter report dated February 10, 1986, concluding that both the proposed resolution for USI A-17 and the EPRI report explored numerous methodologies for identifying SIs. Both assessments conclude that no one methodology by itself can adequately identify functional, spatial, and induced human-intervention-coupled interactions. Therefore, several different analysis techniques should and could be used.

None of the methods presented in the EPRI assessment provide a quicker, easier, or more comprehensive means of identifying SIs. It was, therefore, concluded that the EPRI work brought no new information to the technical resolution of A-17.

#### 5.3 Indian Point Station Unit 3 Laboratory Demonstration Study

The staff initiated a laboratory demonstration study on the Indian Point 3 plant in mid-1983 through Brookhaven National Laboratory (BNL) and Lawrence

Livermore National Laboratory (LLNL). The purpose of the study was to test and compare two potentially useful search methods and to compare the results with the study made by the utility. One method, the digraph matrix method, was applied by LLNL (for further information see NUREG/CR-2915, NUREG/CR-3593, NUREG/CR-4179, and LLNL's report of June 1983) and the other method, the interactive fault tree/failure mode and effect analysis, was applied by BNL (for further information see NUREG/CR-4207). Both studies concentrated on functionally coupled events.

By placing the same \$1 million limit on each study, a meaningful comparison was anticipated.

There was no shortage of postulated intersystems dependencies that could be counted among the possible causes of safety malfunctions (NRC memorandum, March 20, 1985). From the impressively large number of cutsets generated by both groups of analysts, surprisingly few were safety significant.

Two cutsets contributed an estimated core damage frequency as high as  $6 \times 10^{-6}$  per reactor year. The next likely cutset contribution was not greater than about  $5 \times 10^{-9}$  per reactor year. The estimated frequencies of occurrence are highly biased by a pessimistic treatment of recovery actions available to the operators. Therefore, a very small fraction of the intersystems dependencies (which are possible to postulate) were even modestly safety significant.

The only safety-significant systems interaction highlighted by BNL was the unavailability of station battery 32 coincident with a safeguards systems actuation signal. This postulated event would leave both low-pressure injection recirculation pumps and other vital equipment unavailable. The loss of station battery 32 does not meet General Design Criterion (GDC) 35 (PASNY, LER 84-010-00, Docket 05000286, July 16, 1984). The postulated event could lead to core damage with an estimated frequency as high as  $2 \times 10^{-6}$  per reactor year. The plant was modified and is not now vulnerable to this postulated event.

The first significant systems interaction highlighted by LLNL is a misalignment of preselected service water pumps and valves coincident with a loss of offsite power. Without rapid operator intervention, this postulated event could lead to a reactor coolant pump seal failure and hence a small LOCA and the loss of both core heat removal paths. The postulated event could lead to core damage with an estimated frequency as high as  $4 \times 10^{-6}$  per reactor year. (Note: Although this was presented by LLNL as an adverse systems interaction, it does not truly fit the TAP definition.)

The other significant systems interaction highlighted by LLNL is a mechanical failure of the linkage within an interlocking breaker coincident with a loss of offsite power. Without rapid operator intervention, this postulated event could lead to damage to the emergency diesels and the subsequent failure of reactor coolant pump seals LOCA and loss of core-heat-removal paths. It was estimated that this postulated event could lead to core damage with a frequency only as high as  $5 \times 10^{-9}$  per reactor year.

On the basis of the evaluation of the results of the two demonstration analyses, the staff concludes that there is no one method that alone could serve as a mechanism for resolving concerns regarding adverse systems interactions; in other words, there is no panacea. Significant resources were expended by

the two national laboratories and the results indicate that few, if any, risk-significant, functionally coupled systems interactions were uncovered. At least one interaction was uncovered which violated the plant's design basis.

Furthermore, it appears that the ability of one method or another to identify certain systems interactions is often more a function of the skill of the analyst and the modeling detail, than it is a function of a particular method. From this, the staff concluded that there is no one solution to the systems interaction issue and, therefore, focused on a more limited type of analyses. The basis for this was the possibility that a more directed effort, by any number of methods, may be cost effective if it can be determined that certain areas are more prone to significant adverse systems interactions. To this end, the operating experience search was intended to highlight such areas (see Section 5.4). The Indian Point 3 demonstration did point out that the electrical power system, or portions of it, may be such an area. In particular, the study provides some indication that electrical distribution systems sometimes are not designed with total redundancy and channelization and usually include significant non-safety/safety interfaces which make them prone to hidden dependencies.

#### 5.4 Search for Common-Cause Events in Operating Experience

As part of the effort to provide a more focused approach for the resolution of A-17, a set of tasks was defined to search operating experience in order to accumulate a data bank on the types of common-cause events of concern.

The major portion of this work was performed by ORNL, and a summary of ORNL's findings is included in NRC's document, NUREG/CR-3922.

The search emphasized events included in the LER files and involved a screening of those events based on the Task Action Plan definition. On the basis of the characteristics or attributes of the systems interaction events, a group of general categories of SI events was developed. In this manner, it was anticipated that generic areas of concern could be highlighted for possible further action. The results of the ORNL experience review indicate 23 general categories of events that have involved systems interactions. Those categories are listed in Table 4.

From these categories, the staff sought to establish possible safety significance (NUREG/CR-4261). This involved consideration of completed or ongoing related regulatory action. In this manner, it was anticipated that some areas would need no further action and any remaining areas of concern could then be evaluated for potential safety significance. In general, where extensive regulatory action was involved, such as IE bulletins or vendor notifications, the event and action taken could be shown to involve other than plant-specific features. The categories for which little regulatory action was taken often involved scenarios that were specific to a particular plant.

The staff then reviewed all the categories to see if some generic aspects related to adverse systems interaction concerns should be identified for action on all plants. The areas are summarized below on the basis of the type of coupling exhibited, i.e., functional, spatial, or induced human intervention. ORNL also looked at the general adequacy of the ongoing evaluations of operating experience.



Table 4 Event categories involving systems interactions

Category No.	Title	No. of events
1	Adverse interactions between normal or offsite power systems and emergency power systems	34
2	Degradation of safety-related systems by vapor or gas intrusion	15
3	Degradation of safety-related components by fire protection systems	10
4	Plant drain systems allow flooding of safety-related equipment	8
5	Loss of charging pumps due to volume control tank level instrumentation failures	6
6	Inadvertent ECCS/RHR pump suction transfer	4
7	HPSI/charging pumps overheat on low flow during safety injection	6
8	Level instrumentation degraded by HELB conditions	21
9	Loss of containment integrity from LOCA conditions during purge operations	10
10	HELB conditions degrading control systems	3
11	Auxiliary feedwater pump runout under steamline break conditions	2
12	Waterhammer events	4
13	Common support systems or cross-connects	18
14	Instrument power failures affecting safety systems	5
15	Inadequate cable separation	8
16	Safety-related cables unprotected from missiles generated from HVAC fans	3
17	Suppression pool swell	3
18	Scram discharge volume degradation	2
19	Induced human interactions	4
20	Functional dependencies from failures during seismic events	5
21	Spatial dependencies from failures during seismic events	13
22	Other functional dependencies	21
23	Other spatial dependencies	30

## 5.4.1 Functionally Coupled Type

### 5.4.1.1 Electric Power System

For purposes of this work, the electric power system includes the offsite sources, the switchyard, the power distribution buses and breakers, onsite generating equipment, and the control power and logic to operate the breakers and start and load the diesel generators. Some of the lower voltage (typically 120-V ac and 125-V dc) power supply portion of the system is also dealt with under Section 5.4.1.5 below.

As outlined in NUREG/CR-3922 and NUREG/CR-4261, concerns were highlighted in the area of electric power systems in Categories 1 and 13 (Table 4). Three important factors appear to contribute to the possible significance of this area:

- (1) It is one of the most (if not the most) extensive support systems in a plant. Power is supplied from various sources including the offsite network, the main plant turbine-generator, and in certain situations, the safety-related diesel generators. Power is then distributed to various items of equipment for normal plant control which is not related to safety, various engineered safety features equipment which is safety related, and various items of equipment for shutdown and decay heat removal.
- (2) Given these system demands, the power system is therefore an inherently complex system. A large number of normal operating modes at the plant, as well as transient and accident situations, must be accommodated. Interfaces are created between redundant safety-related equipment as well as between non-safety-related equipment and the safety-related equipment. In addition, the power system itself relies on a number of other support systems such as HVAC and cooling water.
- (3) Because of individual plant requirements and situations (a number of significant events occur when the system is in any abnormal temporary alignment), each power system tends to have some unique aspects. Very few specific ASIs can be stated to be generically applicable; however, the staff believes that general classes of electric power events can be potentially generic.

ORNL (NRC, NUREG/CR-3922 and NUREG/CR-4261) categorized the electric power system concerns into four areas.

- (1) load sequencing/load shedding
- (2) diesel generator failures caused by specific operating modes
- (3) breaker failures due to loss of dc power
- (4) failures that propagate between the safety-related portion and the non-safety-related portion of the power systems

With respect to these four areas of concern, the staff noted that although regulatory practice has allowed non-safety-related equipment to be powered from safety-related buses, this practice has created the potential for a number of undesirable interactions. In such situations, the isolation devices protect the safety-related equipment. These isolation devices have been the subject of much concern, both in the main power supply area (such as breakers that open on fault

current or "accident" signals) and in the instrumentation and control power supply area (such as isolation transformers and other devices). In some cases, the "isolation" devices do not isolate the full range of undesirable events. In addition, there are other concerns that the investigation into the A-17 issue has focused on. The ASIs of note involve scenarios in which a non-safety-related load is supplied by a safety-related bus and the non-safety-related load is part of important plant operation and/or control. As a result, a failure in the safety-related portion can create a situation in which a plant transient event occurs and, simultaneously, significant safety-related equipment is unavailable because of the same failure. The most significant types of events appear to be those that involve the instrumentation and control power system. As stated below in the discussion of those specific power supplies, the staff believes that ongoing activities in the area of instrumentation and control power supplies should be integrated and should also address this type of concern.

#### 5.4.1.2 Plant Support Systems

Concerns related to the area of support systems were noted in Categories 1 (as stated, the electric power system is an extensive support system), 13, 14, 18, and 22 (Table 4). Since the electric power system was dealt with separately, the support systems considered here include cooling water systems; heating, ventilation, and air conditioning systems; lube oil systems; air supply systems; and instrumentation and control systems. As was pointed out for the electric systems, these types of support systems tend to be plant unique to some extent.

The main general concern with some of the support systems involves the potential for them to initiate an event and also degrade the systems necessary to mitigate that event. This potential breakdown in the defense-in-depth philosophy can exist in some plants; however, the safety significance is highly dependent on other plant mitigating features such as remaining independent trains of equipment.

Because the loss of these support systems (including the electrical power system) does not lead to events such as a large LOCA or an MSLB which require immediate operator action, the staff concludes that, except for catastrophic failures (see spatially coupled SIs, Section 5.4.2), the potential for recovery of these systems is very great. In conjunction with the conclusions regarding induced human-intervention-coupled SIs (see Section 5.4.3 below), the staff has not recommended a regulatory action in this area, except for spatially coupled interactions. The staff will, however, communicate to the industry this information on support systems.

#### 5.4.1.3 Incorrect Reliance on Failsafe Design Principles

One area of adverse systems interactions involved reactor protection (scram) systems, Category 18. The staff recognized that such ASIs could be significant because of the time response demanded of a trip system. An argument similar to the argument given above (that the operator could have the time to fix a problem) does not apply.

The staff believes that the types of ASI identified in the studies were the result of use of a design approach which actually requires the functioning of certain features (for instance, a BWR discharge volume had to be empty) and,

therefore, an incorrect reliance on fail-safe principles. In fact, the concern with the air system was due to reliance on incorrect failsafe principles. In that case, the air system was assumed to fail safe (i.e., bleed off) and, as a result, a partial failure, at some low pressure, went unanalyzed. Action was taken at all boiling water reactors to correct this problem. In addition, it was noted that the electrical supply system to this scram system also had been previously modified because of similar concerns. Specifically, the electrical power was assumed to fail safe, i.e., voltage going to zero and as a result, partial failure such as low voltage or high voltage went unanalyzed for a time.

Although the staff is concerned with such scenarios, the concern focuses on the reactor trip system and it is acknowledged that the resolution of A-9, "Anticipated Transient Without Scram (ATWS)," should resolve the concerns in the area of the reactor trip system (RTS). The staff acknowledges that there may be other areas of the plant in which incorrect use of failsafe principles has occurred, but in all cases except the RTS, it is concluded that the safety significance would be less because of the greater time available for the operator to take corrective action. The only exception may be during a large LOCA; however, the probability of a large LOCA occurring in conjunction with these types of partial failures should be low. The staff will, however, communicate to the industry this information on the use of failsafe principles.

#### 5.4.1.4 Automated Safety-Related Actions With No Preferred Failure Mode

Another area of adverse systems interactions which was highlighted involved the inadvertent actuation of an engineered safety features (Category 6), inadvertent emergency core cooling system/residual heat removal (ECCS/RHR) pump suction transfer. The most significant characteristic of this area appears to be that such a design feature does not have an "always" preferred (failure) mode. As a result, extra precautions may be needed to avoid (1) a failure to actuate when needed and (2) a failure that actuates the system when not required (i.e., inadvertently). Of particular note is the possibility of inadvertent actuation of these types of functions during testing or maintenance. It is fairly common practice to put portions of the actuation logics in a trip or actuated state and assume that the plant is then in a "safe" condition. Although this may be true for functions that have a preferred (failure) mode, it may not be a conservative assumption for these other functions that do not have an always preferred (failure) mode. The specific area of automatic ECCS switch to recirculation is the subject of a generic issue (GI) that is scheduled for prioritization, GI-24 (NUREG-0933, Rev. 2).

GI-24 will consider the aspect of possible untimely, inadvertent ECCS/RHR pump suction transfer; therefore, the staff concludes that further specific action as part of the A-17 resolution is not warranted. The task manager for A-17 will make the staff responsible for NUREG-0933 aware of the information developed in the ORNL study.

There is some additional concern that other ESF systems may similarly not always have a preferred failure mode. In general, almost all of these systems have been analyzed for inadvertent actuation from a functional standpoint. The staff will, however, communicate to the industry this information on the concern (regarding functionally coupled ASIs) for systems that do not have an always preferred failure mode.



#### 5.4.1.5 Instrumentation and Control Power Supplies

The ORNL review (NRC, NUREG/CR-3922) highlighted several events related to instrumentation and control (I&C) power supplies (Category 14). The events at all plants, and specifically at Babcock & Wilcox plants, have already received significant attention as outlined in the ORNL assessment (NRC, NUREG/CR-4261). As stated in Section 3.4.3, there was some concern that the potential for a significant event related to I&C power supply interactions may still exist. Because of this concern, further review work at ORNL was identified.

ORNL completed this work and summarized it in a report entitled, "Survey and Evaluation of Vital Instrumentation and Control Power Supply Events" (NRC, NUREG/CR-4470). The report included a number of I&C power supply failures, some of which led to initiation of a plant transient and partial disabling of a safety system or operator indication.

On the basis of the additional work performed by ORNL and the staff's further review of the area of I&C power, the staff concluded that a significant number of issues and industry efforts were already under way in this area. The results of the A-17 work in this area will be communicated to the industry for information. However, the conclusion that significant activity is already under way in this area has led the A-17 resolution to include a recommendation that all the issues related to I&C power be combined under one task action plan to better expedite and coordinate the work in this critical area. In addition, the ORNL report should be utilized in this combined task.

#### 5.4.2 Spatially Coupled Type

Spatial dependencies appeared in a number of categories, including 3, 4, 8, 10, 15, 16, 21, and 23 (Table 4). This information was used in conjunction with the review of the utility studies in the spatial area.

See Section 5.6 for the staff's conclusions regarding spatially coupled interactions.

#### 5.4.3 Induced Human-Intervention-Coupled Type

The limited treatment of the operator in the study of the A-17 issue (i.e., as a hardware link) resulted in only a few events in this specific area (Category 19) and, actually, these events could also be classified as another form of functional coupling. Of related interest are those events related to instrumentation and control power losses (Category 14), since such losses can also lead the operator to a false conclusion.

On the basis of actions taken independently of the A-17 issue in the area of operator indication and particularly the implementation of Regulatory Guide 1.97 and the issuance of I&E Bulletin 79-27, the staff concludes that no additional action should be required for adverse systems interactions of this type at this time. The A-17 investigation will supply any additional information uncovered as a result of instrumentation and control power supply investigations as input to GI-76 (NUREG-0933, Rev. 2).



#### 5.4.4 Adequacy of Ongoing Evaluations of Operating Experience

ORNL reviewed (NRC, NUREG/CR-4261) the existing programs for the reporting, evaluation, and dissemination of significant operating experience. This review included the activities considered by AEOD (Section 5.2.5) and I&E (Section 5.2.6) and efforts by the industry. On the basis of this review, ORNL concluded that adequate provisions are in place to continue to monitor the operating experience for adverse systems interactions regardless of whether they are specifically labeled as such.

The staff agrees with the ORNL conclusion and is, therefore, considering taking no action in the area of evaluation of operating experience, except for the one-time dissemination of the information from the ORNL study for ASI: (NRC, NUREG/CR-3922 and NUREG/CR-4261).

#### 5.4.5 Undesirable Results of Systems Interaction Events

Part of the effort to focus USI A-17 involved a set of definitions which included a set of undesirable results (see Section 3.2). Although no conclusion was reached as to the relative consequences or frequency of the various results (except for Undesirable Result 5 - see below), a closer evaluation of the nature of the events which involve these results led to certain observations. Undesirable Result 1 involves breakdowns in the independence of redundant safety systems, divisions, trains, etc. This is a clear violation of the single-failure criterion, and these events often result from errors such as design or installation errors. Although they sometimes involve subtle couplings, they are still caused by errors that probably cannot be rectified by providing additional guidance on the application of the single-failure criterion.

Undesirable Result 2, which addresses the degradation of a safety-related system by a system not related to safety, involves a similar observation: Independence or isolation is clearly required for these cases and typically errors, rather than subtle couplings, cause the problems.

Undesirable Results 3 and 4, on the other hand, involve coupling of any plant accident or transient event and the degradation of any safety system including operation information. This aspect of breakdowns in levels of defense in depth has not typically been the subject of as much guidance as the area of independence between safety systems and non-safety systems. One exception may be in regard to the potential for a LOCA or MSLB to result in an environment that can impact safety-related equipment. This area has been the subject of a large effort to qualify the plant equipment to survive these environments.

ASIs of note that were identified as a result of the A-17 study were events that involved a single failure, such as loss of a power supply or other support system which led to a transient and also led to the loss of a train of some mitigative feature.

Undesirable Result 5 was included in the A-17 issue to address events that may involve plant features such as locked doors or inaccessible areas. The search of operating experience uncovered only a few events of this type (NUREG/CR-3922). In addition, a prioritization (NUREG-0933) of a related area, GI-81, "Impact

of Locked Doors and Barriers on Plant and Personnel Safety," concluded that the issue should be dropped from further consideration. Therefore, the staff did not consider this type of adverse systems interaction further.

## 5.5 Probabilistic Risk Assessments

The following is extracted from the Introduction to NUREG/CR-3852, "Insight Into PRA Methodologies."

In 1975, a new approach to evaluating reactor reliability and risk - Probabilistic Risk Assessment (PRA) - was presented in the Reactor Safety Study (RSS), WASH-1400 [renumbered NUREG-75/014]. This approach is based upon the concept of defining reactor system functions required for specific challenges (event trees) and estimating the probability of failure of system and functional requirements (fault trees). Since the completion of the RSS, reliability and risk assessment methods have been slowly evolving to the degree that they have become generally accepted for providing a reasonable analysis of the safety of a nuclear power plant. During the mid to late 1970s, the Reactor Safety Study Methodology Applications Program (RSSMAP) developed the concept of dominant accident sequences to simplify the construction of detailed event and fault trees. Following RSSMAP, the Interim Reliability Evaluation Program (IREP) sponsored five reliability assessments to determine plant differences by utilizing a variety of probabilistic assessment methods and implementation techniques. In addition to these NRC-sponsored studies, the nuclear power industry has conducted a number of reliability and risk studies. Examples include the Zion, Indian Point, Oconee, and Limerick PRAs. These studies have also made significant advances to the state of the art in probabilistic analysis.

At the present time about 20 probabilistic safety analyses on specific nuclear power plants have been completed. All of the studies are primarily based on the methods developed in the Reactor Safety Study. However, most of the studies have attempted to improve upon the original probabilistic concepts.

Many of the studies, to one degree or another, address some aspects of the general subject area of systems interactions. Adverse systems interactions constitute a small subset of the general area referred to as "dependencies" in a PRA. The dependencies related to systems interactions involve topic areas such as Modeling of AC Power Systems and Modeling of Logic (Actuation) Systems. There are many other dependencies dealt with which are not systems interactions. Among these are evaluation of human error and common mode analysis.

Reports published on probabilistic risk assessment (NRC, NUREG-1050, NUREG/CR-2300, and NUREG/CR-2815) have consistently identified the area of dependencies as critical to the accuracy of the studies. The failure to adequately treat dependencies, including adverse systems interactions, will repeatedly cause the results to underestimate overall risk.

In terms of probabilities, cutsets include independent events so that  $P_{AB} = P_A \cdot P_B$ . However, where there is some dependency,  $P_{AB}$  is greater than

$P_A \cdot P_B$ . Clearly, by A-17 definitions, not all such dependencies are due to adverse systems interactions because a dependency such as could arise from common maintenance practices (e.g., the case of the Salem A and B scram breakers, NUREG-1000) would also be such a dependency. If a PRA would, through very detailed modeling, include all the system and initiating event dependencies (including functional and spatial dependencies), then it would address all concerns for systems interactions.

No PRA to date has been able to make this sort of claim; however, many have highlighted significant system dependencies that are related to the systems interaction issue.

Additional work has been performed in the general subject area of common-cause event analysis. A guide (NRC, NUREG/CR-4780) has been prepared to aid in performing a common-cause analysis as part of a risk or reliability analysis. The guide reflects many years of research by the authors and others in the treatment of dependent failures in reliability and risk studies. As such, it references much related work by organizations such as the Electric Power Research Institute and Pickard, Lowe, and Garrick, Inc.

During its study leading to the resolution of USI A-17, the staff considered both the PRA methods used in these areas and significant systems interactions highlighted by individual studies.

#### 5.5.1 PRA Methods

ORNL reviewed the relationship of systems interactions to PRAs (NRC, NUREG/CR-4261) and concluded that there are three keys to adequately model systems interaction dependencies in a PRA:

- (1) The model must provide adequate detail about the systems. This detail is required to identify functional interactions that occur because support systems fail and is also necessary for examining spatial interactions.
- (2) The model must utilize extensive plant-specific information. This information includes the location of safety-related equipment and its proximity to both redundant equipment and to items that could affect its safety function. Through the use of such plant-specific information, the spatial systems interactions could be identified. Plant-specific information is also needed for identifying functional interactions that can occur in support equipment such as cooling water and electric power systems.
- (3) The models must consider off-normal (i.e., other than anticipated) modes of operation. A number of the systems interactions identified in an operating experience review (see Section 5.4) involved off-normal conditions during which equipment failed because the designer did not anticipate all conditions.

One of the greatest advantages of this type of plant modeling may be found in the process itself: By following patterns of investigation dictated by application of the techniques, the analyst takes a systematic look at plant design and operation. This can provide more insights than just those gained in the traditional design-review process.

To provide a reasonably accurate estimate of the probabilities of accident sequences, a PRA must consider dependencies between the systems and initiating events in the sequence. In some cases this has been done through system failure probabilities (which are derived from failure data that include such things as support system failure) and in other cases explicit detailed modeling has accounted for them.

In either case, the process must include the normal, recognized, systems interaction (e.g., where Train A cooling water supports Train A high-pressure injection through bearing cooling). To resolve issue A-17, a PRA would also have to address the adverse systems interactions. The problem (with respect to A-17) is that the dependencies of concern (referred to as adverse systems interactions) are sometimes so hidden or subtle that the analyst would not recognize them and, therefore, would not account for them either in the failure probabilities or through the modeling process.

The staff has concluded that it is not necessary (or even logical) to perform a separate, full-plant-scope study, such as a PRA, solely for the purpose of addressing adverse systems interactions. However, if for other reasons a PRA is performed, the A-17 program results provide the following guidance.

With respect to future PRAs, the staff concludes that numerous methods are available for identifying the adverse systems interactions, but it is more a question of the amount of effort (and therefore dollars) one can expend. Therefore, contrary to the expectation expressed in NUREG/CR-2815, "Probabilistic Safety Analysis Procedures Guide," the staff does not endorse one methodology. On the other hand, the staff reinforces the conclusions reached in NUREG/CR-2815 regarding functional dependencies and physical dependencies.

Specifically, NUREG/CR-2815 concludes:

(1) Functional Dependenc[i]es

All functional dependenc[i]es should in principle be identified at the FMEA phase and/or included in a correctly drawn fault tree. A fault tree should contain in particular all the shared-hardware and direct-process-coupling types of dependenc[i]es. Additional functional dependenc[i]es could be identified if the basic events in the fault trees are further decomposed to simpler events. The level of resolution in a fault tree depends on whether the analyst believes that a dependence could possibly exist at lower levels and on the relevant significance of such dependenc[i]es.

In this last regard, the A-17 program has highlighted a number of areas of concern which should be the focus of such resolution by the analyst (see Section 5.4).

(2) Physical Dependenc[i]es

A search of physical dependenc[i]es generally consists of generating minimal cutsets and examining whether the elements of these sets are susceptible to the same generic causative factor and in addition are connected by an "environmental" conductor that will



allow such a dependence to be created by a single source. Computer-aided search procedures have been developed for this purpose and are described in Section 3.7.3.9 of the ANS/IEEE, "PRA Procedures Guide" [NUREG/CR-2300].\* In applying these techniques, the information generated during the FMEA and put in the form of generic causative factors list is extremely useful.

Special caution should be exercised if codes that generate minimal cutsets using cutoff probabilities are employed, in order to avoid missing important dependenc[i]es contained in the rejected cutsets.

For certain physical dependenc[i]es the search within minimal cutsets can be combined with the PASNY\*\* approach of identifying "targets" and "sources" for these interactions. If critical combinations of "targets" to be examined during "walkthroughs" are defined on the basis of the minimum cutsets, then the efficiency of the "walkthrough" procedure will improve substantially.

As concluded elsewhere (see Section 5.6 on spatial interactions), the staff believes that a focused walkthrough review could be beneficial to safety. If a specific plant PRA is available, the targets and sources could be identified on the basis of the minimal cutsets and the procedure could be improved substantially.

#### 5.5.2 ASIs Identified From Review of PRA Results

The following ASIs were identified from a review of a number of PRAs (NRC memorandum, December 3, 1984, and May 31, 1985) based on the description of the events as compared to the definitions in the A-17 Task Action Plan.

##### 5.5.2.1 Support Systems

- (1) Direct-current bus supplies actuation power to the turbine-driven emergency feedwater pump and to a diesel generator breaker. Therefore, a single dc bus failure (the breaker connecting the bus fails to close) disables two emergency feedwater pumps in the event of a loss of offsite power.
- (2) Stripping vital loads from the safety buses on a safety injection signal (even though offsite power has not been lost) and then reloading them sequentially on the bus reduces the reliability of the safety function.
- (3) Direct-current bus faults can cause a reactor trip initiating event with concomitant failure of multiple core and containment cooling system trains.
- (4) Failures in the component cooling water (CCW) system have been identified as extremely important support system failures which have the potential of being an initiating event along with disabling mitigative systems required

---

\*Prepared for NRC under auspices of ANS/IEEE.

\*\*Power Authority of the State of New York, now called New York Power Authority (NYPA).



for that sequence. These aspects are discussed together in the next section, "Initiating Events."

- (5) A pipe failure in an air supply system results in failure of all automatic depressurization system (ADS) valves.

#### 5.5.2.2 Initiating Events

- (1) A CCW system pipe break causes loss of cooling to the reactor coolant pump seals and to the charging pumps which provide seal injection flow. Loss of seal cooling and injection flow may result in seal failure (i.e., small LOCA). Core melt may ensue because the high head safety injection pumps (ECCS) also fail when CCW system cooling is lost. Thus, a single initiating event (loss of CCW) may directly result in core melt.
- (2) Loss of cooling to reactor pump seals for short periods of time (30-60 minutes) may result in seal failure even when the reactor coolant pumps have been tripped.

These examples indicate that PRAs have indeed uncovered some adverse systems interactions. These examples of ASIs occur in the areas of support systems and initiating events coupled with mitigating system failures. They tend to reinforce the areas highlighted by the review of operating experience.

### 5.6 Study of Seismic/Spatially Coupled Systems Interactions

As the review of operating events and the review of utility SI studies progressed, it became apparent that a very large number of spatial interactions were possible. To attempt to understand these phenomena, a separate effort was defined to review this area. The approach for the review of SI studies was to compare the results of the IP3 study and the Diablo Canyon study, and from this information to draw conclusions about the possible safety significance of the interactions postulated and the costs associated with conducting a more focused program.

The major portion of this work was performed by Mark Technologies Corp. under subcontract to ORNL. That report (NRC, NUREG/CR-4306) addresses four major aspects of the programs. These aspects are the targets, the scope of the postulated initiating events, the postulated source failures, and the resulting documentation.

#### 5.6.1 Target Scope

The programs reviewed had broad target scopes. They considered most safety systems and one included refueling and fire protection components. The differences in scope in each of the programs appeared to have been based on plant-specific licensing and documentation considerations rather than on any cost/benefit or risk-based criteria. The target scope is the most important factor in the level of effort and cost for all of the programs reviewed.

#### 5.6.2 Initiating Events

A review of the programs shows that greater risk significance is associated with those initiators capable of challenging the plant support functions.

The greatest risk-significant initiators for the reactor coolant pressure boundary include seismic events and fires. Auxiliary feedwater and other frontline systems have significant risk only for plantwide events which are capable of challenging multiple frontline functions simultaneously (e.g., seismic, fire, flood, and possibly tornado winds). Tornado missiles, local internal missiles, and pipe failure (not seismically induced) do not pose significant plant risk outside the plant support systems.

### 5.6.3 Source Failures

All three programs have postulated large numbers of source failures for which limited historical data are available and even less quantitative evaluation has been performed. The program scopes of source failures included low-frequency initiating events such as high-energy line breaks, tornado missiles, plantwide floods, and low-probability seismically initiated component failures such as failure and falling of piping, raceways, and HVAC equipment. In addition to the low-frequency initiating failures, the programs postulated interaction with safety components such as large mechanical equipment, piping, etc., which could be capable of surviving some impacts. Other areas of source failure appear to have been less extensively covered. These include, most notably, the effects of water spray on electrical equipment. The postulation and treatment of water as a source was inconsistent in the documentation of both the walkdown and the flooding study portions of the programs. Limiting the study to only the most credible source initiators and the resulting credible interactions can produce reductions in cost and optimize risk benefit.

### 5.6.4 Documentation

Documentation of the three programs on an individual source/target basis took a lot of engineering and administrative time. Individual documents were generated, revised, edited, controlled, tracked, and sorted in the interests of ensuring traceability and unique identification of the thousands of potential, but in many cases, clearly low-probability, low-risk events. A streamlined and focused program could be developed with a level of documentation commensurate with the level of risk associated with the events being investigated.

### 5.6.5 Analysis of Spatially Coupled Systems Interactions

Each interaction is typically characterized by an initiating event or failure, a coupling or transmission of the failure effects, and a disabling of a target component, system, etc. Of particular note is the uncertain nature of each one of these characteristics. Unlike functionally coupled ASIs, in which a failure usually propagates directly through the connected systems and causes other failure in spatially coupled events, failure propagates through less direct paths and, as a result, other failures are less certain.

On the basis of its review, Mark Technologies Corp. outlined a relative ranking of the targets based on the perceived risk significance of the target groupings.

With respect to the targets, the support systems and controls were noted to be of greatest significance. The basis for this conclusion involves the fact that support systems and controls can potentially affect multiple frontline systems as well as possibly initiate a plant transient. In addition, controls (instrumentation, electrical devices, etc.) tend to be very sensitive to the type of

spatial phenomena (e.g., seismic, flood, spray) which are of concern. These are followed in decreasing importance by the reactor coolant pressure boundary, the auxiliary feedwater (AFW) system and controls, and the other frontline systems.

With respect to the source or initiating event scope, the programs considered a number of initiators which included seismic events, flood, fire, missiles, pipewhip, and tornado, depending on the target system involved.

The report (NRC, NUREG/CR-4306) discusses a simplified search methodology which could be applied to these target groupings and initiating events and provides cost estimates for such searches.

#### 5.6.6 Staff Conclusions

The staff generally agrees with the conclusions of NUREG/CR-4306.

The staff believes that for any future SI reviews, the target scope should be limited to the support systems and controls for the systems required for safe shutdown, the safe shutdown systems themselves, and the reactor coolant pressure boundary.

The staff does not believe that further review for spatially coupled interactions in the area of the ECCS is justified. These areas received a lot of review in the past. The review of the ECCS has not focused on all of the areas listed as concerns, but the need for this equipment is predicated on the occurrence of a LOCA which has a relatively low frequency of occurrence. In addition, the reactor coolant pressure boundary (RCPB) would be evaluated as a target system (both as the RCPB itself and under controls such as relief valves) and, therefore, the potential for a seismically induced LOCA caused by a spatially coupled ASI should be low.

Furthermore, the staff believes that the initiating events to be considered should include only those related to seismic events and fluid-related failures such as flooding and water intrusion, including spray from low- or moderate-energy piping. On the basis of other previous or ongoing activities, each of the other potential initiating events is believed to be adequately covered.

With respect to flooding, actions were taken at all plants as a result of the event at Quad Cities in 1972 (AEC letter, September 26, 1972). The actions taken should have addressed these areas of concern. (See also SRP Section 3.6.1 and Branch Technical Position (BTP) ASB 3-1.) However, there is some evidence that not all flooding and water-intrusion interactions were evaluated. Specifically, both the Diablo Canyon and Indian Point studies, as well as some of the SEP reviews (e.g., NUREG-0824) under Topic III-5.B, "Pipe Break Outside Containment," highlighted some potential interactions. In addition, operating experience has highlighted a number of events that have involved flooding and water intrusion (see Section 5.4.2). On the basis of these findings, the staff developed a number of insights in the area of flooding and water intrusion from internal sources (see the Appendix for additional information).

The area of fire protection has received significant attention as the result of action taken in response to Appendix R of 10 CFR 50. The overall fire reviews include the type of considerations identified in the Mark Technologies Corp.

report. Because of this, the staff is recommending taking no further action related to fire as a hazard. However, the fire suppression system itself may be a source for flood or spray.

(1) Turbine missiles and (2) tornados and tornado missiles have been the subject of a number of proposed generic issues, namely A-37 and A-38, respectively. These issues were prioritized "drop" and "low," respectively. In addition, the SEP group reviewed the area of internal missiles under Topic III-4.C and generally concluded that plants had adequate protection from internal missiles. On this basis, the staff is not recommending that these sources be pursued.

As a result of the above considerations and the spatially coupled ASIs uncovered by the operating experience review (see Section 5.4), the staff concludes that a focused search for certain spatially coupled systems interactions and appropriate corrective measures could benefit safety for some operating plants.

## 6 SUMMARY OF STAFF CONCLUSIONS

The resolution of any safety issue requires that the nature of the concern be clearly described. Concerns described as general subject areas, such as common cause, systems interactions, and dependent failure, can prove so broad that almost every conceivable safety issue could fall within the concern, and therefore the issue itself would prove unmanageable.

Therefore, to proceed with a resolution of the concerns expressed as "systems interactions," the NRC staff developed a set of definitions to attempt to give the safety concern narrower focus. As part of developing this definition, it was decided to take advantage of many ongoing efforts so that if some aspects that might be considered systems interactions were better addressed by other efforts, then the definitions would direct the A-17 effort away from those areas. As a result, a workable set of definitions was developed for the A-17 issue. Many other concerns were left to be addressed outside A-17. These definitions are crucial to the understanding of the issue and its resolution.

On the basis of the definitions, a number of tasks were defined. These tasks were structured to (1) make use of operating experience and other sources of actual or postulated events, (2) take maximum advantage of previous systems interaction studies, (3) evaluate the safety significance of systems interactions, and (4) evaluate the safety benefit and cost effectiveness of potential corrective measures.

Because systems interactions events are for the most part plant specific, the quantification of the potential safety significance was extremely difficult. Therefore, the safety benefit is based mostly on qualitative insights rather than quantitative analysis.

As a result of the investigation into adverse systems interactions the staff concluded the following:

- (1) To address a subject area such as "systems interactions" in its broadest sense tends to be an unmanageable task incapable of resolution. Some bounds and limitations are crucial to proceeding toward a resolution. Considering this, the staff studying the A-17 issue utilized a set of working definitions to limit the issue. It is recognized that such an approach may leave some concerns unaddressed.



- (2) The occurrence of an actual ASI or the existence of a potential ASI is very much a function of an individual plant's design and operational features (such as its detailed design and layout, allowed operating modes, procedures, and test and maintenance practices). Furthermore, the potential overall safety impact (such as loss of all cooling, loss of all electric power, or core melt) is similarly a function of those plant features that remain unaffected by the ASI. In other words, the results of an ASI depend on the availability of other independent equipment and the operator's response capabilities.
- (3) Although each ASI (and its safety impact) is unique to an individual plant, there appear to be some characteristics common to a number of the ASIs.
- (4) Methods are available (and some are under development) for searching out SIs on a plant-specific basis. Studies conducted by utilities and national laboratories indicate that a full-scope plant search takes considerable time and money. Even then, there is not a high degree of assurance all, or even most, ASIs will be discovered.
- (5) Functionally coupled ASIs have occurred at a number of plants, but improved operator information and training (instituted since the accident at Three Mile Island) should greatly aid in recovery actions during future events.
- (6) Induced human-intervention-coupled interactions as defined in A-17 are a subset of the broader class of functionally coupled systems interactions. As stated for functionally coupled SIs, improvements in both operator information and operator training will greatly improve recovery from such events.
- (7) As a class, spatially coupled SIs may be the most significant because of the potential for the loss of equipment which is damaged beyond repair. In many cases, these ASIs are less likely to occur because of the lower probability of initiating failure (e.g., earthquake, pipe rupture) and the less-than-certain coupling mechanisms involved. However, past operating experience highlighted a number of flooding and water intrusion events and more recent operating experience indicates that these types of events are continuing to occur (see the Appendix for additional information).
- (8) Probabilistic risk assessments or other systematic plant-specific reviews can provide a framework for identifying and addressing ASIs.
- (9) Because of the nature of ASIs (they are introduced into plants by design errors and/or by overlooking subtle or hidden dependencies), they will probably continue to happen. In their evaluations of operating experience, NRC and the nuclear power industry can provide an effective method for addressing ASIs.
- (10) For existing plants, a properly focused systematic plant search for certain types of spatially coupled ASIs and functionally coupled ASIs (and correction of the deficiencies found) may improve safety.



- (11) The area of electric power, particularly instrumentation and control power supplies, was highlighted as being vulnerable to relatively significant ASIs. Further investigation showed that this area remains the subject of a number of separate issues and studies. A concentrated effort to coordinate these activities and to include power supply interactions could prove an effective approach in this area.
- (12) For future plants, additional guidance regarding ASIs could benefit safety.
- (13) The concerns raised by the Advisory Committee on Reactor Safeguards (ACRS) on A-17, but which have not been addressed in the staff's study of A-17, should be considered as candidate generic issues, separate from USI A-17.

## 7 REFERENCES

- Advisory Committee on Reactor Safeguards, letter dated November 8, 1974, to the Director of Regulation of the AEC, "Systems Analysis of Engineered Safety Systems."
- , letter dated June 17, 1977, to Chairman of the NRC, "Report on the Zion Station, Units 1 and 2."
- , letter dated October 12, 1979, to Executive Director of Operations of the NRC, "Systems Interactions Study for Indian Point Nuclear Generating Unit No. 3."
- , letter dated May 13, 1986, to Executive Director of Operations of the NRC, "ACRS Comments on Proposal Resolution of USI A-17, "Systems Interactions in Nuclear Power Plants."
- Atomic Energy Commission, letter dated September 26, 1972, from R. C. DeYoung to licensees, "Flooding Event at Quad Cities, Unit 1."
- Atomic Industrial Forum, Inc., letter dated October 8, 1985, from M. R. Edelman to V. Stello "Unresolved Safety Issue A-17 Systems Interactions"
- Commonwealth Edison Company, "Zion Station Interaction Study," Docket 50-304, June 16, 1978.
- Consumers Power Company, "Program Manual Spatial Systems Interaction Program/ Seismic Midland Energy Center," Revision 1, June 6, 1983.
- Electric Power Research Institute, "Systems Interaction Identification Procedures," EPRI NP-3844, Vols. 1-5, July 1985.
- , EPRI NP-5613, see NUREG/CR-4780.
- Lawrence Livermore National Laboratory/Analytic Information Processing, Inc., "Preliminary Systems Interaction Results From the Digraph Matrix Analysis of the Watts Bar Nuclear Power Plant Safety Injection Systems," UCID-19707, June 1983.

Oak Ridge National Laboratory, ORNL/Letter Report, "Summary and Assessment of EPRI Report NP-3834 on 'Systems Interaction Identification Procedures'," February 10, 1986.

Office of Inspection and Enforcement, NRC, Bulletin 79-27, "Loss of Non-Class 1E Instrumentation and Control Power Systems Bus During Operation," November 30, 1979.

Pacific Gas and Electric Company, "Diablo Canyon Seismically Induced Systems Interaction Program," Dockets 50-275 and 50-323, May 7, 1984.

Power Authority of the State of New York, "Systems Interaction Study, Indian Point 3," Docket 50-286, November 30, 1983.

---, LER 84-010-000, Docket 50-286, July 16, 1984.

U.S. Nuclear Regulatory Commission, Memorandum dated September 18, 1984, from R. Kendall to D. Thatcher, "Comments on ORNL Draft NUREG/CR-092."

---, Memorandum dated December 3, 1984, from H. R. Denton to Division Directors, "Insights Gained From Probabilistic Risk Assessments."

---, Memorandum dated March 20, 1985, from A. Thadani to K. Kniel, "RRAB Inputs to the USI A-17 Program."

---, Memorandum dated May 31, 1985, from A. Thadani to K. Kneil, "RRAB Input to USI A-17 Resolution."

---, NUREG-75/014, "Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," October 1975.

---, NUREG-0471, "Generic Task Problem Descriptions (Categories B, C, and D)," June 1978.

---, NUREG-0572, "Review of Licensee Event Reports (1976-1978)," September 1979.

---, NUREG-0649, "Task Action Plans for Unresolved Safety Issues Related to Nuclear Power Plants," September 1984.

---, NUREG-0660, "NRC Action Plan Developed as a Result of the TMI-2 Accident," May 1980.

---, NUREG-0737, Supplement 1, "Clarification of TMI Action Plan Requirements: Requirements for Emergency Response Capability," January 1983.

---, NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," July 1981.

---, NUREG-0824, "Integrated Plant Safety Assessment Systematic Evaluation Program--Millstone Nuclear Power Station, Unit 1," February 1983.

---, NUREG-0933, "A Prioritization of Generic Safety Issues," revised frequently.

- , NUREG-0985, "Human Factors Program Plan," August 1983; Rev. 1, September 1984.
- , NUREG-1000, "Generic Implications of ATWS Events at the Salem Nuclear Power Plant," April 1983.
- , NUREG-1050, "Probabilistic Risk Assessment (PRA) Reference Document," Final Report, September 1984.
- , NUREG-1070, "NRC Policy on Future Reactor Designs," July 1985.
- , NUREG-1229, "Regulatory Analysis for Proposed Resolution of USI A-17," to be published.
- , NUREG/CR-1321, "Final Report - Phase I, Systems Interaction Methodology Applications Program," Sandia National Laboratories (SAND80-0884), April 1980.
- , NUREG/CR-1859, "Systems Interactions: State-of-the-Art Review and Methods Evaluation," Lawrence Livermore National Laboratory, January 1981.
- , NUREG/CR-1896, "Review of Systems Interaction Methodologies," Battelle Memorial Institute, January 1981.
- , NUREG/CR-1901, "Review and Evaluation of Systems Interactions Methods," Brookhaven National Laboratory, January 1981.
- , NUREG/CR-2300, "PRA Procedures Guide," Vols. 1 and 2, January 1983.
- , NUREG/CR-2815, "Probabilistic Safety Analysis Procedures Guide," Brookhaven National Laboratory, January 1984.
- , NUREG/CR-2915, "Initial Guidance on Digraph Matrix Analysis for Systems Interaction Studies," Lawrence Livermore National Laboratory (UCID-19457), March 1983.
- , NUREG/CR-3593, "Systems Interaction Results From the Digraph Matrix Analysis of a Nuclear Power Plant's High Pressure Safety Injection Systems," Analytic Information Processing and Lawrence Livermore National Laboratory, July 1984.
- , NUREG/CR-3852, "Insight Into PRA Methodologies," August 1984.
- , NUREG/CR-3922, "Survey and Evaluation of Systems Interaction Events and Sources," Oak Ridge National Laboratory, January 1985.
- , NUREG/CR-4179, "Digraph Matrix Analysis for Systems Interactions at Indian Point Unit 3, Abridged Version," Vol. 1, January 1986, Vols. 2-6 will be available in the NRC Public Document Room, 1717 H Street, N.W., Washington, D.C., Lawrence Livermore National Laboratory.
- , NUREG/CR-4207, "Fault Tree Application to the Study of Systems Interactions at Indian Point 3," Brookhaven National Laboratory, April 1985.
- , NUREG/CR-4261, "Assessment of System Interaction Experience in Nuclear Power Plants," Oak Ridge National Laboratory, June 1986.

---, NUREG/CR-4306, "Review and Evaluation of Spatial System Interaction Programs," Oak Ridge National Laboratory, December, 1986.

---, NUREG/CR-4470, "Survey and Evaluation of Vital Instrumentation and Control Power Supply Events," August 1986.

---, NUREG/CR-4780, "Procedures for Treating Common Cause Failures in Safety and Reliability Studies: Procedural Framework and Examples," January 1988.

---, SECY-84-133, "Results of SEP," Enclosure 4, "SEP Phase II Safety Lessons Learned" March 23, 1984.

*Camera  
ready*

Document Name:  
NUREG-1174 APPENDIX

Requestor's ID:  
BONNIE

Author's Name:  
D. Thatcher

Document Comments:  
ECS revised 5/1/89 please keep sheet with document



## APPENDIX

### INTERNAL FLOODING AND WATER INTRUSION INSIGHTS

Operating events have demonstrated the susceptibility of individual plant components to water intrusion and flooding from internal plant sources. Flooding, as discussed here, includes flooding of equipment by large volumes of water (i.e., equipment submergence) and other forms of water intrusion, including water spraying, dripping, or splashing on sensitive equipment. Examples of these types of events can be found in an operating experience review (References 1 and 2) conducted by the NRC and in individual NRC information notices (References 3-9). A key point apparent from these events is that the quantity of the water involved is not necessarily a measure of the problems that the water can create; the location of the water is much more significant. For example, a small leak that drips down through electrical equipment can have a more severe impact on the plant than an 8-foot flood in a pump compartment. Also, Generic Issue 77, "Flooding of Safety Equipment Compartments by Back-Flow Through Floor Drains," has received a high priority ranking (Reference 10) because of the possibility that plant designs have overlooked backflow through floor drains as a flooding pathway.

All plants should have conducted some flooding-type studies as part of demonstrating conformance to various requirements. These requirements were typically focused on large volumes of water and the potential for submerging equipment.

(1) The general design criteria (10 CFR Part 50, Appendix A) address the area of flooding. Specifically,

GDC 3, "Fire protection," states: "Fire fighting systems shall be designed to assure that their rupture or inadvertent operation does not significantly impair the safety capability of these structures, systems and components designated as important to safety."

GDC 4, "Environmental and dynamic effects missile design bases," states: "Structures, systems, and components important to safety shall be designed to accommodate the effects of and to be compatible with...normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents. These structures, systems and components shall be appropriately protected against dynamic effects, including the effects of missiles, pipe whipping, and discharging fluids, that may result from equipment failures and from events and conditions outside the nuclear power unit. However, dynamic effects associated with postulated pipe ruptures in nuclear power units may be excluded from the design basis when analyses reviewed and approved by the Commission demonstrate that the probability of fluid system piping rupture is extremely low under conditions consistent with the design basis for the piping."

(2) As part of environmental qualification requirements of 10 CFR 50.49, submergence was evaluated for certain equipment for water associated with design-basis events.

- (3) Generic letters issued to licensed facilities in 1972 required additional review based on an event at the Quad Cities plant.
- (4) For more recently licensed plants, the Standard Review Plan (Reference 11) cites the generic letters of 1972, and therefore, flooding-type analysis should have been performed as part of the licensing process.

In addition, all plants should have developed programs for the review of operating experience per the requirements of Item I.C.5 of NUREG-0737 (Reference 12). These reviews should include consideration of NRC information notices and other industry documents such as those issued by the Institute of Nuclear Power Operations (INPO). Both of these have included events involving flooding and water intrusion.

The staff has concluded that existing requirements lack specific guidance regarding water intrusion events that may involve small amounts of water and subtle paths of communication of water or moisture to sensitive equipment.

The staff also recognizes that it may not be possible to identify all subtle pathways and sources. However, the staff believes that risk could be reduced significantly by conducting a focused review that includes:

- (1) reviewing actual industry operating experience involving water intrusion for applicability to the licensee's plant
- (2) considering action such as sealing conduit or providing shields for sensitive equipment, and
- (3) examining safe-shutdown equipment specifically focusing on the potential for water intrusion problems. Safe-shutdown equipment for a flooding or water intrusion event would typically include the equipment needed to perform the following functions:
  - (a) Bring the plant to hot shutdown and establish heat removal.
  - (b) Maintain support systems necessary to establish and maintain hot shutdown.
  - (c) Maintain control room functions and instrumentation and controls necessary to monitor hot shutdown.
  - (d) Provide alternating current and/or direct current emergency power as needed on a plant-specific basis to meet the above three functions.

(Note: In addition to the above equipment, a review should include electrical equipment that could cause inadvertent actuation of components which in turn could hinder the ability to perform these functions (e.g., logic cabinets that actuate the automatic depressurization system).

On the basis of a large amount of industry experience, the staff has determined that a flooding (including water intrusion) analysis should address the aspects listed below. Water intrusion includes all forms of water or moisture release from water sources internal to plant structures (e.g., leaks or ruptures of water or steam sources or from fire-suppression system actuation). Regardless

of the means of release, the failure mechanism is intrusion of water or moisture to sensitive equipment (e.g., electrical cabinets).

(Note: If an analyses has been performed to demonstrate that the probability of fluid system piping rupture is extremely low under conditions consistent with the design basis for the piping (i.e., per revised GDC 4), then fluid discharge associated with that rupture may be excluded from further consideration.)

### Water Intrusion Considerations

#### (1) Sources

The water can and has been released by failure (e.g., leaks, ruptures), by system actuation (e.g., fire-suppression system), or by special plant situations during maintenance or testing. Actual operating experience has demonstrated problems that emanate from

- domestic water systems (toilets, sinks, eye-wash stations, etc.)
- fire-suppression equipment
- moderate energy piping systems such as circulating water
- maintenance actions (e.g., draining, venting)
- low-pressure steam and condensate leakage

#### (2) Pathways

Operating experience has demonstrated that separate rooms do not necessarily provide protection because of

- drain systems that may be plugged or allow backflow
- heating and ventilation ducts and penetrations between rooms
- unsealed doors
- unsealed or inadequately sealed electrical conduit and penetrations (either by design or from inadequate maintenance)
- unusual maintenance situations (temporary drain lines, water barriers)

#### (3) Operating Experience

Collective industry experience has been described in:

- NRC Information Notice 83-41, "Actuation of Fire Suppression System Causing Inoperability of Safety-Related Equipment," June 22, 1983
- NRC Information Notice 83-44, "Potential Damage to Redundant Safety Equipment As a Result of Backflow Through the Equipment and Floor Drain Systems," July 1, 1983

- NRC Information Notice 85-85, "Systems Interaction Event Resulting in Reactor System Safety Relief Valve Opening Following a Fire-Protection Deluge System Malfunction," October 31, 1985
- NRC Information Notice 86-106, Supplement 2, "Feedwater Line Break," March 18, 1987
- NRC Information Notice 87-14, "Actuation of Fire Suppression System Causing Inoperability of Safety-Related Ventilation Equipment," March 23, 1987
- NRC Information Notice 87-49, "Deficiencies in Outside Containment Flooding Protection," October 9, 1987
- NRC Information Notice 88-60, "Inadequate Design and Installation of Watertight Penetration Seals," August 11, 1988

#### REFERENCES

1. U.S. Nuclear Regulatory Commission, NUREG/CR-3922, "Survey and Evaluation of System Interaction Events and Sources," Vol. 1 and 2, January 1985.
2. ---, AEOD/C402, "Operating Experience Related to Moisture Intrusion in Electrical Equipment at Commercial Power Reactors," June 1984.
3. ---, Information Notice 83-41, "Actuation of Fire Suppression System Causing Inoperability of Safety-Related Equipment," June 22, 1983.
4. ---, Information Notice 83-44, "Potential Damage to Redundant Safety Equipment As a Result of Backflow Through the Equipment and Floor Drain Systems," July 1, 1983.
5. ---, Information Notice 85-85, "Systems Interaction Event Resulting in Reactor System Safety Relief Valve Opening Following a Fire-Protection Deluge System Malfunction," October 31, 1985.
6. ---, Information Notice 86-106, "Supplement 2: Feedwater Line Break," March 18, 1987.
7. ---, Information Notice 87-14, "Actuation of Fire Suppression System Causing Inoperability of Safety-Related Ventilation Equipment," March 23, 1987.
8. ---, Information Notice 87-49, "Deficiencies in Outside Containment Flooding Protection," October 9, 1987.
9. ---, Information Notice 88-60, "Inadequate Design and Installation of Watertight Penetration Seals," August 11, 1988.
10. ---, NUREG-0933, "A Prioritization of Generic Safety Issues," December 1983.

11. ---, NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," LWR edition, July 1981.
12. ---, NUREG-0737, "Clarification of TMI-2 Requirements," September 1980.



---

---

# Regulatory Analysis for Resolution of USI A-17

Systems Interactions in Nuclear Power Plants

---

---

**U.S. Nuclear Regulatory  
Commission**

Office of Nuclear Regulatory Research

D. F. Thatcher



REGULATORY ANALYSIS FOR  
RESOLUTION OF USI A-17

NUREG-1229

---

---

# Regulatory Analysis for Resolution of USI A-17

Systems Interactions in Nuclear Power Plants

---

---

Manuscript Completed:  
Date Published:

D. F. Thatcher

Office of Nuclear Regulatory Research  
U.S. Nuclear Regulatory Commission  
Washington, DC 20555



THIS DOCUMENT HAS  
*mb* BEEN PROOFREAD

Document Name:  
NUREG 1229 TC

Requestor's ID:  
MCKENZIE

Author's Name:  
THATCHER/Sanders

Document Comments:  
PH ECS 5/9/89 final KEEP THIS SHEET WITH DOCUMENT

## ABSTRACT

This report presents a summary of the regulatory analysis conducted by the NRC staff to evaluate the value and impact of potential alternatives for the resolution of Unresolved Safety Issue (USI) A-17, "Systems Interactions in Nuclear Power Plants." The NRC staff's proposed resolution offered in this report is based on this analysis. The staff's technical finding regarding systems interactions can be found in NUREG-1174.

Adverse systems interactions (ASIs) involve subtle and often very complicated plant-specific dependencies between components and systems, possibly compounded by inducing erroneous human intervention. The staff has identified actions to be taken by licensees and the NRC to resolve USI A-17; the staff has also made the judgment that these actions, together with other ongoing activities, would reduce the risk from adverse systems interactions. As discussed further in this report, the staff judgment that the proposed actions are sufficient is not based on the assertion that all systems interactions have been identified, but rather that the A-17 actions, plus other activities by the licensees and staff, will identify precursors to potentially risk-significant interactions so that action can be taken if deemed necessary.

## CONTENTS

		<u>Page</u>
	ABSTRACT .....	iii
	EXECUTIVE SUMMARY .....	vii
1	STATEMENT OF THE PROBLEM .....	1
2	SUMMARY OF TECHNICAL FINDINGS AND CONCLUSIONS .....	1
	2.1 Systems Interaction .....	3
	2.2 Adverse Systems Interaction .....	3
	2.3 Undesirable Result (Produced by SIs) .....	3
	2.4 Classification of Adverse Systems Interactions .....	3
	2.5 Conclusions .....	4
3	ALTERNATIVES .....	5
	3.1 Alternatives for Operating Plants .....	6
	3.2 Alternatives for Future Plants .....	6
	3.3 Alternatives for Improving Systematic Plant Reviews Such As Probabilistic Risk Assessments .....	7
	3.4 Alternatives for Evaluating Operating Experience .....	7
4	DISCUSSION OF ALTERNATIVES .....	7
	4.1 Alternatives for Operating Plants .....	7
	4.2 Alternatives for Future Plants .....	18
	4.3 Alternatives for Improving Systematic Plant Reviews (Such As PRAs) .....	19
	4.4 Alternatives for Evaluating Operating Experience .....	19
5	BASES FOR RESOLUTION OF UNRESOLVED SAFETY ISSUE A-17 .....	20
6	PROPOSED RESOLUTION .....	23
	6.1 Provide Information on ASIs to Ongoing Evaluations of Operating Experience .....	23
	6.2 Acknowledge Seismic SI Aspects of USI A-46 Implementation ..	25
	6.3 Consider Flooding and Water Intrusion From Internal Sources in Individual Plant Examinations .....	25
	6.4 Provide for the Integration and Coordination of Electrical and Instrumentation and Control Power Supply Issues and Concerns .....	28
	6.5 Provide Guidance for Future PRA or Other Systematic Plant Reviews .....	28
	6.6 Define Potential Generic Issues That Are Not Included As Part of the A-17 Resolution or Other Regulatory Programs ...	29
	6.7 Develop a Standard Review Plan for Future Plants .....	29
7	REFERENCES .....	29



## EXECUTIVE SUMMARY

The U.S. Nuclear Regulatory Commission (NRC) has concluded its technical evaluation of Unresolved Safety Issue (USI) A-17, "Systems Interactions in Nuclear Power Plants." The present report summarizes the results of the regulatory analysis conducted by the NRC staff to formulate the resolution of USI A-17. The technical findings and conclusions used in this report are based on those presented in NUREG-1174, "Evaluation of Systems Interactions in Nuclear Power Plants: Technical Findings Related to Unresolved Safety Issue A-17."

As emphasized in NUREG-1174, the set of definitions is critical to proceeding with resolution of the issue. Those definitions are repeated in this document.

Because of the complex and interdependent network of systems, structures, and components that constitute a nuclear power plant, the scenario of almost any significant event can be characterized as a "systems interaction." As a result, the staff recognized that if the term "systems interaction" were interpreted in a very broad sense it became an unmanageable safety issue. To begin to address perceived safety concerns within this potentially broad subject area, requires a narrowing of the scope. To this end, a set of definitions based on the perceived safety concerns has been developed.

It is recognized that by narrowing the focus, all concerns that could be characterized as systems interactions may not be addressed. It is, therefore, extremely important that the scope and boundary of the program be as clearly defined (and understood) as possible. Then, should concerns still exist after the program has been completed, those concerns could be addressed as part of any separate efforts deemed necessary.

The following terms and definitions were used in the A-17 program:

(1) Systems Interaction (SI)

An action or inaction (not necessarily a failure) of various systems (subsystems, divisions, trains), components, or structures resulting from a single credible failure within one system, component, or structure and propagation to other systems, components, or structures by inconspicuous or unanticipated interdependencies. The major difference between an SI and a classic single-failure event is in those hidden or unanticipated aspects of the initiating failure and/or its propagation.

(2) Adverse Systems Interaction (ASI)

A systems interaction that produces an undesirable result.

(3) Undesirable Result (Produced by SIs)

This was defined by a list of the types of events that were to be considered in USI A-17.

- Degradation of redundant portions of a safety system, including consideration of all auxiliary support functions. Redundant portions are those considered to be independent in the design and accident analysis (Chapter 15) of the Final Safety Analysis Report (FSAR) of the plant. (Note: This would violate the single-failure criterion.)
- Degradation of a safety system by a non-safety system. (Note: This result would demonstrate a breakdown in presumed "isolation.")
- Initiation of an "accident" [e.g., loss-of-coolant accident (LOCA), main steamline break (MSLB)] and (a) the degradation of at least one redundant portion of any one of the safety systems required to mitigate that event (Chapter 15, FSAR analyses) or (b) degradation of critical operator information sufficient to cause the operator to perform unanalyzed, unassumed, or incorrect actions. (Note: This includes failure to perform correct actions because of incorrect information.)
- Initiation of a "transient" (including reactor trip) and (a) the degradation of at least one redundant portion of any one of the safety systems required to mitigate the event (Chapter 15, FSAR analyses) or (b) degradation of critical operator information sufficient to cause the operator to perform unanalyzed, unassumed, or incorrect actions. (Note: This includes failure to perform correct actions because of incorrect information.)
- Initiation of an event that requires plant operators to act in areas outside the control room (perhaps because the control room is being evacuated or the plant is being shut down) and disruption of the access to these areas (for example, by disruption of the security system or isolation of an area when fire doors are closed or a suppression system is actuated).

The intersystem dependencies (or systems interactions) have been divided into three classes based on the way they propagate:

(1) Functionally Coupled

Those SIs that result from sharing of common systems/components; or physical connections between systems, including electrical, hydraulic, pneumatic, or mechanical.

(2) Spatially Coupled

Those SIs that result from sharing or proximity of structures/locations, equipment, or components or by spatial inter-ties such as heating, ventilation, and air conditioning (HVAC) and drain systems.

(3) Induced Human-Intervention Coupled

Those SIs that result when a plant malfunction (such as failed indication) inappropriately induces an operator action, or when a malfunction inhibits an operator's ability to respond. As analyzed in the A-17 program, these SIs are considered another example of functionally coupled ASIs. (Note: Random human errors and acts of sabotage are excluded.)

As a result of the staff's studies of alternative actions that might resolve the A-17 safety issue, the staff has concluded that certain actions should be taken. These actions are:

- (1) Send a generic letter to all plants providing information developed during the resolution of A-17.
- (2) Consider flooding and water intrusion from internal plant sources in the Individual Plant Examinations (IPEs).
- (3) Consider systems interactions involving the electrical power systems in the integrated program on electrical power reliability.
- (4) Provide information for use in future probabilistic risk assessments (PRAs).
- (5) Provide a framework for addressing those other concerns related to systems interactions which are not covered by the A-17 program.
- (6) Acknowledge that the resolution of USI A-46 addresses aspects of systems interactions.
- (7) Develop a standard review plan for future plants to address protection from internal flooding and water intrusion.

THIS DOCUMENT HAS  
BEEN PROOFREAD  
MK

Document Name:  
NUREG 1229 TEXT

Requestor's ID:  
MCKENZIE

Author's Name:  
Thatcher/Sanders

Document Comments:  
PH ECS 5/9/89 Final KEEP THIS SHEET WITH DOCUMENT

# REGULATORY ANALYSIS FOR PROPOSED RESOLUTION OF USI A-17: SYSTEMS INTERACTIONS IN NUCLEAR POWER PLANTS

## 1 STATEMENT OF THE PROBLEM

A nuclear power plant is composed of numerous systems, structures, and components which are designed and analyzed by several engineering disciplines. The degree of functional and physical integration of all these systems, components, and structures into any single power plant may vary considerably. Concerns have been raised which question the adequacy of this functional and physical integration coordination process. Also, it has been postulated that adverse systems interactions (ASIs) may be inadvertently incorporated into plants by inadequacies in the process. Given that a nuclear power plant includes many systems, components, and structures, including (1) systems that normally control the plant, (2) systems that respond to off-normal events, and (3) systems that both functionally and physically support other systems, it is reasonable to suspect that such interactions may exist. Current regulatory requirements and guidance address this area. The unresolved safety issue (USI) A-17 program was initiated to investigate the area of systems interactions and to consider viable alternatives for regulatory requirements (including doing nothing) to ensure that adverse systems interactions have been or will be minimized at operating plants and at new plants.

## 2 SUMMARY OF TECHNICAL FINDINGS AND CONCLUSIONS

The technical findings and conclusions presented here are based on the results reported in NRC staff report NUREG-1174.

Because a nuclear power plant is composed of systems, structures, and components both complex and interdependent, any significant event scenario can potentially be characterized as a "systems interaction." As a result, the staff has determined that if the term systems interaction were interpreted in its broadest sense, it became an unmanageable safety issue. To begin to address perceived safety concerns within this potentially broad subject area, requires some focusing. One way to focus on such an effort is to develop a working set of definitions based on the perceived safety concerns.

It is recognized that by the very nature of narrowing the focus, all concerns that could be characterized as systems interactions may not be addressed. It is, therefore, extremely important that the scope and boundary of the focused program be as clearly defined (and understood) as possible. Then, should concerns still exist after the program has been completed, those concerns could be addressed as part of any separate efforts deemed necessary.

The terms and definitions used in the A-17 program follow in Sections 2.1 through 2.4. In addition, Table 1 (which is reproduced here from NUREG-1174) is included to help clarify the scope of A-17 and its bases.



Table 1 Scope of USI A-17, "Systems Interactions": General subject area involves system failures which are due to system dependencies

Concerns	Covered by	Clarification
(1) Recognized/analyzed single failures directly propagate to other equipment/systems within the same safety division	Existing regulations • Single failure defined in the GDC	Not analyzed in A-17
(2) Single failures subtly propagate to cause plant transients/accidents and/or degrade the required safety systems. Includes: • Subtle spatial interties • Subtle functional interties	USI A-17 definition of adverse systems interactions	
(3) Common failure of redundant safety systems due to commonalities such as: • Same manufacturing defect • Same testing error • Same maintenance error	Improvements in maintenance and test procedures, ATWS rule, A-44 proposed rule	Not analyzed in A-17
(4) Operator errors that disable redundant safety systems	Improvements in operator training	Not analyzed by A-17
(5) Events that could cause multiple plant problems simultaneously: • Particularly earthquakes • Also fire and pipe break/flooding	USI A-46 plus current licensing requirements cover earthquakes  Appendix R deals with fire  Equipment qualification rule (10 CFR 50.49) deals with design-basis pipe breaks  None of these programs deals with multiple, simultaneous events. Therefore, this area is to be further evaluated under the Multiple System Responses Program.	Not analyzed in A-17, except for internal flooding/water intrusion events occurring one at a time

## 2.1 Systems Interaction

A systems interaction (SI) is an action or inaction (not necessarily a failure) of various systems (subsystems, divisions, trains), components, or structures resulting from a single credible failure within one system, component, or structure and propagation to other systems, components, or structures by inconspicuous or unanticipated interdependencies. The major difference between an SI and a classic single-failure event is in those hidden or unanticipated aspects of the initiating failure and/or its propagation.

## 2.2 Adverse Systems Interaction

An adverse systems interaction (ASI) is an SI that produces an undesirable result.

## 2.3 Undesirable Result (Produced by SIs)

A list of types of events that were to be considered in USI A-17 defines this term:

- (1) Degradation of redundant portions of a safety system, including consideration of all auxiliary support functions. Redundant portions are those considered to be independent in the design and accident analysis (Chapter 15) of the Final Safety Analysis Report (FSAR) of the plant. (Note. This would violate the single-failure criterion.)
- (2) Degradation of a safety system by a non-safety system (Note: This result would demonstrate a breakdown in presumed "isolation.")
- (3) Initiation of an "accident" [e.g., loss-of-coolant-accident (LOCA), main steamline break (MSLB)] and (a) the degradation of at least one redundant portion of any one of the safety systems required to mitigate that event (Chapter 15, FSAR analyses) or (b) degradation of critical operator information sufficient to cause the operator to perform unanalyzed, unassumed, or incorrect actions. (Note: This includes failure to perform correct actions because of incorrect information.)
- (4) Initiation of a "transient" (including reactor trip) and (a) the degradation of at least one redundant portion of any one of the safety systems required to mitigate the event (Chapter 15, FSAR analyses) or (b) degradation of critical operator information sufficient to cause the operator to perform unanalyzed, unassumed, or incorrect actions. (Note: This includes failure to perform correct actions because of incorrect information.)
- (5) Initiation of an event that requires plant operators to act in areas outside the control room (perhaps because the control room is being evacuated or the plant is being shut down) and disruption of the access to these areas (for example, by disruption of the security system or isolation of an area when fire doors are closed or when a suppression system is actuated).

## 2.4 Classification of Adverse Systems Interactions

The intersystem dependencies (or systems interactions) have been divided into three classes based on the way they propagate:

(1) Functionally Coupled

Those SIs that result from sharing of common systems/components; or physical connections between systems, including electrical, hydraulic, pneumatic, or mechanical.

(2) Spatially Coupled

Those SIs that result from sharing or proximity of structures/locations, equipment, or components, or by spatial inter-ties such as heating, ventilation, and air conditioning (HVAC) and drain systems.

(3) Induced Human-Intervention Coupled

Those SIs that result when a plant malfunction (such as failed indication) inappropriately induces an operator action, or when a malfunction inhibits an operator's ability to respond. As analyzed in the A-17 program, these SIs are considered another example of functionally coupled ASIs. (Note: Random human errors and acts of sabotage are excluded.)

2.5 Conclusions

As a result of the staff's studies of ASIs undertaken as part of its search for a solution to the USI A-17 safety issue, the staff has concluded the following:

- (1) To address a subject area such as "systems interactions" in its broadest sense tends to be an unmanageable task incapable of resolution. Some bounds and limitations are crucial to proceeding toward a resolution. Considering this, the A-17 program utilized a set of working definitions to limit the issue. It is recognized that such an approach may leave some concerns unaddressed.
- (2) The occurrence of an actual ASI or the existence of a potential ASI is very much a function of an individual plant's design and operational features (such as its detailed design and layout, allowed operating modes, procedures, and test and maintenance practices). Furthermore, the potential overall safety impact (such as loss of all cooling, loss of all electric power, or core melt) is similarly a function of those plant features that remain unaffected by the ASI. In other words, the results of an ASI depend on the availability of other independent equipment and the operator's response capabilities.
- (3) Although each ASI (and its safety impact) is unique to an individual plant, there appear to be some characteristics common to a number of the ASIs.
- (4) Methods are available (and some are under development) for searching out SIs on a plant-specific basis. Studies conducted by utilities and national laboratories indicate that a full-scope plant search takes considerable time and money. Even then, there is not a high degree of assurance all, or even most, ASIs will be discovered.

- (5) Functionally coupled ASIs have occurred at a number of plants, but improved operator information and training (instituted since the accident at Three Mile Island) should greatly aid in recovery actions during future events.
- (6) Induced human-intervention-coupled interactions as defined in A-17 are a subset of the broader class of functionally coupled SIs. As stated for functionally coupled SIs, improvements in both operator information and operator training will greatly improve recovery from such events.
- (7) As a class, spatially coupled SIs may be the most significant because of the potential for the loss of equipment which is damaged beyond repair. In many cases these ASIs are less likely to occur because of the lower probability of initiating failure (e.g., earthquake, pipe rupture) and the less-than-certain coupling mechanisms involved. However, past operating experience highlighted a number of internal flooding and water intrusion events and more recent operating experience indicates that these type of events are continuing to occur.
- (8) Probabilistic risk assessments or other systematic plant-specific reviews can provide a framework for identifying and addressing ASIs.
- (9) Because of the nature of ASIs (they are introduced into plants by design errors and/or by overlooking subtle or hidden dependencies), they will probably continue to happen. In their evaluations of operating experience, NRC and the nuclear power industry can provide an effective method for addressing ASIs.
- (10) For existing plants, a properly focused, systematic plant search for certain types of spatially coupled ASIs and functionally coupled ASIs (and correction of the deficiencies found) may improve safety.
- (11) The area of electric power, and particularly instrumentation and control power supplies, was highlighted as being vulnerable to relatively significant ASIs. Further investigation showed that this area remains the subject of a number of separate issues and studies. A concentrated effort to coordinate these activities and to include power supply interactions could provide a more effective approach in this area.
- (12) For future plants, additional guidance regarding ASIs could benefit safety.
- (13) The concerns raised by the Advisory Committee on Reactor Safeguards (ACRS) on A-17, but which have not been addressed in the staff's study of A-17, should be considered as candidate generic issues, separate from USI A-17.

Although there does not seem to be a generic safety concern that warrants immediate attention, some potential exists for plant-specific problems and, therefore, alternatives for action were considered further.

### 3 ALTERNATIVES

The alternatives considered were grouped into four areas:

- (1) the need to take action at operating plants



- (2) the adequacy of current licensing requirements and guidance (for future plants)
- (3) the possibility of providing additional guidance for those utilities which perform a systematic safety analysis such as a probabilistic risk assessment (PRA)
- (4) the adequacy of the existing processes for review and evaluation of operating experience

Then for each of these areas, various alternatives were considered as discussed below.

### 3.1 Alternatives for Operating Plants

- (1) Requiring a comprehensive plant study would involve modeling the plant dependencies (functional and spatial) and then evaluating them.
- (2) Taking no action would involve addressing only the requirements already resulting from previous attention to ASIs, such as staff bulletins and generic letters.
- (3) Requiring all plants to meet a prescriptive set of specific generic requirements would involve implementing specific plant actions and/or modifications to specific systems. In the past, this approach has been used for individual ASIs.
- (4) Requiring all plants to provide a separate and independent, alternate shutdown system would involve the design and implementation of a functionally and physically independent plant system(s) that would be free from ASIs with respect to the rest of the plant.
- (5) Requiring all plants to do a focused individual study in specific areas for spatially coupled and functionally coupled ASIs would necessitate that individual plants do evaluations in rather specific areas based on guidelines that would focus the more significant concerns for ASIs. As a result of individual plant evaluations, actions may be required.

### 3.2 Alternatives for Future Plants

- (1) Adding a new and separate ASI review section to the Standard Review Plan would inaugurate a new section in the Standard Review Plan (SRP) (NUREG-0800) containing a set of acceptance criteria and review guidelines, and designating a lead review branch.
- (2) Taking no action would indicate that the requirements and guidance in the SRP are adequate and no new guidance is necessary.
- (3) Providing additional regulatory guidance/criteria for ASIs would consider the existing regulatory guidance (e.g., acceptance criteria and review guidelines) in the appropriate sections of the SRP and would establish the adequacy of the guidance. Where the guidance is inadequate, individual revisions would be proposed.



### 3.3 Alternatives for Improving Systematic Plant Reviews Such As Probabilistic Risk Assessments

- (1) Providing additional guidance for future systematic reviews would involve developing new guidance to such studies.
- (2) Taking no action would conclude that present guidance is sufficient.
- (3) Requiring a specific search method for uncovering ASIs would endorse one particular method as the solution for the subject area of ASIs and would recommend that all systematic type reviews use it.

### 3.4 Alternatives for Evaluating Operating Experience

- (1) Providing for new recommendations in the future evaluation of operating experience for ASIs would consider the existing programs that deal with operating experience and would make recommendations for improving them to address ASIs.
- (2) Taking no action would consider the present programs for the review and dissemination of operating experience and would conclude that they are adequate with respect to ASIs.
- (3) Providing information on ASIs to ongoing evaluations of operating experience would involve the one-time dissemination of information developed regarding ASIs.

## 4 DISCUSSION OF ALTERNATIVES

### 4.1 Alternatives for Operating Plants

- (1) Require a comprehensive plant study.

This alternative would require all plants to perform a large study for SIs. The study would consider the total plant and would address both functionally and spatially coupled ASIs.

A number of large studies have been performed by utilities such as Pacific Gas and Electric (May 1984), the Power Authority of the State of New York (June 1983), and Consumers Power Company (June 1983). In addition, the NRC sponsored two studies by national laboratories at one plant, Indian Point Station, Unit 3 (NRC, NUREG/CR-4179, and NRC, NUREG/CR-4207). None of these studies could be called a comprehensive or full plant study, except possibly the overall Midland program (Consumers Power Company, June 1983) which was never completed. Each of the other studies had a limited scope (to varying degrees) based on a specific set of objectives and/or assumptions.

The staff's review of ASIs (both postulated and actual) has shown that selecting this alternative provides only a small potential to reduce risk.

The safety benefit of the completed programs was extremely hard to quantify. In general, based on the reported results, many modifications were made but the utilities considered few, if any, truly safety significant. Some quantification of safety benefit has been estimated on the basis of the NRC-sponsored

work. As reported in the evaluation of the two demonstration analyses for SIs, the one event considered to be an ASI involving the station battery was estimated to have a core-melt frequency of  $2 \times 10^{-6}$  per reactor year.

The costs of the utility-sponsored studies (including modifications) ranged from a low of about \$2 million to a high of between \$10 and \$12 million. The laboratory studies were limited to \$1 million each. A comprehensive study for both functionally coupled and spatially coupled ASIs would cost approximately \$10 million.

Considering that a significant safety benefit was not evident and considering the high costs of a full study, this alternative was not seen as a viable option. Assuming a cost-to-benefit criterion of \$1000 per man-rem, at \$10 million per plant study, a safety benefit (for 100 plants) of 1 million man-rem would have to be realized.

(2) Take no action.

This alternative would be to take no actions beyond the actions already resulting from all the previous attention given to ASIs (e.g., IE Bulletins, IE Notices, and 10 CFR 50.49).

This alternative was seriously considered; however, the staff believes that there is still some potential for plant-specific ASIs based on the results of further review of the utility studies, further review of the operating experience, and plant-specific PRAs.

No safety benefit is involved with this alternative nor are industry costs involved in such a resolution.

(3) Require all plants to meet a prescriptive set of specific generic requirements.

The intention of this alternative would be to require a specific set of plant "fixes" based on results of previously conducted SI studies and the A-17 work. From these results, a list of actual and postulated events would be compiled. The objective of the plant-specific review would be to ensure that certain specific events would not occur at that facility. This alternative was judged to be impractical for two reasons. First, a large number of the SIs that have occurred have already been dealt with at the facilities in question. Action was generally taken in response to generic letters or IE bulletins. Sometimes the industry initiated its own action. In some cases, postulated events (that is, events that have not actually occurred) have also been the subject of generic letters or IE bulletins. Second, most existing nuclear power plants have significant differences in systems, components, and structures in the areas of concern highlighted in the review of operating experience and the review of utility studies. For example, probably no two plants are identical in physical aspects (except maybe a dual-unit plant) and no two plants have identical electrical systems. If a set of prescriptive alternatives were developed, it would not be able to properly take these differences into account. This alternative would not be able to give guidance in all areas that may need improvement at some plants and not at others, nor would it be able to give credit for mitigative design aspects at some plants which don't exist at others.

For these reasons, the staff abandoned consideration of this alternative.

- (4) Require all plants to provide a separate and independent alternative shutdown system.

This alternative was considered as a possible solution because, in theory, if a totally independent (i.e., separate and independent from all existing plant features) design feature is provided, it would not be subject to ASIs. This type of alternative received consideration under another unresolved safety issue, namely USI A-45, "Shutdown Decay Heat Removal Requirements."

This solution could theoretically solve all SI concerns; however, the costs for a "new design feature" to accomplish independent plant shutdown is high, probably on the order of tens of millions to \$100 million per plant. Therefore, this alternative was not considered feasible when only the resolution of A-17 was considered.

- (5) Require all plants to perform a focused individual study in specific areas for spatially coupled and functionally coupled ASIs.

Performing a focused review and potential associated modifications would reduce the probability of core melt. The quantification of the possible reduction proved extremely difficult. To estimate a reduction in core-melt frequency (and then calculate risk in terms of radiation release) requires that specific event sequences be selected and failure/success estimates be made for each function in the event tree. All the ASIs involve very specific plant conditions (such as operating modes, design features, and test and maintenance practices) and the overall results (such as loss of all cooling, loss of all ac power, and core melt) of an individual ASI are highly dependent on which specific plant design features remain intact after the ASI (such as remaining independent divisions, remaining displays) and the operator's response. Therefore, the risk analyses could not be used generically. Studies conducted to identify ASIs and the risks associated with them have indicated that the associated risk is very low. For instance, as reported by the Atomic Industrial Forum, the Indian Point Unit 3 Study (1985), the most comprehensive study completed to date, has indicated that the risk imposed by ASIs is insignificant. Brookhaven National Laboratory (BNL) (NRC, April 1985) and Lawrence Livermore National Laboratory (LLNL) (NRC, January 1986) studies (also on Indian Point Unit 3) confirmed that uncovering subtle ASIs can be difficult; these reports also predicted very low risk from those ASIs that were identified.

For these reasons, the assessment of safety benefit is primarily qualitative.

The audit of the utilities program was estimated to require 1 man-week per plant; therefore, about 2 man-years (total) would be involved. The audit of results (analysis/modifications) of the program and the subsequent safety evaluation report were estimated to require about 3 man-weeks per plant. Therefore, total NRC cost should not exceed \$1 million. However, the cost to utilities would be much greater, as discussed in the following subsections of Section 4.1: (5.1(b)), (5.1(c)), (5.2(b)), and (5.2(c)), below.

Considering operating experience (NRC, NUREG/CR-3922), the evaluation of the major utility programs, and recent plant-specific PRAs (NRC memorandum, December 1984), a number of "areas" of the plants appeared to be vulnerable to specific

types of ASIs. On the basis of the above work, the concerns were focused in the areas of spatially coupled ASIs and functionally coupled ASIs as follows:

### (5.1) Spatially Coupled ASIs

A number of licensee event reports (LERs) identified actual events or postulated conditions that involved spatially coupled ASIs. The following categories, as defined in NRC's NUREG/CR-3922, include spatially coupled adverse systems interactions identified in LERs:

- Category 3      degradation of safety-related components by fire protection systems
- Category 4      plant drain systems that allow flooding of safety-related equipment
- Category 8      level instrumentation degraded by high-energy line break (HELB) conditions
- Category 10     HELB conditions degrading control systems
- Category 15     inadequate cable separation
- Category 16     safety-related cables unprotected from missiles generated from HVAC fans
- Category 17     suppression pool swell
- Category 21     spatial dependencies due to failures during postulated seismic events
- Category 23     other spatial dependencies

In addition, consultants to Oak Ridge National Laboratory compared the utility studies done at Indian Point Station, Unit 3, and Diablo Canyon Nuclear Power Plant, Units 1 and 2, in the area of spatially coupled SIs (NRC, NUREG/CR-4306). As a result of this work, a focused study was defined. The study would include (1) a limited target scope, (2) a list of hazards or initiating events (related to the targets), and (3) a simplified search method. The staff reviewed the results of the consultant's report and developed a proposed target scope and hazard scope based on other considerations, as follows:

#### • Target Scope

Target is the term typically used to describe a structure, system, or component that is to be protected from ASIs. The consultant's report considered four target groupings:

- support systems and controls
- reactor coolant pressure boundary (RCPB)
- auxiliary feedwater system
- other frontline systems (such as ECCS)

The staff concluded that auxiliary feedwater systems have received significant attention as a result of the accident at Three Mile Island and other ongoing issues and staff actions.

Regarding the other frontline systems, it was concluded that if the RCPB is adequately protected from spatially coupled ASIs, the need for the operability of frontline systems under conditions such as earthquake is greatly reduced.



Therefore, the staff proposed to limit the scope to consideration of the systems required to achieve hot shutdown (and maintain it for 72 hours). This is consistent with the proposed resolution of USI A-46 in the area of seismic qualification of equipment.

### Hazard Scope

Regarding the "hazards" evaluated in the utility programs, the following were identified: seismic events, fire, flood, missiles, pipe whip, and tornadoes. On the basis of earlier regulatory actions in certain of these areas, the staff proposed that only two types of the hazards needed to be considered: earthquake and flooding.

Fire reviews have been performed at all plants to meet the requirements of Appendix R to 10 CFR 50. These reviews include criteria that address the concerns for spatially coupled ASIs. However, the potential for ASIs from the fire protection equipment was noted (e.g., spray, flood). Therefore, the A-17 resolution would not propose to reevaluate this area except as it relates to the possibility of fluid interactions from the fire protection system.

Flood reviews were required by the Atomic Energy Commission (AEC) at all plants in 1972 after the Quad Cities flood of 1972 (AEC, 1972). There is some indication from the Systematic Evaluation Program (SEP) reviews and operating experience that this area needs more attention. Therefore, the staff examined the need to reevaluate flooding (and spraying and dripping) as potential hazards.

Missiles have been evaluated under the SEP reviews, and, in general, the staff concluded that plant systems were well protected from internal missiles (NRC, SECY-84-133). Therefore, the staff eliminated this hazard from further consideration.

Tornado-initiated missiles are not considered within the scope of USI A-17 and, therefore, are eliminated from further consideration.

#### (a) Safety Benefits

Because of the way nuclear power plants are designed and constructed by the various engineering disciplines, the possibility exists that space allocations for systems and interrelationships between systems may not have been adequately analyzed. The review of SI studies by utilities appears to support this conclusion. Although large numbers of spatially coupled interactions were identified in these programs, many of them are of low probability. Nevertheless, some of the operating experience (NRC, January 1985) and PRA results (NRC, December 1984) indicate that the potential for some risk-significant SIs exists. Also it can be inferred from these studies that there was probably no rigorous or systematic procedure in older plants to uncover these potential SIs during the design phase.

With respect to probability of occurrence, it can be argued that the probability of any one occurrence is low. On the other hand, some of the



spatially coupled ASIs could be the result of very pervasive events, such as an earthquake or an internal flood. Given this "pervasive" aspect and the frequency of some of the initiators, for example safe shutdown earthquake (SSE)--on the order of  $10^{-4}$  per reactor year, or internal flood on the same order--concerns in these areas may still remain.

Many of the ASIs could damage support systems which have been shown by PRA analyses to potentially affect multiple safe shutdown or frontline systems as well as to initiate events. Therefore, if the probability of the initiating event is on the order of an SSE (and then subsequent damage to a support system is assumed) and this support system can initiate a transient and degrade the mitigation of that transient, it is clear that such spatially coupled ASIs involving support systems could be significant.

Another aspect that was considered is the potential for the operator to take recovery action. When the plant recovery actions that an operator might take are considered, it becomes apparent that for some of these spatially coupled SIs, and depending on the specific plant design, there may be few if any actions that can be taken, given the ASI occurs. That is, the potential physical damage involved may not be recoverable in a short time frame.

(b) Costs

The cost for a focused spatial study was estimated based on a review of the utility studies (NRC, NUREG/CR-4306).

The required resources were broken down into the Plant Document Review Phase and the In-Plant Assessments Phase (onsite review). Their costs were estimated by apportioning the total costs of the utility programs to the target scopes reviewed in the programs.

Resolution costs for analysis and/or modifications have a very large range. The costs are dependent on the interactions identified by the programs, the method required for resolution, and many plant-dependent factors such as feasibility of plant modification.

The manpower requirements for in-plant assessment for each of the three target groups and the associated estimates for plant document review and analysis and modifications are shown below on a per plant basis:

Targets	Plant document review (man-months)	In-plant assessment (man-months)	Analysis/mod. cost (x 1000)
Supports & controls	8	8	\$750-2000
RCPB	2	2	\$200-550
Safe shutdown equipment	2	2	\$200-550

It should be noted that these costs were obtained by scaling down the scope of industry-conducted studies. These studies were first of a kind and were very thoroughly done, both in identifying possible interactions and in documenting them. As a result of the experience gained during this learning period, more-efficient reviews could be defined. It is expected, therefore, that the per plant costs could be substantially reduced from the estimates presented above, based on a number of potential efficiencies such as a better defined scope, reduced level of documentation and quality assurance, and a cooperative effort by plant owners through formation of an industry group to develop implementation procedures. It is estimated that these economies could amount to at least a 50% reduction in costs per plant. The foregoing data provide the basis for evaluating the potential cost associated with the review, identifying and resolving spatial SIs for each of the major groups of target systems by the utility.

(c) Value/Impact

The total costs per plant were estimated to range from about \$0.5 million to \$3.5 million; most plants were in the lower range because of actions already taken in these areas and the economies outlined above. A very rough estimate of overall industry costs would be on the order of \$100 million. Although the value and impact were not calculated, the staff believes that the study of certain specific spatially coupled ASIs should be pursued for a number of reasons. Specifically, a number of potential ASIs have been noted in the SI studies and in the operating experience reviews. As an example, one recently postulated event involves a possible seismically induced SI with the reactor coolant pressure boundary. Westinghouse identified a concern with the potential for non-seismically qualified equipment (flux mapping system located over the instrumentation seal table) to jeopardize the integrity of the RCPB as a result of a seismic event. This type of potential event coupled with the concerns that recovery from an actual event may be very difficult, forms the bases for further actions. (See Section 6, "Proposed Resolution.")

Similarly, events have occurred, have been postulated to occur, and appear to continue to occur involving internal flooding. The term "flooding" is used here to cover many types of events such as spraying and dripping as well as submergence.

Recently, a fire deluge system actuated inadvertently and water traveled through HVAC ducts and dripped down on sensitive electrical equipment. As a result of this event, the Office of Inspection and Enforcement issued Information Notice 85-85.

In another recent event, a temporary floor fan was used to cool an inverter and the inverter failed when water on the floor was blown into it.

Both the seismically induced ASIs and the flooding ASIs can have very widespread effects and, as a result, may affect many systems required for safe shutdown.

A dedicated search for these types of ASIs could be costly; however, a number of activities related to these concerns are under way. The staff

believes that these ongoing activities can be used to address the A-17 concerns. See the proposed resolution (Section 6) regarding the seismic concerns (Section 6.2) and the flooding and water intrusion ASIs (Section 6.3).

## (5.2) Functionally Coupled ASIs

The review of operating experience highlighted a number of areas that involved functionally coupled ASIs. The staff concluded that for continued review the events could be grouped as follows:

- electric power systems
- support systems
- overreliance on failsafe design concept
- automatic action with no preferred failure mode
- instrumentation and control power supplies

Each significant area is discussed individually below.

### • Electric Power Systems

Concerns related to this area were highlighted in Categories 1 and 13 of NUREG/CR-3922. The three most important factors contributing to the possible significance of this area are:

- It is one of the most extensive support systems in the plant.
- The systems are inherently among the most complex in the plant.
- Each plant design is different to some extent (i.e., there is very little standardization).

### • Support Systems

Concerns related to the area of support systems were noted in Categories 1 (as stated, the electric power system is an extensive support system), 13, 14, 18, and 22 in NUREG/CR-3922. Since the electric power system was dealt with separately, the support systems considered here include: cooling water systems; heating, ventilation, and air conditioning systems; lube oil systems; air supply systems; and instrumentation and control systems. It was noted that all of these types of support systems tend to be plant unique to some extent, as is true with electric systems.

The main concern with many of the support systems is their potential to initiate an event and also degrade the systems necessary to mitigate that event. This potential breakdown in the defense-in-depth philosophy can exist in some plants; however, the safety significance is highly dependent on other plant mitigating features, such as remaining independent trains of equipment.

In addition, because the loss of these support systems (including the electrical power system) does not lead to events such as large LOCAs or MSLBs which require immediate operator action, the staff concluded that,

except for catastrophic failures (such as some spatially coupled SIs), the potential for recovery from ASIs involving these systems is very great.

#### Overreliance on Failsafe Design Concept (Failure Modes)

One area of ASIs involved reactor protection (scram) systems--Category 18 in NUREG/CR-3922. The staff recognized that the ASIs in these systems could be significant because of the time response demanded of a trip system. An argument that the operator has time to compensate for a problem might not apply.

In Category 18, a potential problem with the scram discharge volume (SDV) at all boiling-water reactors was noted. It was discovered that there could be water in the SDV because of poor drainage or a failure of air supply. Water in the SDV would inhibit control rod insertion. The failure involving the air system was of particular concern because it involves a system typically considered a portion of the reactor protection system that is not safety related. Action was taken at all boiling-water reactors to correct the problem.

The staff believes that this type of ASI was the result of using a design approach which actually requires the "functioning" of a number of features that include systems not related to safety and therefore, an incorrect reliance on failsafe principles. In the case of the air system, the system was assumed to "fail safe" (i.e., bleed off), and as a result, a partial failure, at some intermediate pressure, went unanalyzed. It was noted, too, that the electrical supply system to this scram system had been previously modified because of a similar type of concern. Specifically, the electrical power was assumed to fail safe (i.e., voltage going to zero) and as a result, partial failure such as low voltage or high voltage went unanalyzed for a time.

The staff acknowledges that there may be other areas of the plant in which failsafe principles have been used incorrectly, but in all cases except in the reactor trip system (RTS) case, it is concluded that the safety significance would be less because of the time for the operator to take action. The only other case may be during a large LOCA, however the probability of a large LOCA or MSLB in conjunction with these types of failures should be low.

#### Automatic Action With No Preferred Failure Mode

Another area of ASIs that was highlighted involved the inadvertent actuation of an engineered safety feature (ESF) (Category 6 in NUREG/CR-3922), i.e., inadvertent ECCS/RHR (emergency core cooling system/residual heat removal) pump suction transfer. The most significant characteristic of this area appears to be the fact that such a design feature does not have an "always" preferred failure mode. As a result, extra precaution may be needed to avoid (a) a failure to actuate when needed and (b) a failure that actuates the system when the system is not required (i.e., inadvertently).



The area of automatic switching of ECCS from the injection mode to the recirculation mode is the subject of a generic issue that is scheduled for prioritization, GI-24.

GI-24 will consider the aspect of possible untimely, inadvertent ECCS/RHR pump suction transfer and, therefore, it is concluded that further specific action as part of the A-17 resolution is not warranted.

Some additional concern exists that other ESF systems at specific plants may similarly not always have a preferred failure mode. Some examples could be containment isolation, low-/high-pressure interface for RHR, and automatic selection for feeding intact steam generators only. In general, almost all of these systems have been analyzed for inadvertent actuation from a functional standpoint.

#### Instrumentation and Control Power Supplies

The Oak Ridge National Laboratory (ORNL) review reported in NUREG/CR-3922 highlighted a few significant events related to instrumentation and control (I&C) power supplies. These events at all plants, and specifically at Babcock and Wilcox (B&W) plants, have already received significant attention as outlined in the ORNL followup review. Since there was some concern that the potential for significant events related to I&C power supply interactions may still exist, further review work at ORNL was identified.

ORNL completed this additional work and reported it in NRC's NUREG/CR-4470. The report included a number of I&C power supply failures, some of which led to initiation of a plant transient and partial disabling of a safety function or operator information.

As a result of the additional work performed by ORNL and the staff's further review of the area of I&C power, it was concluded that a significant number of issues and industry efforts are already under way in this area. In addition, the staff is proposing to integrate I&C power issues into a comprehensive program independent of A-17.

#### (a) Safety Benefits

With respect to the functionally coupled ASIs, the following parallel conclusions were reached:

- (1) Unlike the possible lack of consideration of spatial allocations, the designers must usually consider all functional interrelationships in great detail. This is because the system will probably not operate if the functional ties are not operating correctly.

As a result, the functional aspects get a significant amount of pre-operational checkout and testing. On the other hand, the operating experience review has indicated that in some cases errors may cause some functionally coupled ASIs to exist, and in other cases subtle ASIs may be designed into the plant.



- (2) If the large number of unanalyzed functionally coupled occurrences which could involve permutations and combinations of systems and all their failure states (including off, on, halfway, etc.) are contemplated, it is clear that not all possible functionally coupled ASIs have been analyzed. However, this is not always necessary if the analyses performed bound all possible cases (i.e., the analyses are conservative). In general, this is believed to be the case and most experience proves this.
- (3) Similar to the spatially coupled ASIs of concern, the functionally coupled ASIs of concern often involve the support systems (and for the same reasons).
- (4) The nature of the functionally coupled ASIs has led the staff to conclude that the majority of them would be recoverable (i.e., equipment was not damaged beyond use) given that the operator has the time and the information needed. In this regard, the actions taken with respect to Regulatory Guide 1.97 and I&E Bulletin 79-27 (NRC, November 1979) have provided improvements in the area of operator information.

(b) Costs

To perform a study for functionally coupled ASIs would involve some type of plant-specific systematic analysis such as an FMEA (failure mode and effects analysis), PRA, or sneak circuit analysis (NRC, NUREG/CR-4261). The costs of these types of studies are tied very closely to the scope and detail of the study. Much modeling is required if the scope is not limited to very specific areas or problems.

The Brookhaven and Livermore studies were held to \$1 million each; it would be expected that a focused study for functionally coupled ASIs would cost about the same amount.

(c) Value/Impact

Since the safety benefit of taking actions for these ASIs was also not practical to quantify, no value/impact was calculated.

As in the case of the spatially coupled ASIs, the review of the operating experience uncovered a number of functionally coupled ASIs. In addition, recent operating experience continues to show events that involve the same characteristics that were highlighted in the A-17 review.

Of particular note are events involving the electrical system and the instrumentation and control system. There continue to be inadvertent actuations which cause undesirable actions, such as initiation of switchover to the containment sump. Also, isolation problems between safety and non-safety equipment still occur.

As was concluded for the spatially coupled ASIs, a dedicated search for these types of functionally coupled ASIs could be costly. However, the staff believes that there are in place a number of ongoing programs related to these concerns, and they should be used to address the A-17 concerns.

See the proposed resolution (Section 6) regarding the operating experience reviews (Section 6.1), the USI A-46 implementation (Section 6.2), the further investigation of flooding/water intrusion (Section 6.3), the instrumentation and control power supply issues reviews (Section 6.4), and the Severe Accident Policy Statement (Section 6.5).

### (5.3) Induced Human-Intervention-Coupled ASIs

As a result of the definitions used in the USI A-17 program, these ASIs have been included in the evaluation of functionally coupled ASIs (Section 4.1(5) (5.2) above).

## 4.2 Alternatives for Future Plants

### (1) Add a new and separate ASI review section to the Standard Review Plan.

The safety benefit of this alternative would be that ASIs would receive a dedicated review. The staff has generally concluded that the individual SRPs cover the area of ASIs. However, there is some question of whether the present approach is adequate for spatially coupled ASIs.

The cost to the utility would be to address a separate section in the review process. This would add another licensing burden; however, the concerns should already have been considered in the design and construction process. For example, plant walkdowns are often conducted by an applicant for the area of impacts of equipment that is not seismically qualified (Category II equipment) on seismically qualified (Category I) equipment ("II over I review") and for high-energy line break (HELB) effects. Adding this to the SRP would require that these reviews be broadened somewhat to consider other systems interactions. These costs would be expected to be less than \$0.5 million per plant, especially given the prospect that future plants would be "standard" plants. NRC costs would be somewhat increased because the SRP would recommend that the staff perform some additional review and audit walkdowns. This cost was estimated to be less than \$100,000 per plant based on about 6 to 7 man-months of effort.

### (2) Take no action.

This alternative was considered because: (a) the individual SRPs were believed to address ASIs, (b) future plants will perform a PRA or some type of systematic analysis, and (c) if A-17 recommendations regarding PRAs are included in those studies, consideration of ASIs could be addressed. (Refer to Section 4.3, "Alternatives for Improving Systematic Plant Reviews (Such as PRAs).")

### (3) Provide additional regulatory guidance for ASIs.

It was concluded that, in general, the existing SRPs cover the ASIs of concern. There is a potential benefit to provide more guidance and, if the guidance is followed early enough in the design process, little added cost would result.

The one area of ASIs which the staff concluded needed additional guidance is the area of internal flooding and water intrusion (see Section 6.3). On the basis of this conclusion, the staff will pursue the development of a standard review plan in this area. (See Section 6.7.)

ASIs can surface in a systematic plant review (such as a PRA) which will be required of all future plants. Therefore, the staff considered future plants in conjunction with PRAs. (See Section 4.3 which follows.)

#### 4.3 Alternatives for Improving Systematic Plant Reviews (Such As PRAs)

In the Commission policy statement on severe accidents in nuclear power plants issued on August 8, 1985 (50 FR 32138), the Commission concluded, based on available information, that existing plants pose no undue risk to the public health and safety and that there is no present basis for immediate action on generic rulemaking or other regulatory requirements for these plants. However, the Commission has recognized, based on NRC and industry experience with plant-specific probabilistic risk assessments (PRAs), that systematic examinations are beneficial in identifying plant-specific vulnerabilities to severe accidents that could be fixed with low-cost improvements. Therefore, each existing plant should perform a systematic examination to identify any plant-specific vulnerabilities to severe accidents and report the results to the Commission. Therefore, the resolution of A-17 considered alternatives for future systematic studies or PRAs.

##### (1) Provide additional guidance.

By including more guidance in the specific areas of concern regarding ASIs, it is anticipated that better studies can be developed and safety-significant ASIs can be uncovered. The cost to the industry of the added guidance would be minimal and may in fact save money by focusing industry efforts in certain areas. [See the proposed resolution regarding flooding and water intrusion (Section 6.3) and PRAs (Section 6.5).]

##### (2) Take no action.

To date, there has been guidance given to PRAs regarding dependent failure analysis. This alternative would choose not to add any new information specific for ASIs.

There would be neither safety benefit, cost, nor value/impact in selecting this alternative.

##### (3) Require and endorse a specific search method for uncovering ASIs.

This alternative evaluated various search methods; however, it was concluded that any number of methods could be acceptable and the largest benefit appeared to involve focusing the study in the right areas.

There did not appear to be a greater safety benefit in choosing one method over another, and the particular method did not appear to be as critical as the focus: the costs to implement the various methods appear to be equivalent.

#### 4.4 Alternatives for Evaluating Operating Experience

##### (1) Provide for new recommendations in the future evaluation of operating experience for ASIs.

The existing programs that deal with operating experience were reviewed by ORNL (NRC, NUREG/CR-4261). It was concluded that the scope of the programs do include ASIs.

(2) Take no action.

Based on the above, it was concluded not to consider other alternatives, except for the possible one-time dissemination of the information developed in USI A-17.

(3) Provide information on ASIs to ongoing evaluations of operating experience.

As just stated in item 2, the A-17 resolution is considering a one-time dissemination of information (see Section 6.1).

## 5 BASES FOR RESOLUTION OF UNRESOLVED SAFETY ISSUE A-17

Adverse systems interactions (ASIs) involve subtle and often very complicated plant-specific dependencies between components and systems, possibly compounded by inducing erroneous human intervention. The staff has identified actions to be taken by licensees and the NRC to resolve USI A-17, and has made the judgment that these actions, together with other ongoing activities, would reduce the risk from adverse systems interactions.

As discussed further below, the resolution of USI A-17 is not based on the assertion that all adverse systems interactions have been identified, but rather that the A-17 actions plus other activities by the licensees and staff will identify precursors to potentially risk-significant interactions so that action can be taken if necessary.

(1) Actions To Be Taken by Licensees As a Result of USI A-17

(a) Water Intrusion and Flooding From Internal Sources

As part of the resolution of USI A-17, the staff has identified that water intrusion and flooding of equipment from internal plant sources may result in a risk-significant adverse systems interaction. Such events could cause a transient and could also disable the equipment needed to mitigate the consequences of the event. The Appendix to NUREG-1174 provides insights regarding plant vulnerabilities to flooding and water intrusion from internal plant sources. It is expected that these insights will be considered in the Individual Plant Examinations (IPEs).

(b) Use of Information

The staff plans to issue a letter to all licensees that summarizes the A-17 information for use in ongoing operating experience evaluations and references the pertinent NRC reports developed during the course of the resolution of USI A-17. The letter and referenced reports provide information about potential adverse systems interactions that licensees are expected to consider as part of their ongoing operating experience reviews required by TMI Action Plan Item I.C.5 of NUREG-0737.

(c) Review of Events at Nuclear Power Plants

Licensees are expected to continue to review information on events at operating nuclear power plants in accordance with the requirements of Item I.C.5 of NUREG-0737. Such information is disseminated by the NRC in the form of



information notices, bulletins, and other reports; by individual licensees in the form of licensee event reports; and by industry groups such as the Institute of Nuclear Power Operations (INPO). The NRC has an aggressive program of reviewing events at nuclear power plants. Each licensee is required to notify the NRC staff rapidly by telephone of any event that meets or exceeds the threshold defined in 10 CFR 50.72 and to file a written licensee event report for those events that meet or exceed the threshold defined in 10 CFR 50.73. Also, the NRC regional offices report events of significance every day. This information is reviewed daily by members of the NRC staff and followup efforts are assigned for events that appear to be potentially risk significant and/or are judged to be a possible precursor to a more severe event. A weekly meeting is held to brief NRC management on those events of significance. This ongoing process provides a great deal of assurance that any potentially significant event is brought to the attention of the appropriate NRC staff and management. Depending on the significance, further action may be taken to notify licensees or to impose additional requirements. The total process offers a high degree of assurance that precursors to potentially significant events, including those involving adverse systems interactions, are treated expeditiously.

(2) Actions To Be Taken by the NRC Related to Adverse Systems Interactions

(a) Integration of Specific, Ongoing, Generic Issues Related to A-17

The NRC is considering certain aspects of potential interactions as part of the resolution of identified generic issues.

• USI A-46, "Seismic Qualification of Equipment"

Requirements to resolve this issue have been sent to the licensees. The NRC and industry are working on detailed procedures that will be used to implement the requirements on a plant-specific basis. These implementation procedures will include walkdowns of individual plants to ensure that the systems needed to shut down the plant and maintain it in a safe condition for 72 hours can withstand a design-basis seismic event. The scope includes not only the systems needed to control reactivity and remove decay heat, but also the supporting power supplies, controls, instrumentation, and environmental control subsystems needed by those systems. The plant walkdown reviews include seismic systems interactions.

• Generic Issue 128, "Electric Power Reliability"

The work on USI A-17 reemphasized the potential interactions stemming from the electric power system and, in particular, instrumentation and control (I&C) power supply failures. I&C power loss can cause significant transients and can simultaneously affect the operator's ability to proceed with recovery by disabling portions of the indications and the equipment needed for recovery. Because a number of generic issues already existed in the area of electric power, it was concluded that the information developed during the resolution of USI A-17 could be best utilized as part of those programs.



The specific electric issues are:

- GI-48, "LCO for Class 1E Vital Instrument Buses in Operating Plants"
- GI-49, "Interlocks and LCOs for Redundant Class 1E Tie Breakers"
- GI-A-30, "Adequacy of Safety Related DC Power Supplies"

To better deal with all the activities on electric power, it was decided to handle all these issues in one integrated program; this became Generic Issue 128, "Electric Power Reliability."

(b) Define and Prioritize Other Issues

The Advisory Committee for Reactor Safeguards (ACRS) and other groups have identified concerns in the context of systems interactions. In many cases, the concerns are not considered to be within the scope of systems interactions as defined in the USI A-17 Task Action Plan. In some cases, these concerns have not been described specifically enough to permit the risk to be estimated. The NRC has undertaken a program [referred to as the Multiple System Responses Program (MSRP)] with Oak Ridge National Laboratory (ORNL) to define these concerns in sufficient detail so that they may be prioritized in accordance with NRC procedures.

Examples of concerns involve potential coupling of postulated plant events such as seismically induced fires and seismically induced flooding, and the attendant potential for multiple, simultaneous, adverse systems responses. These concerns are beyond the defined scope of USI A-17. The staff believes that these concerns involve low probability events, but that they may have the potential for significant consequences. If the definition, priority determination, and peer review process identify one or more issues as having high or medium priority, the issue(s) will be assigned to the appropriate organization for resolution.

(c) Probabilistic Risk Analyses or Other Systematic Plant Reviews

• Existing Plants

The Commission's Severe Accident Policy, 50 FR 32128 (August 8, 1985), requires that all existing plants perform a plant-specific search for vulnerabilities. Such searches, referred to as individual plant examinations (IPEs), involve a systematic plant review (which could be a PRA-type analysis). NRC is issuing guidance for performing such reviews. One subject area to be treated by the IPEs is common-cause failures (or dependent failures). USI A-17 recognizes that ASIs are a subset of this broader subject area and, therefore, is providing for the dissemination of the insights gained in the A-17 program for use in the IPE work.

## Future Plants

According to the Commission's Severe Accident Policy, all applicants who submit a plant docket for a construction permit or an operating license in the future are required to perform a probabilistic risk assessment (PRA) of the plant. NRC is issuing guidance on the content of PRA submittals for future light-water reactors (LWRs). As part of that guidance, A-17 is providing the insights gained in the A-17 program for the treatment of plant dependencies.

### (d) Additional Considerations for Future Plants

The above actions acknowledge the fact that future plants will perform probabilistic risk assessments, and that such studies can uncover ASIs. The staff also recognizes that the continual review of operating experience will identify systems interactions, some of which may be ASIs. Further, prioritization of issues defined by the MSRP may result in additional generic issues whose resolution may lead to requirements applicable to future plants.

Therefore, future plants should keep current on lessons learned from operating experience and continue to monitor the ongoing NRC process of developing, prioritizing, and resolving generic issues.

In addition, the staff plans to develop a standard review plan (SRP) for future plants. The SRP would include specific guidance regarding protection from internal flooding and water intrusion events.

## Staff Findings

On the basis of the technical findings reported in NUREG-1174 and the regulatory analysis reported herein, the staff has concluded that these actions can further reduce the risk from ASIs. The staff does not recommend further broad searches for ASIs because such searches have not proved to be cost-effective, and in any case, there is no guarantee after such a study is performed that all ASIs have been uncovered. Although these actions complete the staff's work under the Task Action Plan for USI A-17, and constitute technical resolution of the issue as defined therein, the potential for systems interactions remains an important consideration in the design and operation of nuclear power plants.

## 6 PROPOSED RESOLUTION

Considering the alternatives and other related activities, the staff proposes the resolution that follows. The staff's proposed resolution is summarized in Table 2.

### 6.1 Provide Information on ASIs to Ongoing Evaluations of Operating Experience

Ongoing industry and NRC review of operating experience can provide a framework for assessing ASIs (both those that have occurred and those that could occur). In addition, the ongoing reviews are specifically addressing some of the ASIs of concern highlighted by A-17.

Table 2 Proposed resolution of USI A-17

Identified concern	Action	Clarification
Spatial interactions that may be seismically initiated	USI A-46 considered	Multiple System Responses Program to consider this area further
Spatial interactions that result from a flooding-type event	A-17 proposes further action relative to IPEs	Multiple System Responses Program to consider this area further
Functional interactions that involve safety systems and their support systems <ul style="list-style-type: none"> <li>• Electric power systems               <ul style="list-style-type: none"> <li>- Instrumentation and control power supplies</li> </ul> </li> <li>• Failsafe principles, misapplication</li> <li>• Safety functions with no, always-preferred, failure direction</li> </ul>	A-17 proposes sending information to utilities for use in their operating experience reviews	A-17 will also provide information to NRC staff responsible for IPE reviews, GI-128 to consider A-17 information

Therefore, to ensure that these operating experience review programs consider the concerns highlighted in USI A-17, the staff recommends that a summary of the information developed from the work on USI A-17 be sent to all utilities for their use. Although no specific action would be required of the utilities, the staff believes that the transmittal of this information in itself will give the information that has been developed on the A-17 issue the appropriate level of attention.

Furthermore, to confirm that utilities are evaluating operational experience properly, both the NRC's inspectors and the Institute of Nuclear Power Operation's (INPO's) evaluation teams routinely audit and review this area. For example, NRC inspectors verify that utilities are reviewing events and issues discussed in NRC information notices for applicability to their facilities.

The information developed as a result of the A-17 program will be attached to the generic letter sent to all utilities. It will cover the following specific areas:

- electric power systems
- support systems

- reliance on failsafe design principles
- automatic safety actions with no (always) preferred failure mode
- instrumentation and control power supplies

## 6.2 Acknowledge Seismic SI Aspects of the USI A-46 Implementation

One of the areas of concern highlighted in A-17 involves seismically induced SIs. The staff has concluded that activities are already taking place that adequately address this concern. Specifically, 72 older plants will be implementing requirements imposed by the resolution of USI A-46, "Seismic Qualification of Equipment in Operating Plants." The newer plants, not covered by the A-46 program, have been reviewed to current requirements which address seismically induced SIs.

The proposed resolution of A-46 involves an onsite review and walkdown of equipment required for safe shutdown. As part of this review and walkdown, the evaluation team will review the potential for certain ASIs which might disable (1) the safe shutdown system components, (2) cable trays, and to a limited extent, (3) the support systems. On the basis of this activity, the staff concluded that further review in this area (to resolve the A-17 issue), was not required. Although USI A-46 is not covering all possible ASIs, the staff has concluded that any further work in the area of seismically induced failures should be pursued as a generic issue separate from A-46 and A-17. For further information see the action under Section 6.6 below.

## 6.3 Consider Flooding and Water Intrusion From Internal Sources in Individual Plant Examinations (IPEs)

The staff intends to provide insights to all licensees for use in performing analysis of flooding and water intrusion from internal sources. It is expected that these insights will be used in their Individual Plant Examinations (IPEs). For further information see the Appendix to NUREG-1174.

## 6.4 Provide for the Integration and Coordination of Electrical and Instrumentation and Control Power Supply Issues and Concerns

Work on USI A-17 highlighted a number of ASI concerns in the area of instrumentation and control (I&C) power supplies (NRC, NUREG/CR-4470).

One specific aspect of note for A-17 was the potential that the loss of one power supply could cause an event (such as a transient or trip) and then could also affect the systems required to respond to the event and/or the operators' information displays.

Although only a fraction of the events led to such type of results, the work under A-17 highlighted a number of other concerns that involved the failure of certain I&C power supply components (such as the inverters) and the lack of consistent limiting conditions for operation (LCOs) on the I&C power supplies.

Additional review showed that the area of I&C power has been the subject of a number of actions and is the subject of a number of continuing issues. To achieve a more coordinated approach to this area, the NRC staff working on the



A-17 program recommends that the area of I&C power be integrated into one program and that these various issues be addressed under a single program plan to deal with the overall adequacy of nuclear power plant I&C power systems.

The NRC staff initiated this activity with the assistance of national laboratories under integrated issue GI-128, "Electric Power Reliability." Some of the issues and concerns being addressed include the following:

- A-30, "Adequacy of Safety-Related DC Power Supplies"
- GI-48, "LCO for Class IE Vital Instrument Buses in Operating Reactors"
- GI-49, "Interlocks and LCOs for Redundant Class IE Tie Breakers"

#### 6.5 Provide Guidance for Future PRA or Other Systematic Plant Reviews

The staff and the nuclear power industry have been involved in developmental work for probabilistic risk assessments. One portion of that work involved the "PRA Procedures Guide" (NRC, NUREG/CR-2300) and the "PSA Procedures Guide" (NRC, NUREG/CR-2815). As stated above, the A-17 results can help focus on areas of the plant that need to be emphasized because of the high potential for these areas to be vulnerable to ASIs.

Therefore, the resolution of A-17 will provide the information on ASIs highlighted in A-17 for use in future PRA review.

#### 6.6 Define Potential Generic Issues That Are Not Included As Part of the A-17 Resolution or Other Regulatory Programs

As was discussed under the scope and definition of the A-17 issue, some systems interaction concerns may not have been covered as part of the A-17 study. The staff, with the assistance of ORNL, is in the process of defining these other issues and concerns in sufficient detail so that they can be prioritized separately. As a result of this prioritization, additional work effort may be defined for the separate issues. This research program is designated, "Multiple System Responses Program."

#### 6.7 Develop a Standard Review Plan for Future Plants

The staff plans to develop a standard review plan for future plants. The SRP would include specific guidance regarding protection from internal flooding and water intrusion events.

### 7 REFERENCES

Atomic Energy Commission, letter dated September 26, 1972, from R. C. DeYoung to licensees, "Flooding Event at Quad Cities, Unit 1."

Atomic Industrial Forum, Inc., letter dated October 8, 1985, from M. R. Edelman to V. Stello, "Unresolved Safety Issue A-17 Systems Interactions."

Consumers Power Company, "Program Manual Spatial Systems Interaction Program/ Seismic Midland Energy Center," Revision 1, June 6, 1983.



Office of Inspection and Enforcement, NRC, Bulletin 79-27, "Loss of Non-Class IE Instrumentation and Control Power Systems Bus During Operation," November 30, 1979.

---, Information Notice 83-41, "Actuation of Fire Suppression System Causing Inoperability of Safety-Related Equipment," June 22, 1983.

---, Information Notice 83-44, "Potential Damage to Redundant Safety Equipment as a Result of Backflow Through the Equipment and Floor Drainage System," July 1, 1983.

---, Information Notice 85-85, "Systems Interaction Event Resulting in Reactor System Safety Relief Valve Opening Following a Fire-Protection Deluge System Malfunction," October 31, 1985.

---, Information Notice 87-14, "Actuation of Fire Suppression System Causing Inoperability of Safety-Related Ventilation Equipment," March 23, 1987.

Pacific Gas and Electric Company, "Diablo Canyon Seismically Induced Systems Interaction Program," Dockets 50-275 and 50-323, May 7, 1984.

Power Authority of the State of New York, "Systems Interaction Study, Indian Point 3," Docket 50-286, November 30, 1983.

U.S. Nuclear Regulatory Commission, Memorandum dated September 18 1984, from R. Kendall to D. Thatcher, "Comments on ORNL Draft NUREG/CR-3922.

---, Memorandum dated December 3, 1984, from H. R. Denton to Division Directors, "Insights Gained From Probabilistic Risk Assessments."

---, Memorandum dated March 20, 1985, from A. Thadani to K. Kniel, "RRAB Inputs to the USI A-17 Program."

---, Memorandum dated May 31, 1985, from A. Thadani to K. Kniel, "RRAB Input to USI A-17 Resolution."

---, NUREG-75/014, "Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," October 1975.

---, NUREG-0471, "Generic Task Problem Descriptions (Categories B, C, and D)," June 1978.

---, NUREG-0572, "Review of Licensee Event Reports (1976-1978)," September 1979.

---, NUREG-0649, "Task Action Plans for Unresolved Safety Issues Related to Nuclear Power Plants," September 1984.

---, NUREG-0660, "NRC Action Plan Developed as a Result of the TMI-2 Accident," May 1980.

---, NUREG-0737, "Clarification of TMI Action Plan Requirements," November 1980.

- , NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," July 1981.
- , NUREG-0824, "Integrated Plant Safety Assessment Systematic Evaluation Program--Millstone Nuclear Power Station, Unit 1," February 1983.
- , NUREG-0933, Rev. 2, "A Prioritization of Generic Safety Issues," December 1984.
- , NUREG-1070, "NRC Policy on Future Reactor Designs," July 1985.
- , NUREG-1174, "Evaluation of Systems Interactions in Nuclear Power Plants: Technical Findings Related to Unresolved Safety Issue A-17," May 1989.
- , NUREG/CR-2300, "PRA Procedures Guide," Vols. 1 and 2, January 1983.
- , NUREG/CR-2815, "Probabilistic Safety Analysis Procedures Guide," Brookhaven National Laboratory, January 1984.
- , NUREG/CR-3922, "Survey and Evaluation of System Interaction Events and Sources," Oak Ridge National Laboratory, January 1985.
- , NUREG/CR-4179, "Digraph Matrix Analysis for Systems Interactions at Indian Point Unit 3, Abridged Version," Vol. 1, (January 1986) Vols. 2-6 will be available in the NRC Public Document Room, 1717 H Street, N. W., Washington, D.C., Lawrence Livermore National Laboratory.
- , NUREG/CR-4207, "Fault Tree Application to the Study of Systems Interactions at Indian Point 3," Brookhaven National Laboratory, April 1985.
- , NUREG/CR-4261, "Assessment of System Interaction Experience in Nuclear Power Plants," Oak Ridge National Laboratory, June 1986.
- , NUREG/CR-4306, "Review and Evaluation of Spatial System Interaction Programs," Oak Ridge National Laboratory, Unpublished.
- , NUREG/CR-4470, "Survey and Evaluation of Vital Instrumentation and Control Power Supply Events," August 1986.
- , SECY-84-133, "Results of SEP," Enclosure 4, "SEP Phase II Safety Lessons Learned," March 23, 1984.

U.S. NUCLEAR REGULATORY COMMISSION  
NOTICE OF ISSUANCE AND AVAILABILITY OF  
NUREG-1174, "EVALUATION OF  
SYSTEMS INTERACTIONS IN NUCLEAR  
POWER PLANTS: - TECHNICAL FINDINGS  
RELATED TO UNRESOLVED SAFETY ISSUE A-17," AND  
NUREG-1229, "REGULATORY ANALYSIS FOR  
PROPOSED RESOLUTION OF USI A-17-  
SYSTEMS INTERACTIONS IN NUCLEAR POWER PLANTS"

The U. S. Nuclear Regulatory Commission (NRC) staff is issuing the resolution of Unresolved Safety Issue (USI) A-17, "Systems Interactions in Nuclear Power Plants." The resolution is documented in two NUREG reports entitled "Evaluation of Systems Interactions in Nuclear Power Plants: Technical Findings Related to Unresolved Safety Issue A-17" (NUREG-1174) and "Regulatory Analysis for Resolution of USI A-17 - Systems Interactions in Nuclear Power Plants" (NUREG-1229). Systems interactions was identified as an Unresolved Safety Issue (USI) in NUREG-0510, "Identification of Unresolved Safety Issues Relating to Nuclear Power Plants," January 1979, and was reported to the Congress pursuant to Section 210 of the Energy Reorganization Act of 1974 as amended on December 13, 1977.

Nuclear power plants contain many structures, systems, and components (SSCs), some of which are safety-related. Certain SSCs are designed to interact to perform their intended functions. These "systems interactions" are usually well recognized and therefore accounted for in the evaluation of plant safety by the designers and by those who assess plant safety.

A number of significant events have involved unintended or unrecognized dependencies among the SSCs. Some of these events have involved subtle dependencies between safety-related SSCs and other SSCs. Some events have also involved subtle dependencies between redundant safety-related SSCs that were believed to be independent.

Therefore, the purpose of USI A-17 was to investigate the potential that unrecognized, subtle dependencies among SSCs have remained hidden and that they could lead to safety-significant events. The terms used to describe these unrecognized, subtle dependencies is adverse systems interactions (ASIs).

The staff is not recommending that further broad searches specifically for all ASIs be undertaken because such searches have not proved to be cost effective in the past, and there is no guarantee after such a study that all ASIs have been uncovered. Rather, the staff has concluded that certain more specific actions, together with other ongoing activities, could reduce the risk from adverse systems interactions.

The staff has concluded from its A-17 investigations that the following actions should be taken:

- (1) Issuance of a generic letter that includes:
  - (a) the bases for resolution of USI A-17,
  - (b) a summary of information for use in ongoing operating experience reviews.
- (2) Recognition that Individual Plant Examinations (IPEs) already include evaluation of internal flooding and the A-17 insights will be referenced in the IPE guidance documents.
- (3) Recognition that the USI A-46 resolution will address seismically induced systems interactions to verify that components and systems needed to safely shut down the plant are protected, given loss of offsite power. (New plants, not covered by A-46, have been reviewed to current requirements that address seismically induced systems interactions.)
- (4) Communication of information regarding ASIs for staff review of PRAs and for staff evaluation of electric power supplies as part of GI-128, "Electric Power Reliability."

- (5) Identification and definition of concerns related to A-17 and other programs that have not been specifically addressed. (The objective of this program is to define the concerns with sufficient specificity to permit them to be prioritized as potential generic safety issues.)
- (6) Development of a Standard Review Plan for future plants that would include guidance regarding protection from internal flooding and water intrusion events.

Copies of the documents included in the final resolution for USI A-17 may be purchased from the Superintendent of Documents, U. S. Government Printing Office, P. O. Box 37082, Washington, DC 20013-7082. Copies are also available from the National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161. A copy is also available for public inspection and/or copying at the NRC Public Document Room, 2120 L Street, N.W., Washington DC.

Dated at Rockville, Maryland this \_\_\_\_ day of \_\_\_\_\_.

FOR THE NUCLEAR REGULATORY COMMISSION

---

R. Wayne Houston, Director  
Division of Safety Issue Resolution  
Office of Nuclear Regulatory Research



SUMMARY STATEMENTNotice

The following documents have been issued by the U.S. Nuclear Regulatory Commission (NRC): NUREG-1174, "Evaluation of Systems Interactions in Nuclear Power Plants: Technical Findings Related to Unresolved Safety Issue A-17," and NUREG-1229, "Regulatory Analysis for Resolution of USI A-17 - Systems Interactions in Nuclear Power Plants."

NUREG-1174 contains a summary of the technical findings related to Unresolved Safety Issue (USI) A-17, "Systems Interactions in Nuclear Power Plants." As a result of these findings, the NRC staff has developed a regulatory analysis and a resolution for USI A-17. NUREG-1229 contains the regulatory analysis. The staff concluded from its A-17 investigations that certain actions should be taken by the NRC and licensees.

These actions include guidance to the staff for use in severe accident policy implementation and probabilistic risk assessment (PRA) review and development, and guidance to licensees in the area of operating experience reviews. The resolution also includes insights regarding internal flooding and water intrusion analyses for consideration in performing an Individual Plant Examination per Generic Letter 88-20.

The staff concluded that certain older plants should perform seismic system interaction reviews. However, these reviews are required to be performed as a part of USI A-46 implementation; therefore, a separate requirement under USI A-17 is not proposed.

ADDRESSEES: ALL POWER REACTOR LICENSEES AND APPLICANTS

SUBJECT: RESOLUTION OF UNRESOLVED SAFETY ISSUE A-17, "SYSTEMS INTERACTIONS IN NUCLEAR POWER PLANTS" (GENERIC LETTER 89- )

This generic letter informs licensees and applicants of the final resolution of USI A-17, "Systems Interactions in Nuclear Power Plants." There are two attachments which are provided for information.

Attachment 1 outlines the bases for resolution of USI A-17.

Attachment 2 provides a grouping of five general lessons learned from the review of the overall systems interaction issue. The review of this information will give licensees additional appreciation of the kinds of adverse systems interaction which have appeared in operating experience and can aid them in continuing evaluation of operating experience.

No specific action or written response is required by this letter. If you have any question about this matter, please contact the technical contact listed below or the Regional Administrator at the appropriate regional office.

Sincerely,

Technical Contacts:

D. Thatcher, RES  
(301) 492-3935

Attachments:

1. Bases for Resolution of Unresolved Safety Issue A-17
2. Summary Information for Use in Operating Experience Evaluations

BASES FOR RESOLUTION OF UNRESOLVED SAFETY ISSUE A-17

Introduction

The U.S. Nuclear Regulatory Commission (NRC) has concluded its resolution of Unresolved Safety Issue (USI) A-17, "Systems Interactions in Nuclear Power Plants." This document provides a summary of that resolution. More detailed background information is provided in References 1 and 2.

Adverse systems interactions (ASIs) involve subtle and often very complicated plant-specific dependencies between components and systems, possibly compounded by inducing erroneous human intervention. The staff has identified actions to be taken by licensees and the NRC to resolve USI A-17, and has made the judgment that these actions, together with other ongoing activities, could reduce the risk from adverse systems interactions.

As discussed further below, the staff's judgment is not based on the assertion that all adverse systems interactions have been identified, but rather that the A-17 actions plus other activities by the licensees and staff will identify precursors to potentially risk-significant interactions so that action can be taken if necessary.

Resolution

(1) Actions To Be Taken by Licensees

(a) Water Intrusion and Flooding From Internal Sources

As part of the resolution of USI A-17, the staff has identified that water intrusion and flooding of equipment from internal plant sources may result in a risk-significant adverse systems interaction. Such events could cause a transient and could also disable the equipment needed to mitigate the consequences of the event. The appendix to NUREG-1174 (reference 1) provides insights regarding plant vulnerabilities to flooding and water intrusion from internal plant sources. It is expected that these insights will be considered in implementing Generic Letter 88-20 [Individual Plant Examinations (IPE)] which requires an assessment of internal flooding.

(b) Use of Information

Attachment 2 to this letter summarizes the A-17 information for use in ongoing operating experience evaluations and references the pertinent NRC reports developed during the course of the resolution of USI A-17. That attachment and referenced reports provide information about potential adverse systems interactions that licensees are expected to consider as part of their ongoing operating experience reviews required by TMI Action Plan Item I.C.5 of NUREG-0737.

(c) Review of Events at Nuclear Power Plants

Licensees are expected to continue to review information on events at operating nuclear power plants in accordance with the requirements of Item I.C.5 of NUREG-0737. Such information is disseminated by the NRC in the form of information notices, bulletins, and other reports; by individual licensees in the form of licensee event reports; and by industry groups such as the Institute of Nuclear Power Operations (INPO). The NRC has an aggressive program of reviewing events at nuclear power plants. Each licensee is required to notify the NRC staff rapidly by telephone of any event that meets or exceeds the threshold defined in 10 CFR 50.72 and to file a written licensee event report for those events that meet or exceed the threshold defined in 10 CFR 50.73. Also, the NRC regional offices report events of significance every day. This information is reviewed daily by members of the NRC staff and followup efforts are assigned for events that appear to be potentially risk significant and/or are judged to be a possible precursor to a more severe event. A weekly meeting is held to brief NRC management on those events of significance. This ongoing process provides a great deal of assurance that any potentially significant event is brought to the attention of the appropriate NRC staff and management. Depending on the significance, further action may be taken to notify licensees or to impose additional requirements. The total process offers a high degree of assurance that precursors to potentially significant events, including those involving adverse systems interactions, are treated expeditiously.

(2) Actions To Be Taken by the NRC Related to Adverse Systems Interactions

(a) Integration of Specific, Ongoing, Generic Issues Related to A-17

The NRC is considering certain aspects of potential interactions as part of the resolution of identified generic issues.

\* USI A-46, "Seismic Qualification of Equipment"

Requirements to resolve this issue have been sent to the licensees. The NRC and industry are working on detailed procedures that will be used to implement the requirements on a plant-specific basis. These implementation procedures will include walkdowns of individual plants to ensure that the systems needed to shut down the plant and maintain it in a safe condition for 72 hours can withstand a design-basis seismic event. The scope includes not only the systems needed to control reactivity and remove decay heat, but also the supporting power supplies, controls, instrumentation, and environmental control subsystems needed by those systems. The plant walkdown reviews include seismic systems interactions.

\* Generic Issue 128, "Electric Power Reliability"

The work on USI A-17 reemphasized the potential interactions stemming from the electric power system and, in particular, instrumentation and control (I&C) power supply failures. I&C power

loss can cause significant transients and can simultaneously affect the operator's ability to proceed with recovery by disabling portions of the indications and the equipment needed for recovery. Because a number of generic issues already existed in the area of electric power, it was concluded that the information developed during the resolution of USI A-17 could be best utilized as part of those programs.

The specific electric issues are:

- GI-48, "LCO for Class 1E Vital Instrument Buses in Operating Plants"
- GI-49, "Interlocks and LCOs for Redundant Class 1E Tie Breakers"
- GI-A-30, "Adequacy of Safety Related DC Power Supplies"

To better deal with all the activities on electric power, it was decided to handle all these issues in one integrated program; this became Generic Issue 128, "Electric Power Reliability."

(b) Define and Prioritize Other Issues

The Advisory Committee for Reactor Safeguards (ACRS) and other groups have identified concerns in the context of systems interactions. In many cases, the concerns are not considered to be within the scope of systems interactions as defined in the USI A-17 Task Action Plan. In some cases, these concerns have not been described specifically enough to permit the risk to be estimated. The NRC has undertaken a program [referred to as the Multiple System Responses Program (MSRP)] with Oak Ridge National Laboratory (ORNL) to define these concerns in sufficient detail so that they may be prioritized in accordance with NRC procedures.

Examples of concerns involve potential coupling of postulated plant events such as seismically induced fires and seismically induced flooding, and the attendant potential for multiple, simultaneous, adverse systems responses. These concerns are beyond the defined scope of USI A-17. The staff believes that these concerns involve low probability events, but that they may have the potential for significant consequences. If the definition, priority determination, and peer review process identify one or more issues as having high or medium priority, the issue(s) will be assigned to the appropriate organization for resolution.

(c) Probabilistic Risk Analyses or Other Systematic Plant Reviews

• Existing Plants

The Commission's Severe Accident Policy, 50 FR 32128 (August 8, 1985), requires that all existing plants perform a plant-specific search for vulnerabilities. Such searches, referred to as individual plant



examinations (IPEs), involve a systematic plant review (which could be a PRA-type analysis). NRC is issuing guidance for performing such reviews. One subject area to be treated by the IPEs is common-cause failures (or dependent failures). USI A-17 recognizes that ASIs are a subset of this broader subject area and, therefore, is providing for the dissemination of the insights gained in the A-17 program for use in the IPE work.

#### Future Plants

According to the Commission's Severe Accident Policy, all applicants who submit a plant docket for a construction permit or an operating license in the future are required to perform a probabilistic risk assessment (PRA) of the plant. NRC is issuing guidance on the content of PRA submittals for future light-water reactors (LWRs). As part of that guidance, A-17 is providing the insights gained in the A-17 program for the treatment of plant dependencies.

#### (d) Additional Considerations for Future Plants

The above actions acknowledge the fact that future plants will perform probabilistic risk assessments, and that such studies can uncover ASIs. The staff also recognizes that the continual review of operating experience will identify systems interactions, some of which may be ASIs. Further prioritization of issues defined by the MSRP may result in additional generic issues whose resolution may lead to requirements applicable to future plants.

Therefore, future plants should keep current on lessons learned from operating experience and continue to monitor the ongoing NRC process of developing, prioritizing, and resolving generic issues.

In addition, the staff plans to develop a standard review plan (SRP) for future plants. The SRP would include specific guidance regarding protection from internal flooding and water intrusion events.

#### Staff Findings

On the basis of the technical findings reported in NUREG-1174 and the regulatory analysis reported in NUREG-1229 the staff has concluded that these actions can further reduce the risk from ASIs. The staff does not recommend further broad searches for ASIs because such searches have not proved to be cost-effective, and in any case, there is no guarantee after such a study is performed that all ASIs have been uncovered. Although these actions complete the staff's work under the Task Action Plan for USI A-17, and constitute technical resolution of the issue as defined therein, the potential for systems interactions remains an important consideration in the design and operation of nuclear power plants.

#### References:

1. U.S. Nuclear Regulatory Commission, NUREG-1174, "Evaluation of Systems Interactions in Nuclear Power Plants."
2. ---, NUREG-1229, "Regulatory Analysis for Resolution of USI A-17."

SUMMARY INFORMATION FOR USE IN  
OPERATING EXPERIENCE EVALUATIONS

I. SUMMARY

The U.S. Nuclear Regulatory Commission (NRC) has concluded its technical resolution of Unresolved Safety Issue (USI) A-17, "Systems Interactions in Nuclear Power Plants." This summary presents a portion of the results of that technical resolution for use in operating experience evaluations. More detailed background information is provided in References 1 and 2.

Because of the complex, interdependent network of systems, structures, and components that constitute a nuclear power plant, the scenario of almost any significant event can be characterized as a "systems interaction." As a result, the staff recognized that if the term 'systems interaction' was to be interpreted in a very broad sense, it became an unmanageable safety issue. Focusing was required to address perceived safety concerns. It is recognized that by the very nature of such a focusing effort, all concerns that one may characterize as systems interactions may not be addressed. It is, therefore, extremely important that the scope and boundary of the focused program be clearly defined and understood. Then, if other concerns still exist after completion of the program, they can be addressed as part of separate efforts as deemed necessary.

The information presented in this document is based on the following definitions:

(1) Systems Interaction (SI)

Actions or inactions (not necessarily failures) of various systems (subsystems, divisions, trains), components, or structures resulting from a single credible failure within one system, component, or structure and propagation to other systems, components, or structures by inconspicuous or unanticipated interdependencies. The major difference between this type of event and a classic single-failure event is in those aspects of the initiating failure and/or its propagation that are not obvious (i.e., that are hidden or unanticipated).

(2) Adverse Systems Interaction (ASI)

A systems interaction that produces an undesirable result.

(3) Undesirable Result (Produced by Systems Interaction)

This was defined by a list of the types of events that were to be considered in USI A-17:

- (a) Degradation of redundant portions of a safety system, including consideration of all auxiliary support functions. Redundant

portions are those considered to be independent in the design and accident analysis (Chapter 15) of the Final Safety Analysis Report (FSAR) of the plant. (Note: This would violate the single-failure criterion.)

- (b) Degradation of a safety system by a non-safety system. (Note: This result would demonstrate a breakdown in presumed "isolation.")
- (c) Initiation of an "accident" (e.g., LOCA, MSLB) and (i) the degradation of at least one redundant portion of any one of the safety systems required to mitigate the event (Chapter 15, FSAR analyses); or (ii) degradation of critical operator information sufficient to cause the operator to perform unanalyzed, unassumed, or incorrect actions. (Note: This includes failure to perform correct actions because of incorrect information.)
- (d) Initiation of a "transient" (including reactor trip) and (i) the degradation of at least one redundant portion of any one of the safety systems required to mitigate the event (Chapter 15, FSAR analyses); or (ii) degradation of critical operator information sufficient to cause the operator to perform unanalyzed, unassumed, or incorrect actions. (Note: This includes failure to perform correct actions because of incorrect information.)
- (e) Initiation of an event that requires plant operators to act in areas outside the control room (Perhaps because the control room is being evacuated or the plant is being shut down) and disruption of the access to these areas (for example, by disruption of the security system or isolation of an area when fire doors are closed or when a suppression system is actuated).

The intersystem dependencies (or systems interactions) have been divided into three classes based on the way they propagate:

(1) Functionally Coupled:

Those SIs that result from sharing of common systems/components; or physical connections between systems, including electrical, hydraulic, pneumatic, or mechanical.

(2) Spatially Coupled:

Those SIs that result from sharing or proximity of structures/locations, equipment, or components or by spatial inter-ties such as HVAC and drain systems.

(3) Induced Human-Intervention Coupled:

Those SIs in which a plant malfunction (such as failed indication) inappropriately induces an operator action, or a malfunction inhibits an operator's ability to respond. As analyzed in the A-17 program, these SIs are considered another example of functionally coupled ASIs. (Induced human-intervention-coupled systems interactions exclude random human errors and acts of sabotage.)

As a result of the staff's studies of adverse systems interactions (ASIs) undertaken as part of A-17 and reported in Reference 1, the staff has concluded the following:

- (1) To address a subject area such as "systems interactions" in its broadest sense tends to be an unmanageable task incapable of resolution. Some bounds and limitations are crucial to proceeding toward a resolution. Considering this, the A-17 program utilized a set of working definitions to limit the issue. It is recognized that such an approach may leave some concerns unaddressed.
- (2) The occurrence of an actual ASI or the existence of a potential ASI is very much a function of an individual plant's design and operational features (such as its detailed design and layout, allowed operating modes, procedures, and tests and maintenance practices). Furthermore, the potential overall safety impact (such as loss of all cooling, loss of all electric power, or core melt) is similarly a function of those plant features that remain unaffected by the ASI. In other words, the results of an ASI depend on the availability of other independent equipment and the operator's response capabilities.
- (3) Although each ASI (and its safety impact) is unique to an individual plant, there appear to be some characteristics common to a number of the ASIs.
- (4) Methods are available (and some are under development) for searching out SIs on a plant-specific basis. Studies conducted by utilities and national laboratories indicate that a full-scope plant search takes considerable time and money. Even then, there is not a high degree of assurance all, or even most, ASIs will be discovered.
- (5) Functionally coupled ASIs have occurred at a number of plants, but improved operator information and training (instituted since the accident at Three Mile Island) should greatly aid in recovery actions during future events.
- (6) Induced human-intervention-coupled interactions as defined in A-17 are a subset of the broader class of functionally coupled SIs. As stated for functionally coupled SIs, improvements in both operator information and operator training will greatly improve recovery from such events.
- (7) As a class, spatially coupled SIs may be the most significant because of the potential for the loss of equipment which is damaged beyond repair. In many cases, these ASIs are less likely to occur because of the lower probability of initiating failure (e.g., earthquake, pipe rupture) and the less-than-certain coupling mechanisms involved. However, past operating experience highlighted a number of flooding and water intrusion events and more recent operating experience indicates that these types of events are continuing to occur.
- (8) Probabilistic risk assessments or other systematic plant-specific reviews can provide a framework for identifying and addressing ASIs.



- (9) Because of the nature of ASIs (they are introduced into plants by design errors and/or by overlooking subtle or hidden dependencies), they will probably continue to happen. In their evaluations of operating experience, NRC and the nuclear power industry can provide an effective method for addressing ASIs.
- (10) For existing plants, a properly focused, systematic plant search for certain types of spatially coupled ASIs and functionally coupled ASIs (and correction of the deficiencies found) may improve safety.
- (11) The area of electric power, and particularly instrumentation and control power supplies, was highlighted as being vulnerable to relatively significant ASIs. Further investigation showed that this area remains the subject of a number of separate issues and studies. A concentrated effort to coordinate these activities and to include power supply interactions could prove an effective approach in this area.
- (12) For future plants, additional guidance regarding ASIs could benefit safety.
- (13) The concerns raised by the Advisory Committee on Reactor Safeguards (ACRS), on A-17, but which have not been addressed in the Staff's study of A-17, should be considered as candidate generic issues, separate from USI A-17.

It should be noted that the staff has concluded that adverse systems interactions (ASIs) involve subtle, and often very complicated, dependencies. Therefore, total elimination of ASIs is unachievable. For these reasons, the staff is not recommending that each plant undertake a large, comprehensive study to uncover ASIs. Instead, the staff is recommending other, more cost-effective actions for reducing the frequency and impact of ASIs. Although these actions complete the staff's work under the task action plan for USI A-17, and constitute technical resolution of the issue as defined therein, the potential for ASIs remains an important consideration in the design and operation of nuclear power plants. The staff has, therefore, acknowledged the continuing importance of ongoing activities such as probabilistic risk assessments or other systematic plant evaluations and the continuing review and evaluation of the industry's operating experience.

The regulatory analysis (Reference 2) considered a number of alternatives for resolution, and based on that analysis, the staff has concluded that certain actions should be taken to resolve USI A-17. These actions are:

- (1) Send a generic letter to all plants outlining the resolution of USI A-17 and providing information developed during the resolution of A-17.
- (2) Consider flooding and water intrusion from internal sources in the Individual Plant Examinations (IPE).
- (3) Consider systems interactions involving the electrical power systems in the integrated program on electrical power reliability.
- (4) Provide information for use in future PRAs.



- (5) Provide a framework for addressing those other concerns related to systems interactions which are not covered by the USI A-17 program.
- (6) Acknowledge that the resolution of USI A-46 addresses aspects of systems interaction.
- (7) Develop a standard review plan for future plants to address protection from internal flooding and water intrusion.

The following discussion addresses the first action. The second action is addressed in the IPE guidance documents. The remaining five actions involve staff actions.

#### A. Background

The adverse systems interactions (ASIs) sorted from the survey of experience appeared to be due to two general causes. Some of the ASIs resulted from obvious errors or failures to meet clearly specified design requirements and/or guidance. Others arose from more subtle causes such as the lack of sufficient consideration, or analysis, of all the significant failure mechanisms or modes and the associated event combinations and/or sequences.

In the case of older plants, the causes often are related to the fact that less design guidance and associated analyses were available and/or required when the plants were licensed.

Although no specific licensee actions are required, the staff concluded that if certain highlighted concerns identified in the A-17 studies were communicated to the industry, the ongoing industry evaluations of operating experience could provide adequate treatment of this information.

#### B. Highlighted Concerns\*

As part of the effort to provide a more focused approach for the resolution of A-17, a set of tasks was defined to accomplish a search of operating experience to accumulate a data bank on the types of common-cause events of concern. The major portion of this work was performed by the Oak Ridge National Laboratory (ORNL), and a summary of ORNL's findings is included in Reference 3.

The search emphasized events included in the LER (licensee event report) files and involved a screening of those events based on the task action plan definition. On the basis of the characteristics or attributes of the systems interaction events, a group of general categories of SI events was developed. The results of the ORNL experience review indicate 23 general categories of events (see Table 1) which have involved systems interactions.

\*More details on the highlighted concerns and other ASIs are provided in References 1, 3, and 4, and those documents should be consulted for additional information.

Table 1 Event categories involving systems interactions

Category No.	Title	No. of events
1	Adverse interactions between normal or offsite power systems and emergency power systems	34
2	Degradation of safety-related systems by vapor or gas intrusion	15
3	Degradation of safety-related components by fire protection systems	10
4	Plant drain systems allow flooding of safety-related equipment	8
5	Loss of charging pumps due to volume control tank level instrumentation failures	6
6	Inadvertent ECCS/RHR pump suction transfer	4
7	HPSI/charging pumps overheat on low flow during safety injection	6
8	Level instrumentation degraded by HELB conditions	21
9	Loss of containment integrity from LOCA conditions	10
10	HELB conditions degrading control systems	3
11	Auxiliary feedwater pump runout under steamline break conditions	2
12	Waterhammer events	4
13	Common support systems or cross-connects	18
14	Instrument power failures affecting safety systems	5
15	Inadequate cable separation	8
16	Safety-related cables unprotected from missiles generated from HVAC fans	3
17	Suppression pool swell	3
18	Scram discharge volume degradation	2
19	Induced human interactions	4
20	Functional dependencies from failures during seismic events	5
21	Spatial dependencies from failures during seismic events	13
22	Other functional dependencies	21
23	Other spatial dependencies	30

Review of these 23 general categories led to the identification of five areas of highlighted concerns. These are discussed below:

### Electric Power System

The electric power system includes the offsite sources, the switchyard, the power distribution buses and breakers, onsite generating equipment, and the control power and logic to operate the breakers and start and load the diesel generators. Some of the lower voltage (typically 120-V ac and 125-V dc) power supply portion of the system is also dealt with under the "Instrumentation and Control Power Supplies" heading below.

As outlined in References 3 and 4, concerns were highlighted in the area of electric power systems in Categories 1 and 13 (Table 1). Three important factors appear to contribute to the possible significance of this area:

- (1) It is one of the most (if not the most) extensive support systems in a plant. Power is supplied from various sources including the offsite network, the main plant turbine-generator and, in certain situations, the safety-related diesel generators. Power is then distributed to various items of equipment for normal plant control which is not related to safety, various engineered safety feature equipment which is safety related, and various items of equipment for shutdown and decay heat removal.
- (2) Given these system demands, the power system is therefore an inherently complex system. A large number of normal operating modes at the plant, as well as transient and accident situations, must be accommodated. Interfaces are created between redundant safety-related equipment. In addition, the power system itself relies on a number of other support systems such as HVAC and cooling water.
- (3) Because of individual plant requirements and situations (a number of significant events occur when the system is in any abnormal temporary alignment), each power system tends to have some unique aspects. Very few specific ASIs can be stated to be generically applicable; however, the staff believes that general classes of electric power events can be potentially generic.

ORNL (References 3 and 4) categorized the electric power system concerns into four areas:

- load sequencing/load shedding
- diesel generator failures caused by specific operating modes
- breaker failures due to loss of dc power
- failures that propagate between the safety-related portion and the non-safety-related portion of the power systems

With respect to these four areas of concern, the staff noted that although regulatory practice has allowed non-safety-related equipment to be powered from safety-related buses, this practice has created the potential for a number of undesirable interactions. In such situations, the isolation devices protect the safety-related equipment. These isolation devices have been the

subject of much concern, both in the main power supply area (such as breakers that open on fault current or "accident" signals) and in the instrumentation and control power supply area (such as isolation transformers and other devices). In some cases, the "isolation" devices do not isolate the full range of undesirable events. In addition, the A-17 investigation has focused on another concern. Specifically, some ASIs involve scenarios in which a non-safety-related load is supplied by a safety-related bus and is adequately isolated. The non-safety load is part of the normal plant operation and/or control. A failure in the safety-related portion can propagate and create a situation in which a plant transient occurs as a result of non-safety loads supplied by the safety-related bus and, simultaneously, significant safety-related equipment is unavailable because of the same failure.

The most significant events of this type appear to be those that involve the instrumentation and control power systems. As stated below in the discussion of these specific power supplies, the staff believes that current activities in the area of instrumentation and control power supplies should be integrated and should address this type of concern specifically. Accordingly, the staff has initiated an integrated program to review these issues.

#### Plant Support Systems

Although relatively few events of note were identified from the operating experience (Categories 13, 14, 18, and 22 of Table 1 and References 3 and 4), PRAs have consistently shown the potential importance of support systems. (Note: The electric power system, also a support system, was dealt with separately above.) This category includes other support systems such as component cooling water; service water; heating, ventilating, and air conditioning; lube oil; and compressed air.

As is the case for the electric power system, these support systems are often extensive and may be unique. These support systems can affect multiple frontline safety systems and can often affect systems not related to safety. As a result, failures in support systems can potentially initiate a transient and also can degrade other systems, some of which may have been designed to mitigate that very same event.

The support systems of concern often have interconnections between redundant divisions for operational flexibility or they may have interconnections to non-safety-related equipment. In some cases, single failures such as headers, drain lines, and vents are designed into the systems because the probability of a passive failure in conjunction with the need for the system is assumed to be low.

If the support system failure and the initiation of an event are coupled, a risk-significant situation could result from the failure of the support system (depending on other plant mitigating features).

Less attention may have been paid to the design and review of plant support systems than was paid to some of the frontline systems such as the ECCS. The



safety significance of event initiation coupled with limiting the capability for mitigation may not have been recognized.

#### Incorrect Reliance on Failsafe Design Principles

Protection systems at nuclear power plants rely on the design principle of "failsafe" to varying degrees. There have been instances (see Category 18 in Table 1 and References 3 and 4) in which some failure modes were insufficiently analyzed because someone relied too much on the concept of failsafe.

The events to date have involved the scram system and its related support functions such as the air system and electric power system. Specifically, it was discovered that water could be in the scram discharge volume (SDV) of a BWR as a result of poor drainage or an air supply failure. Water in the SDV would inhibit the insertion of control rods. The failure involving the air system was of particular concern because it involved a system that had been considered a portion of the reactor protection system not related to safety. Action was taken at all boiling-water reactors to correct this problem.

This type of ASI may have resulted from the use of a design approach that actually requires of a number of non-safety-related features to function and, therefore, does not truly rely on failsafe principles. In the case of the air system, the system was assumed to fail safe, i.e., bleed off, and, as a result, a partial failure went unanalyzed. It was also noted that the electric supply system to this scram system had been modified previously because of a similar type of concern. Specifically, the electric power was originally assumed to fail safe (i.e., voltage going to zero) and, as a result, partial failure (such as low voltage or high voltage) went unanalyzed for a time.

The problems appear to have been created when portions of the systems were allowed to be classified as not related to safety because they were assumed to always fail safe.

#### Automated Safety-Related Actions With No Preferred Failure Mode

Another area of adverse systems interactions that was highlighted involved the inadvertent actuation of an engineered safety feature (ESF) (Category 6, "Inadvertent ECCS/RHR pump suction transfer"). The most significant characteristic of this area appears to be that, unlike a reactor trip, such a function does not have an "always preferred" failure mode. As a result, extra precautions may be needed to avoid (a) a failure to actuate when needed and (b) a failure that actuates the system when not required (i.e., inadvertently). The area of automatic ECCS switch to recirculation is the subject of a separate generic issue, Generic Issue 24.

Although the reported events involved only the automatic switchover to the sump in PWRs, some concern exists that individual plants may have other functions with the same characteristic. Some possible other functions include:

- \* containment isolation functions
- \* logic that selects a faulted steam generator to isolate it
- \* low-pressure-to-high-pressure system interlocks in the RHR system



Of particular note is the possibility that these types of functions will actuate inadvertently during testing or maintenance. It is a fairly common practice to put portions of the actuation logic in a trip or actuated state and to assume then that the plant is in a "safe" condition. Although this may be true for functions that have a preferred failure mode, it may not be a conservative assumption for functions that do not have an always preferred failure mode.

#### Instrumentation and Control Power Supplies

The ORNL review (NRC, NUREG/CR-3922) highlighted several events related to instrumentation and control (I&C) power supplies (Category 14). The events at all plants, and specifically at B&W plants, have already received significant attention as outlined in the ORNL assessment. Some residual concern was expressed that the potential for a significant event related to I&C power supply interactions may still exist. Because of this concern, further review work at ORNL was identified.

ORNL completed this work (reported in Reference 5). A significant number of I&C power supply events were noted, some of which involve ASIs. Although there is concern about the area of I&C power supplies, a significant amount of work (both at NRC and in the industry) has addressed this area. The A-17 resolution has not recommended any specific requirements to deal with this area at this time, but has concluded that the existing efforts at NRC be coordinated to ensure that this critical area receives the proper emphasis. This is being done under Generic Issue 128, "Electric Power Reliability."

#### C. Recommendations

Ongoing industry reviews and evaluations of operating experience should consider the above types of events. It is further recommended that where utilities determine that specific evaluations (e.g., plant walkdowns, limited-scope accident safety analyses, or probabilistic risk assessments) are needed to address other safety concerns, awareness and recognition of potential adverse systems interactions such as highlighted above should be included in these evaluations.

#### D. References

1. U.S. Nuclear Regulatory Commission, NUREG-1174, "Evaluation of Systems Interactions in Nuclear Power Plants."
2. ---, NUREG-1229, "Regulatory Analysis for Resolution of USI A-17."
3. ---, NUREG/CR-3922, "Survey and Evaluation of System Interaction Events and Sources," January 1985.
4. ---, NUREG/CR-4261, "Assessment of System Interaction Experience in Nuclear Power Plants," June 1986.
5. ---, NUREG/CR-4470, "Survey and Evaluation of Vital Instrumentation and Control Power Supply Events," August 1986.



UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
WASHINGTON, D. C. 20555

MAY 2 1989

MEMORANDUM FOR: Edward L. Jordan, Chairman  
Committee to Review Generic  
Requirements

FROM: Eric S. Beckjord, Director  
Office of Nuclear Regulatory Research

SUBJECT: CRGR REVIEW OF PROPOSED RESOLUTION OF GI-128 WHICH INCLUDES:  
GI-48 "LCOs FOR CLASS 1E VITAL INSTRUMENT BUSES"  
GI-49 "INTERLOCKS AND LCOs FOR 1E TIE BREAKERS"  
GI A-30 "ADEQUACY OF SAFETY-RELATED DC POWER SUPPLIES"

The staff has completed its proposed resolution of Generic Issue 128 which includes Generic Issues A-30, 48 and 49. Results of the staff evaluation and the proposed licensee actions are presented in the enclosures to this letter. These documents are submitted for review by the CRGR.

Generic Issue 128 is a combination of three electrical power systems issues listed below. The three related issues were worked together in order to integrate their resolutions.

- (1) GI-48 "LCOs FOR CLASS 1E VITAL INSTRUMENT BUSES"
- (2) GI-49 "INTERLOCKS AND LCOs FOR CLASS 1E TIE BREAKERS"
- (3) GI A-30 "ADEQUACY OF SAFETY-RELATED DC POWER SUPPLIES"

Generic Issues 48 and 49 involve the potential for some plants to be operating in electrical configurations which are in violation of the plant's design basis. The proposed action involves a generic request (per 50.54(f)) to verify that the plant's safety design basis is being satisfied.

Generic Issue A-30 involves the adequacy of provisions for monitoring, maintaining and testing the dc power supplies. Since a number of related activities have resulted in recommendations to improve these areas, the proposed resolution involves a generic request for information to verify the extent of implementation of the recommendations.

Therefore, to resolve GI-128, the staff is proposing two information requests. If staff review of the licensee responses to the 50.54(f) requests indicates that additional actions are required, they will be backfit on a plant specific basis.

The proposed CRGR package has been reviewed by the Office of Nuclear Reactor Regulation (NRR), the Office for Analysis and Evaluation of Operational Data (AEOD), and the Office of General Counsel (OGC). AEOD concurred without

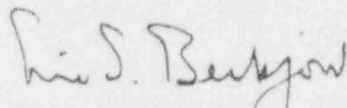
9107090004

MAY 2 1989

comment. NRR supplied a number of comments which we believe have been addressed in the enclosed package. Based on our resolution of their comments, OGC has no legal objection.

Subject to a favorable recommendation by CRGR, the GI-128 proposed resolution will be implemented by issuing the generic letters to all plants. In order to meet the schedule of the Commission's Five Year Plan, CRGR review and comments are required within five weeks of the date of this memorandum.

For further information on this matter, contact Dale Thatcher, GI-128 Task Manager (x23935).



Eric S. Beckjord, Director  
Office of Nuclear Regulatory Research

Enclosures:

1. Evaluation and Resolution of GI 48 and 49
2. Proposed Generic Letter for Resolution of GI 48 and 49
3. Technical Findings for Proposed Integrated Resolution of Generic Issue 128 (Issues 48 and 49) - EGG-NTA-7727
4. Evaluation and Resolution of GI A-30
5. Proposed generic letter for Resolution of GI A-30
6. Technical Findings for Proposed Resolution of Generic Issue 128 (Issue A-30) - EGG-NTA-8197

cc: w/o enclosures

T. Speis  
W. Houston  
W. Minners  
D. Thatcher  
R. Baer  
E. Jordan  
T. Murley  
W. Parler

w/enclosures

O. Chopra  
P. Gill  
M. Chiramal  
S. Lewis

ENCLOSURE I

## EVALUATION AND RESOLUTION OF GI 48 AND 49

### INTRODUCTION

The resolution of GI 48 and 49 includes a request for information to verify licensee compliance with the current licensing basis. Under 50.109(a)(4)(ii), a "backfit analysis" is not required where staff finds that a modification is necessary to bring facility into compliance "with a license or the rules or orders of the Commission, or into conformance with written commitments by the licensee." Therefore, under the above exception no backfit analysis is required. Under 50.54(f), if the information requested is needed to verify compliance with the facility's licensing basis, then the staff does not have to specifically justify the request in view of the potential safety significance of the issue to be addressed.

The information contained in this evaluation is intended to aid the CRGR in their review. Although not required for a compliance issue, the information presented includes that requested in the CRGR Charter (Revision A dated April 1987) and identified in the second paragraph of Section III.A.(iii). It also provides the information required by NUREG/BR-0058 Appendix A, "Analyses Required to Justify the Imposition of an Information Collection Requirement."

### BACKGROUND

GI 48 "LCOs for Class 1E Vital Instrument Buses" deals with a safety concern that some operating nuclear power plants do not have administrative controls or technical specifications governing operational restrictions for their Class 1E 120 Vac vital instrument buses and associated inverters.

Without such restrictions, the normal or alternate power sources for one or more VIBs could be out of service indefinitely. This could place certain safety systems in a situation where they could not meet the plant safety design basis, including the loss of off-site power or the single failure criterion.

GI 49 "Interlocks and LCOs for Class 1E Tie Breakers" involves a safety concern that independent, redundant Class 1E ac or dc buses can be interconnected via tie breakers which are left closed by mistake. When left closed, the tie breakers can compromise the independence of the redundant safety-related buses and, in some cases, may prevent loading of the emergency diesel generator.

These issues both involve concerns for the electrical power system. The proposed resolution of both these issues involve implementation or related administrative controls and/or technical specifications to limit conditions of operation. Therefore both issues were integrated into a single technical program. The complete technical findings for these issues are reported in Idaho National Engineering Laboratory (INEL) Report EGG-NTA-7727, Revision 3, "Technical Findings for Proposed Integrated Resolution of Generic Issue 128 (Issue 48 and Issue 49)," March 1989.



The resolution of these two issues involves an information request to all plants. The information request contains questions (to be answered by the licensees) designed to identify plants which may not comply with their license. Follow-up action will be developed if necessary, based on the responses to the information request.

#### SAFETY BENEFIT

All plants are required to be designed to withstand single failure of any Class IE power division. There have been numerous recorded events in which there have been failure of a single power division. While most plants have recovered from these events without severe complication: there have been a variety of undesirable plant conditions resulting from such failures. Events resulting from loss of vital instrument buses include the following, either singularly or in combination:

1. Severe system transients, including undercooling and overcooling transients
2. Challenges to plant operators due to lost indication
3. Inadvertent actuations of safety systems, including reactor protection and safety injection systems
4. Improper control system responses, including systems provided for feedwater and steam generator level control
5. Loss of redundancy for safety-related instrumentation channels and power supplies
6. Loss of indicators that provide information concerning plant and safety system status
7. Damage to mechanical equipment such as running pumps with closed suction valves.

Since plant operators have had difficulty in coping with the loss of a single Class IE power division, the consequences of the loss of more than one division might lead to even more severe consequences. In addition, such events may not have been analyzed and could, therefore, exceed the plant's design basis. Failure of more than one division has not typically been included in a plant's safety analysis because it is assumed that:

1. The Class IE divisional power buses are capable of performing their function independent of the offsite power source and
2. The redundant Class IE divisions are independent from each other.

The concerns covered by Generic Issues 48 and 49 involve identified situations that can compromise the assumed redundancy and independence and increase the

probability of failure of more than one division of class IE from the same event. In such cases, the plant may be in non-compliance with its design basis.

Regarding GI-48, without LCO's there are no limitations on the number of buses that can be powered from the offsite system, or the period of time during which the plant may be operated in an unanalyzed configuration. For example, if an inverter is unavailable and its corresponding bus is transferred to the offsite system, then during that unlimited time period, a loss of offsite power and a single failure (in the other divisional system) could put the plant in an unanalyzed situation. The other failure could be an inverter. A recent AEOD report entitled "Operational Experience Involving Losses of Electrical Inverters" has highlighted a large number of inverter failures.

A more serious example could occur because, with no limit on operation with inverters out-of-service, it is possible that more than one bus may be removed from service and their loads transferred to an offsite power source for extended periods of time. Then, if offsite power is lost, during the time until the diesel generators can pick up the load, the plant would be without power for those instrument buses which are connected to the offsite power source. This would result in significant loss of information to the control room and simultaneous unwanted actuations of protection systems and control systems.

Possible added safety benefit may result from the implementation of technical specifications on inverters. Plant owners would then have an additional incentive to improve the reliability of these components. Since loss of an inverter can result in plant transients/trips, an improvement in inverter reliability could provide a reduction in inverter failure rate and could reduce the potential for plant transients.

GI-49 involves tie breakers which also have the potential for compromising the assumed independence of the redundant divisions. A variety of single failures could lead to loss of both redundant emergency power divisions during time periods when a tie breaker is closed.

Also of concern is the increased probability of loss of all ac power (station blackout). If a plant were operated with the tie breaker between the two main safety-related ac buses closed, a loss of offsite power would probably result in station blackout because:

1. There are typically interlocks which prevent the diesel generator output breakers from closing when tie breakers are closed.
2. If the interlocks are not installed or malfunction, the output of two or more unsynchronized diesel generators would be tied together, causing one or more of the diesel generators to trip or fail.
3. If only one diesel generator is operable, it would not have the capability to carry the accident loads on both buses and would trip or fail.

The concerns of these issues are resolved for recently licensed and future plants by implementation of Standard Technical Specifications. It has been determined that the issue would be resolved in older plants if each plant adopts provisions equivalent to the Standard Technical Specifications

The staff and its contractor made a survey of the technical specifications of 113 plants. The following is summary of the results:

1. LCOs for Power Sources for Vital Instrument Buses  
The technical specification for 65 of the 113 plants surveyed have no listed restrictions on operation with an unavailable preferred (uninterruptible) power source for a vital instrument bus. Thirteen plants have some restrictions, but not as restrictive as the Standard Technical Specifications. Thirty-five plants have the same restrictions as contained in the Standard Technical Specifications.
2. LCOs for Vital Instrument Buses  
The technical specifications for 31 of the 113 plants surveyed have no restrictions for operating with a vital instrument bus de-energized. Sixteen plants have some restrictions but not as restrictive as contained in the Standard Technical Specifications.
3. Tie Breakers LCOs  
Of the 113 plant technical specifications surveyed, 77 have no stated restriction on plant operations with tie breakers closed. Some of these plants may not have tie breakers. Thirty-six plants do have LCO restrictions on operation with the ac breakers closed. Of these, 27 also have restriction on operations with the dc tie breakers closed.

Although the analyses conducted on these issues are mostly qualitative, the safety benefit is clear. Based on the potential safety benefit, the staff concludes that all plants should be asked to verify that they have adequate technical specifications to cover the potential safety significant situations for both the vital instrument buses and the tie breakers, or provide justification of why such provisions are not needed.

#### Proposed Resolution

The staff proposes to submit an Information Request to all licensees to identify plants that should develop additional administrative control to avoid operating under conditions that are in violation of the single failure criterion. The licensee's responses are expected to identify plants in which further action may be necessary. In most cases it is expected that licensees will voluntarily take appropriate actions without specific direction from the staff.

#### Cost

The proposed information request contains two questions. A confirmation is required from licensees with plants that have adopted the appropriate LCOs. Approximately 50% of the plants are expected to fall into this category. More

detailed information is required from plants with non-standard technical specifications unless they have chosen to incorporate the appropriate provisions. The requested information should be readily available.

The licensee cost to respond to the information request will depend on plant specifics. For a conforming plant the cost will be limited to whatever is required to provide a response to the information request. This is not expected to exceed 100 man-hours effort. Assuming \$50/man-hour, the cost would be \$5000.

Plants with deficiencies may be required to revise their plant technical specification to incorporate appropriate LCOs. A cost estimate for a change of this type to the technical specifications is stated in NUREG/CR-4568, "A Handbook for Quick Cost Estimates" to be between \$16K and \$32K. Training to accommodate the change in the technical specification may require an additional \$8K.

There is an additional cost saving consideration associated with the implementation of technical specifications on inverters. Plant owners would then have additional incentive to improve the reliability of these components. Since loss of an inverter can result in plant transients/trips, a reduction in the number of inverter failures could also result in a cost saving by reducing plant shutdowns and outages.

Implementation of the proposed plan will require NRC review for all plants not initially found to be in compliance. Once implemented, there will be no further impact on NRC resources. Total NRC resources estimated for this plan based on 50 plant reviews is 100 man-weeks.

#### Schedule

The proposed resolution allows 180 days for licensee response to the request for information. It is expected that NRC evaluation will be completed within 1 year after the licensee's submittals are received.

ENCLOSURE 2



Enclosure

DRAFT GENERIC LETTER

To: ALL HOLDERS OF OPERATING LICENSES

SUBJECT: RESOLUTION OF GENERIC ISSUES GI-48, "LCOS FOR CLASS 1E VITAL INSTRUMENT BUSES," AND GI-49, "INTERLOCKS AND LCOS FOR CLASS 1E TIE BREAKERS"

The NRC staff has completed the evaluation of Generic Issues GI-48 and GI-49, which focus on vital ac buses and tie breakers between redundant, safety-related buses. Attachment 1 provides a brief description and history of each of these GIs. Additional details are provided in reference 1.

As a result of our evaluation, the staff concludes that all licensees should include appropriate Limiting Conditions for Operation (LCOs) in their Technical Specifications and have proper administrative controls to implement these Technical Specifications unless there is adequate justification why such provisions are not needed at their specific facilities.

In order to determine whether any further staff actions are necessary to assure implementation of recommended corrective measures, we request pursuant to 10 CFR 50.54(f) and Section 182 of the Atomic Energy Act that you provide the NRC with a response to the questions in the attachment within 180 days of the date of this letter. This information should be submitted to NRC, signed under oath and affirmation. The information will enable the Commission to determine whether any further action should be taken on your license.

This request is covered by Office of Management and Budget Clearance Number 3150-0011, which expires December 31, 1989. The estimated average burden hours is 100 man-hours per licensee response, including assessment of the recommendations, searching data sources, gathering and analyzing the data, and preparing the required responses. These estimated average burden hours pertain only to these identified response related matters and do not include time for actual implementation of any related actions. Comments on the accuracy of this estimate and suggestions to reduce the burden may be directed to the Office of Management and Budget, Room 3208, New Executive Office Building, Washington, D.C. 20503, and to the U. S. Nuclear Regulatory Commission, Records and Reports Management Branch, Office of Administration and Resources Management, Washington, D.C. 20555.

If you have any questions, please contact your project manager.

Sincerely,

Attachment: 10 CFR 50.54(f) Request - GI-48, "LCOs for Class 1E Vital Instrument Buses," GI-49, "Interlocks and LCOs for Class 1E Tie Breakers"

Reference: EGG-NTA-7727 Revision 3  
"Technical Findings for Proposed Integrated Resolution of Generic Issue 128 (Issue 48 and Issue 49)"

## Attachment

### 10 CFR 50.54(f) Request GI-48, "LCOs for Class 1E Vital Instrument Buses" GI-49, "Interlocks and LCOs for Class 1E Tie Breakers"

#### INTRODUCTION

The designation "Vital Instrument Bus" may be interpreted differently for different plants. In this document, the term "Vital Instrument Buses" refers to the ac buses that provide power for the Instrumentation and Controls of the Engineered Safety Features (ESF) Systems and the Reactor Protection System (RPS) and are designed to provide continuous power during postulated events including the loss of normal offsite power. Tie breakers are devices used to cross connect either redundant class 1E buses in one unit or Class 1E buses in different units at the same site.

The NRC staff has evaluated the concerns of generic issue GI-48, "LCOs for Class 1E Vital Instrument Buses," and GI-49, "Interlocks and LCOs for Class 1E Tie Breakers." The staff has concluded that these concerns can be generally resolved by the verification or implementation of appropriate limiting conditions of operations (LCOs) in the plant technical specifications and by inclusion of associated administrative controls in plant procedures for the Class 1E buses and tie breakers. For both issues, the primary objective is to verify that plants are not being operated in violation of the design criteria of 10 CFR 50 Appendix A, for example, GDC 17, 21, 34, and 35. Conditions identified by the staff evaluation suggested a strong possibility that the single failure criterion may be violated for substantial time periods in some plants. These plants, therefore, may not meet the requirements of the design basis events considered in the plant safety analysis report.

#### BACKGROUND

The primary concern of GI-48 was identified when it was found that some operating nuclear power plants do not have any administrative controls or technical specifications governing operational restrictions for their Class 1E 120V ac Vital Instrument Buses (VIBs) and associated inverters. Without such restrictions, the normal or alternate power sources for one or more VIBs could be out of service indefinitely. This could place certain safety systems in a situation where they could not meet the plant design basis, including loss of off-site power or the single failure criterion.

Specifically, the VIBs may be subjected to power failure modes that may not have been considered during the safety analysis of the plant. For example, this situation could occur as a result of removing one or more of the normal or alternate power sources for the VIBs from service for repair or maintenance. Without some type of restrictions, more than one VIB could be connected to an offsite alternate power source. The loss of the alternate power source would then cause the simultaneous loss of more than one VIB, at least until the diesel generators pick up the loads.

The concerns of GI-49 were raised by an incident that occurred at the Point Beach Unit 2 plant. On June 9, 1980 it was discovered that a tie breaker between

the safeguards buses at the plant was improperly left closed after a plant shutdown. The improper electrical lineup probably occurred after a loss of ac power test that was conducted on May 2, 1980 and was attributed to personnel error.

This concern is limited to manually actuated tie breakers that have the capability of connecting either nominally independent, redundant Class 1E ac or dc buses at one unit or Class 1E buses in different units at the same site. These tie breakers permit convenient maintenance of supply buses and equipment without de-energizing plant equipment. The maintenance is normally conducted when the plant is not in operation. These tie breakers require special consideration, because, when closed, they can compromise the independence of the redundant safety-related buses and, in some cases, may prevent loading of the emergency diesel generator. It is also recognized that the tie breakers could be beneficial under very special conditions (such as loss of off-site power coincident with loss of a diesel or batteries) to provide flexibility to supply power across division boundaries.

Approximately 5 weeks elapsed before the improper closure at the Point Beach plant was discovered. With the two breakers closed, the two redundant buses were connected; and, consequently, the independence of the buses was lost. If there had been a loss of off-site ac power with the tie breaker closed, interlocks would have prevented automatic closure of the diesel generator output breakers.

The event at Point Beach was subsequently evaluated by the NRC staff, resulting in the identification of the generic concerns of GI-49 regarding procedural controls to reduce human error of the type that occurred at Point Beach. The staff also noted that the tie breaker interlocks to prevent manual paralleling of standby power sources, which are a provision of Regulatory Guide (RG) 1.6, Item 4(d), had not been implemented at the Point Beach plant.

It should be noted that the proposed resolution does not include a recommendation regarding the verification of tie breaker interlocks. The interlocks raised as a concern were to help protect against the potential for an operator committing an error and inadvertently closing a tie breaker between either:

- (1) two operating diesel generators which are potentially out-of-phase, or
- (2) an operating diesel generator and an incoming feeder line which are potentially out-of-phase.

Although such interlocks can provide an additional degree of assurance for some infrequent situations, we believe that such interlocks can also have a potential negative impact on safety. For example, in some emergency situations (such as loss of offsite power and failure or nonavailability of a divisional diesel generator, or a station blackout) an operator may need to cross connect power (via tie breakers) to an opposite division. In such instances, a failure in the interlocking circuits could inhibit the operator from taking such action. PRA analyses have shown that cross connecting can allow for options that can prove to be beneficial.

In addition, there is some protection provided for inadvertent out-of-phase connections by the normal protective relaying and breaker coordination. If the protective relaying actuates, equipment would be protected and normal restart could be undertaken. Therefore, the staff concluded that if proper administrative controls are placed on the operation of the tie breakers and normal protective relaying is present, then the addition of these interlocks would not be cost beneficial.

The GI-48 and GI-49 concerns have been resolved in recently licensed plants by implementation of Standard Technical Specifications and current licensing practice.

#### QUESTIONS

1. Do your plant Technical Specifications include Limiting Conditions for Operations (LCOs) and surveillance requirements for:
  - a. Vital instrument buses (typically 120V ac buses),
  - b. Inverters or other onsite power sources to the vital instrument buses, and
  - c. Tie breakers which can connect redundant Class 1E buses (ac or dc) at one unit or which can connect Class 1E buses between units at the same site.
2. Do your plant procedures include appropriate corresponding administrative controls to implement these technical specification requirements?

If the answer to any of the previous questions is no, then provide an explanation of the basis for your belief that your plant will not be operated indefinitely in violation of the single failure criterion regarding the Class 1E vital instrument buses and the closure of tie breakers connecting Class 1E ac or dc buses. This may be accomplished by either: (a) providing information and supporting analyses, or (b) submitting an amendment request proposing that appropriate LCOs be incorporated in the plant technical specifications on the above items.

The information to be provided should demonstrate that adequate consideration has been given to loss of off-site power in conjunction with a worst case additional single failure. In conjunction with these postulations, the analysis should consider the time delay for the emergency generators to pick up load, since in typical plants, if an inverter serving a vital instrument bus is out of service, a loss of off-site power will cause numerous actuations due to the delay time while the diesels are starting. The analysis should, therefore, also consider malfunctions that do not always have a preferred failure mode (e.g., instrumentation or controls that initiate a switch of emergency core cooling from injection to recirculation or initiate isolation of the steam generators). If the alternate power sources for the vital buses are not backed up by the diesel generators, then this should be stated.



An example of acceptable LCO and surveillance requirements (from the Westinghouse Standard Technical Specifications) is included for guidance.



## 3/4 LIMITING CONDITIONS FOR OPERATION AND SURVEILLANCE REQUIREMENTS

### 3/4.0 APPLICABILITY

#### LIMITING CONDITION FOR OPERATION

---

3.0.1 Limiting Conditions for Operation and ACTION requirements shall be applicable during the OPERATIONAL MODES or other conditions specified for each specification.

3.0.2 Adherence to the requirements of the Limiting Condition for Operation and/or associated ACTION within the specified time interval shall constitute compliance with the specification. In the event the Limiting Condition for Operation is restored prior to expiration of the specified time interval, completion of the ACTION statement is not required.

3.0.3 In the event a Limiting Condition for Operation and/or associated ACTION requirements cannot be satisfied because of circumstances in excess of those addressed in the specification, the unit shall be placed in at least HOT STANDBY within 1 hour, in at least HOT SHUTDOWN within the next 6 hours, and in at least COLD SHUTDOWN within the following 24 hours unless corrective measures are completed that permit operation under the permissible ACTION statements for the specified time interval as measured from initial discovery or until the reactor is placed in a MODE in which the specification is not applicable. Exceptions to these requirements shall be stated in the individual specifications.

3.0.4 Entry into an OPERATIONAL MODE or other specified applicability condition shall not be made unless the conditions of the Limiting Condition for Operation are met without reliance on provisions contained in the ACTION statements unless otherwise excepted. This provision shall not prevent passage through OPERATIONAL MODES as required to comply with ACTION statements.

#### SURVEILLANCE REQUIREMENTS

---

4.0.1 Surveillance Requirements shall be applicable during the OPERATIONAL MODES or other conditions specified for individual Limiting Conditions for Operation unless otherwise stated in an individual Surveillance Requirement.

4.0.2 Each Surveillance Requirement shall be performed within the specified time interval with:

- a. A maximum allowable extension not to exceed 25% of the surveillance interval, and

### 3/4.8.3 ONSITE POWER DISTRIBUTION

#### OPERATING

#### LIMITING CONDITION FOR OPERATION

---

---

3.8.3.1 The following electrical busses shall be energized in the specified manner with tie breakers open [both] between redundant busses within the unit [and between units at the same station]:

- a. Division #1 A.C. Emergency Busses consisting of:
  - 1) [4160]-Volt Emergency Bus # \_\_\_\_\_, and
  - 2) [480]-Volt Emergency Bus # \_\_\_\_\_.
- b. Division #2 A.C. Emergency Busses consisting of:
  - 1) [4160]-Volt Emergency Bus # \_\_\_\_\_, and
  - 2) [480]-Volt Emergency Bus # \_\_\_\_\_.
- c. [120]-Volt A.C. Vital Bus # \_\_\_\_\_ energized from its associated inverter connected to D.C. Bus # \_\_\_\_\_\*,
- d. [120]-Volt A.C. Vital Bus # \_\_\_\_\_ energized from its associated inverter connected to D.C. Bus # \_\_\_\_\_\*,
- e. [120]-Volt A.C. Vital Bus # \_\_\_\_\_ energized from its associated inverter connected to D.C. Bus # \_\_\_\_\_\*,
- f. [120]-Volt A.C. Vital Bus # \_\_\_\_\_ energized from its associated inverter connected to D.C. Bus # \_\_\_\_\_\*,
- g. [250/125]-Volt D.C. Bus #1 energized from Battery Bank #1, and
- h. [250/125]-Volt D.C. Bus #2 energized from Battery Bank #2.

APPLICABILITY: MODES 1, 2, 3, and 4.

#### ACTION:

- a. With one of the required divisions of A.C. emergency busses not fully energized, reenergize the division within 8 hours or be in at least HOT STANDBY within the next 6 hours and in COLD SHUTDOWN within the following 30 hours.
- b. With one A.C. vital bus either not energized from its associated inverter, or with the inverter not connected to its associated D.C. bus: (1) reenergize the A.C. vital bus within 2 hours or be in at least HOT STANDBY within the next 6 hours and in COLD SHUTDOWN within the following 30 hours; and (2) reenergize the A.C. vital bus from its associated inverter connected to its associated D.C. bus within 24 hours or be in at least HOT STANDBY within the next 6 hours and in COLD SHUTDOWN within the following 30 hours.

\*Two inverters may be disconnected from their D.C. bus for up to 24 hours as necessary, for the purpose of performing an equalizing charge on their associated battery bank provided: (1) their vital busses are energized, and (2) the vital busses associated with the other battery bank are energized from their associated inverters and connected to their associated D.C. bus.

## ONSITE POWER DISTRIBUTION

### LIMITING CONDITION FOR OPERATION

---

#### ACTION (Continued)

- c. With one D.C. bus not energized from its associated battery bank, reenergize the D.C. bus from its associated battery bank within 2 hours or be in at least HOT STANDBY within the next 6 hours and in COLD SHUTDOWN within the following 30 hours.

### SURVEILLANCE REQUIREMENTS

---

4.8.3.1 The specified busses shall be determined energized in the required manner at least once per 7 days by verifying correct breaker alignment and indicated voltage on the busses.

ENCLOSURE 3



**Idaho  
National  
Engineering  
Laboratory**

*Managed  
by the U.S.  
Department  
of Energy*

EGG-NTA-7727  
Revision 3

**TECHNICAL EVALUATION REPORT**

TECHNICAL FINDINGS FOR PROPOSED INTEGRATED  
RESOLUTION OF GENERIC ISSUE 128 (ISSUE 48 AND  
ISSUE 49)

R. O. Haroldsen



*Work performed under  
DOE Contract  
No. DE-AC07-76ID01570*

*Prepared for the  
U.S. NUCLEAR REGULATORY COMMISSION*



TECHNICAL FINDINGS FOR PROPOSED INTEGRATED RESOLUTION  
OF GENERIC ISSUES 128 (ISSUE 48 AND ISSUE 49)

R. O. Haroldsen

Published March 1989

Idaho National Engineering Laboratory  
EG&G Idaho, Inc.  
Idaho Falls, Idaho 83415

Prepared for the  
U.S. Nuclear Regulatory Commission  
Washington, DC 20555  
Under DOE Contract No. DE-AC07-76ID01570570  
FIN No. D6025

~~9107090014~~

## ABSTRACT

This Idaho Nuclear Engineering Laboratory report provides the technical findings and conclusions for a proposed integrated resolution of Generic Issues 48 (LCOs for Class 1E Vital Instrument Buses in Operating Reactors) and 49 (Interlocks and LCOs for Class 1E Tie Breakers).

## FOREWORD

This report is supplied as part of a program to resolve four predefined safety issues. This work is being conducted by EG&G Idaho, Inc., for the U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Research, Division of Engineering.

The NRC Task Manager for this project is D. F. Thatcher of the Engineering Issues Branch, Division of Safety Issues Resolution, Office of Nuclear Regulation Research.

The U.S. Nuclear Regulatory Commission funded this work under authorization B&R 9-60-19-520010, FIN No. D6025.

## CONTENTS

ABSTRACT .....	ii
FOREWORD .....	iii
1. INTRODUCTION .....	1
2. BACKGROUND .....	2
2.1 Generic Issue 48 .....	2
2.2 Generic Issue 49 .....	8
3. OTHER RELATED ISSUES .....	12
4. TECHNICAL FINDINGS .....	13
4.1 Generic Issue 48 .....	13
4.2 Generic Issue 49 .....	16
4.3 Alternatives for Resolution of GI 48 and 49 .....	17
5. CONCLUSIONS .....	21
5.1 Estimated Cost .....	22
6. - REFERENCES .....	23
APPENDIX 1, SURVEY OF PLANT TECHNICAL SPECIFICATIONS .....	26

TECHNICAL FINDINGS FOR PROPOSED INTEGRATED RESOLUTION  
OF GENERIC ISSUES 128 (ISSUE 48 AND ISSUE 49)

1. INTRODUCTION

A number of generic safety issues in the area of electric power systems have been identified over a period of years. These issues are listed and prioritized in NUREG-0933.<sup>1</sup> Three issues have been selected for integrated action because they are interrelated. These are:

Generic Issue A-30	"Adequacy of Safety-related DC Supplies"
Generic Issue 48	"LCOs for Class 1E Vital Instrument Buses in Operating Reactors"
Generic Issue 49	"Interlocks and LCOs for Redundant Class 1E Tie Breakers"

These three issues taken together are identified as Generic Issue 128. This report is a part of the action to resolve Generic Issue 128.

This report presents the background and technical findings for Generic Issue 48 and 49 actions recommended to resolve these two issues. These two issues are treated together because the recommended resolution for both issues involves establishing or verifying appropriate Limiting Conditions of Operations (LCOs). The resolution of Generic Issue A-30 requires a different approach described in a separate reports, EGG-NTA-8197, Revision 1.<sup>2</sup>

It is concluded in this report that Generic Issues 48 and 49 can be resolved by verifying that all licensees have appropriate LCOs in their plant technical specifications.



## 2. BACKGROUND

### 2.1 Generic Issue 48

Generic Issue 48, LCOs for Class 1E Vital Instrument Buses, involves the concern that some operating nuclear power plants do not have any administrative controls or technical specifications governing operational restrictions for their Class 1E-120 Vac Vital Instrument Buses (VIBs) and associated inverters. Without such restrictions, the normal or alternate power sources for one or more VIBs could be out of service for long periods of time, perhaps indefinitely. This could place certain safety systems in a situation where they could not meet the single failure criterion, subjecting the VIBs to loss of power events that may not have been evaluated during the safety analysis of the plant.

This situation could occur as a result of removing one or more of the normal or alternate power sources for the VIBs from service for repair or maintenance.

Initially, this problem was identified only in operating PWR plants; however, subsequent investigation indicates that the problem may also include BWR plants. This problem should not exist in recently licensed plants, because appropriate LCOs are incorporated into the plant technical specifications. The appropriate LCOs are contained in the Westinghouse and Combustion Engineering Standard Technical Specifications. These LCOs restrict operation of the plant when the normal or alternate power sources for the VIBs are out of service.

This issue was first brought to the attention of the NRC by two similar transmittals from two independent licensees. The first was a letter from the Duke Power Company dated June 6, 1980, which transmitted a Reportable Occurrence Report, RO-287/80-8.<sup>3</sup> The event at the Oconee Unit 3 plant involved the failure of an inverter power supply for a Vital Instrument

Bus (VIB) at the same time that an RPS channel was in bypass for testing. Duke Power Co. submitted a followup report in a letter<sup>4</sup> dated June 20, 1980. The followup report clarified details of the event and concluded that the event did not constitute a reportable occurrence but did provide useful information for the NRC.

Three days later, the Sacramento Municipal Utility District (SMUD) submitted a Licensee Event Report (LER),<sup>5</sup> with a followup report<sup>6</sup> on June 19, 1980. The SMUD reports describe a possible scenario in which a single failure could prevent an automatic SFAS initiation, i.e., failure of a Class 1E inverter while another is out of service. The event at Ocone and the scenario described by SMUD provided the basis for the GI 48 Issue.

Based on the licensees reports, AEOD issued a memorandum<sup>7</sup> to NRR (July 15, 1980) recommending that Limiting Conditions of Operation (LCOs) similar to those in the Standard Technical Specification be required for all operating nuclear plants.

Three subsequent NRC memoranda followed<sup>8,9,10</sup> which all concurred with the AEOD recommendation. The first of these<sup>8</sup> (from the Division of Licensing dated July 24, 1980) discusses the length of time that a VIB should be permitted to be powered by off-site power. It concludes with the recommendation that operation be limited to no more than 24 hours per month with a VIB powered from other than a battery-backed power source.

The second memorandum<sup>9</sup> was from the director of NRR (September 29, 1980) and instructed the Division of Licensing to implement appropriate technical specifications.

The third memorandum<sup>10</sup> (August 7, 1981) contains model technical specifications developed to be used as a guideline for implementing the appropriate LCOs. It also includes technical background information relating to this matter.

The current Standard Technical Specifications for Westinghouse plants<sup>11</sup> and Combustion Engineering plants<sup>12</sup> include the appropriate LCOs but equivalent LCOs are not included in the current standard specifications for GE<sup>13</sup> and B&W<sup>14</sup> plants.

While there was general agreement among the staff that the LCOs should be required for all operating reactors, there was some concern that the time limits invoked by the LCOs should be further analyzed to determine their risk benefit. A contract was implemented with the Lawrence Livermore National Laboratory (LLNL) for additional analysis. The results of the analysis were published in a report<sup>15</sup> dated October 28, 1982. The analysis was limited to an evaluation of a typical Westinghouse pressurized reactor for a specific accident sequence (LOCA).

The report includes a probabilistic risk assessment based on failure rate estimate data from WASH-1400.<sup>16</sup> It provides an estimate of the incremental risk from the operation of a VIB powered from an interruptible power source as compared to the normal mode with the bus powered from a battery-backed power source. Using a cost benefit criteria of \$1000 per man-rem, LLNL concluded that 72 hours per year is an optimum time limit that an off-normal power source should be permitted to energize a VIB during operation of a PWR.

On October 15, 1984, the Reliability and Risk Assessment Branch (RRAB), DST, provided comments<sup>17</sup> on the LLNL report in a memorandum to the Power Systems Branch, DSI. The memorandum indicates that the LLNL report may have underestimated the core melt frequency when LCO requirements for VIBs are not imposed and recommends against using the LLNL report results. The memorandum states that in addition to the accident sequence covered by the LLNL report, other accident sequences, such as loss-of-offsite power initiators without a concurrent LOCA, should have been considered. The memorandum provides a preliminary frequency estimate for this accident of between  $5 \times 10^{-6}$  and  $5 \times 10^{-5}$  per reactor year. This estimate is more than an order of magnitude higher than estimates for the accident sequence (loss of offsite power with LOCA) evaluated in the LLNL report.

The RRAB offered to perform a more comprehensive study. However, the offer was contingent on receipt of a considerable amount of plant-specific information, including descriptions of the various VIB configurations, failure modes of equipment powered from the VIBs, and maintenance schedules for VIB equipment in operating plants.

Two NRC memoranda, dated December 5, 1984,<sup>18</sup> and December 14, 1984,<sup>19</sup> contain some of the information requested by RRAB; however, much of the requested information was unavailable in existing NRC files. The search for the information revealed clearly that there is a large diversity among the plants regarding the configuration of the VIBs and the failure modes of the equipment powered from these buses. From this it is concluded that a standard set of LCOs cannot be identified (by PRA analysis) that will provide uniformly optimum risk benefit for all plants.

It should be noted that all of the risk analysis has been based on failure of a VIB caused by interruption of source power. A plant that has no restriction on operation with VIBs powered by interruptible power sources may operate with more than one VIB powered by interruptible power sources. Failure of offsite power then could cause the simultaneous failure of more than one VIB. The failure would be expected to be momentary with the power being re-established upon start of plant diesel generators but there is also the possibility that more than one of the VIBs may be connected to the same power division. In this case the independence of the VIBs would remain vulnerable to continuous failure if one of the diesel generators fails to start or if the loading sequence does not go through to completion.

Over a period from 1980 to 1984 several different time limits were considered that a VIB should be permitted to remain connected to a nonbattery-backed power source. These are summarized in the following table:

<u>Source</u>	<u>LCO</u>	<u>Reference</u>
Standard Technical Specification	Limits power operating to 24 hours with VIB connected to nonbattery source	11,12
ORAB	No more than 1 day per month with VIB connected to nonbattery source	8
DL	Start hot shutdown in 2 hours if VIBs are not supplied by battery source. Be in cold shutdown in 30 hours. Compatible with 24 hour limit in standard technical specification	10
LLNL	72 hour limit per year with VIB powered from nonbattery-backed source	15
RRAB	Disputed LLNL 72 hour limit (said risks may be underestimated) proposed a new PRA study	17

AEOD issued a report<sup>20</sup> in December 1986 addressing some of the concerns of GI-48. It includes the review of 94 licensee event reports (LERs), totaling 107 events involving inverter failures that occurred during 1982 through 1984. The study includes 35 additional events from the Nuclear Plant Reliability Data System (NPRDS) that occurred in the same timeframe. These 142 events occurred at 51 distinct plants: 26 designed by Westinghouse, 11 by General Electric, 9 by Combustion Engineering, 4 by Babcock & Wilcox, and 1 by General Atomic.

The report states that even though previous action has been taken in past years to reduce inverter failure, the actual number of inverter failures in the industry is continuing to increase. The report recommended that the office of Inspection and Enforcement issue an information notice addressing events involving inverter losses. It also recommended that plant technical specification be reviewed to ensure appropriate operating restrictions.

The recommended information notice,<sup>21</sup> IN 87-24, "Operational Experience Involving Losses of Electrical Inverters" was issued June 4, 1987. Other relevant notifications previously issued include IE



Bulletin 79-27,<sup>22</sup> "Loss of Non-Class-1E Instrumentation and Control Power Systems Bus During Operations" issued November 30, 1979 and IE Circular 79-02,<sup>23</sup> "Failure of 120 Volt Vital AC Power Supplies, January 16, 1979. The latter describes an event in which two vital instrument buses failed simultaneously.

The results of a survey of Vital Instrument power events was published in a report,<sup>24</sup> NUREG/CR-4470 in August 1986. The report evaluated 251 failures of vital instrument buses. Fifty-six percent of these occurred during steady state operations. Human error and failure of dc source power were also identified as significant causes.

The Nuclear Safety Analysis Center published two earlier relevant topical reports. These are NSAC/44,<sup>25</sup> "Investigations of Failures in I&C Power Supply Hardware," December 1981 and NSAC/48,<sup>26</sup> "Workshop on Vital DC Power," May 1982. These reports provide information to the industry regarding the numbers and types of VIB equipment failures and recommendations on preventive maintenance and repair to avoid problems.

Brookhaven National Laboratory has published three relevant topical reports. The first of these<sup>27</sup> dated April 1983 titled "Analysis of Inverter Failures in Nuclear Power Plants provides a limited analysis of inverter failures based on probability risk analysis methodology. The second<sup>28</sup> and third<sup>29</sup> reports, NUREG/CR-4564 and NUREG/CR-5051, published in June 1986 and August 1988 provide useful information on detecting and mitigating aging effects on inverters.

A survey was conducted by DSRO in April 1987 of the technical specifications for existing plants to determine, as far as was possible from available staff records, the number and identity of plants utilizing acceptable LCOs in their technical specifications.

The technical specifications for 65 of the 113 plants surveyed have no listed restrictions on operation with an unavailable preferred (uninterruptible) power source for a vital instrument bus. Thirteen plants

have some restrictions but not as restrictive as the Westinghouse or CE Standard Technical Specifications. Thirty-five plants have the same restrictions as contained in the Westinghouse and CE Standard Technical Specifications.

The technical specifications for 31 of the 113 plants surveyed have no restrictions for operating with a vital instrument bus de-energized. Sixteen plants have some restrictions but not as restrictive as contained in the Westinghouse or CE Standard Technical Specifications. Sixty-Six plants have the same restrictions as are contained in the Westinghouse or CE Standard Technical Specifications.

A more complete summary of the survey results is presented in the appendix to this report.

## 2.2 Generic Issue 49

Generic Issue 49, "Interlocks and LCOs for Redundant Class 1E Tie Breakers", involves the tie breakers that have the capability of connecting independent, redundant Class 1E ac or dc buses. These tie breakers permit convenient maintenance of supply buses and equipment without de-energizing plant equipment. The maintenance is normally conducted when the plant is not in operation. These tie breakers on the other hand, may have a potential adverse effect on plant safety when closed, because they can compromise the independence of the redundant buses and, in some cases, may prevent loading of the emergency diesel generators.

This issue was first noted in a licensee event report (LER) from Point Beach Nuclear Power Station.<sup>30</sup> The LER indicated that on June 9, 1980, it was discovered that a tie breaker between the safeguards buses at the Point Beach Unit 2 Nuclear Power Plant was improperly left closed. Approximately five weeks elapsed before the improper breaker alignment was discovered. With this breaker closed, the two redundant buses were connected. Consequently, the independence of the buses was lost. If there had been a loss of normal ac power with the tie breaker closed, interlocks would have prevented closure of both diesel generator output breakers.

The improper electrical lineup probably occurred after a loss of ac power test conducted on May 2, 1980, but prior to the unit's return to critical on May 12, 1980. A letter and attachment from the licensee to the NRC, dated June 27, 1980,<sup>31</sup> analyzed the event and consequences and attributed the improper electrical lineup to personnel error.

The event at Point Beach was evaluated in an AEOD memorandum dated August 27, 1980<sup>32</sup> which identified the generic concern regarding procedural controls to reduce human error of the type that occurred at Point Beach. The memorandum also stated that tie breaker interlocks to prevent manual paralleling of standby power sources recommended by Regulatory Guide 1.6, Item 4(d) had not been implemented at the Point Beach Plant.

A DST memorandum<sup>33</sup> dated October 10, 1980, reiterated the AEOD concerns and noted that the present licensing practice, as stated in Section 8.3.1, III 2.b, of the Standard Review Plan, requires two physically separated tie breakers, in series, between redundant Class 1E buses. The purpose for this requirement is to satisfy the single failure criterion and to assure independence between the redundant buses. It is also required that these tie breakers open automatically upon an accident, concurrent with the loss of offsite power. In addition, the Standard Technical Specifications for new plants require tie breakers between redundant buses to be open as a Limiting Condition of Operation. The Point Beach plant lacked these redundant breakers and technical specifications.

To determine the generic implications of this problem, DST reviewed the ac one-line diagrams for 20 plants. DST found that eight of these plants had at least one situation where a single tie breaker was located between redundant buses. It could not be determined from the Final Safety Analysis Reports (FSARs) if there were adequate interlock schemes for those tie breakers due to the generally insufficient FSAR information. The technical specifications for each of the eight plants were examined for requirements regarding these safety bus tie breakers; only two of the eight plants had such requirements.

The DST Memorandum concluded that a generic concern exists, and that, although it is not applicable to all plants, a significant percentage may have the problem. It also recommended that the Division of Licensing survey operating reactors to: (1) determine which, if any, operating plants have a single tie breaker between redundant safety related buses; (2) require implementation of design changes for breaker control schemes to include the above described interlocks for Class 1E buses; and (3) implement technical specifications covering the tie breakers between redundant buses as previously described.

A memorandum<sup>34</sup> dated October 16, 1980, provided an NRR response to the August 27, 1980, memorandum<sup>30</sup> from the AEOD. The NRR memorandum states that NRR had completed a review of the AEOD recommendations and concurred with its recommendations.

The current standard technical specification for Westinghouse<sup>11</sup> and Combustion Engineering<sup>12</sup> reactors have specific LCOs requiring tie breakers between redundant Class 1E buses and between units to be open during plant operation. The standard technical specifications for General Electric<sup>13</sup> and B&W<sup>14</sup> plants do not have a specific LCO requiring the tie breakers to be open but do have requirements that correct breaker alignment be verified once each 7 days. A similar requirement for verifying correct breaker alignment is included in the Westinghouse and Combustion Engineering plant technical specifications.

A survey was conducted by DSRO in April 1987 of the technical specifications for existing plants to determine, as far as possible from staff records, the number and identity of plants having acceptable Limiting Conditions of Operation for tie breakers in their technical specifications.

Of the 113 plant technical specifications surveyed, 77 have no stated restrictions on plant operations with tie breakers closed. Some of these plants may not have tie breakers. Thirty-six plants do have LCO restrictions on operation with the ac tie breakers closed. Of these, 27 also have restrictions on operations with dc tie breakers closed. Some

plants close dc tie breakers during periods when an equalizer charge is being applied to station batteries.

A more complete summary of the survey results is presented in the appendix of this report.



### 3. OTHER RELATED ISSUES

The following NRC issues are indirectly related to Generic Issues 48 and 49.

Generic Issue A-30, "Adequacy of Safety-Related DC Power Supplies," is a generic issue that is included within the larger generic issue 128. It is directed toward improving the reliability of the equipment that supplies power to the VIBs. Any action on this issue is compatible and supportive with the objectives of GI-48 and 49.

Generic Issue A-25, "Nonsafety Loads on Class 1E Power Sources" is directed toward improving the reliability of Class 1E power sources. Any action on this issue is compatible and supportive with the objective of GI-48.

Generic Issue A-44, "Station Blackout," will require plants to maintain safe conditions during periods when both on-site and off-site ac power are unavailable. Implementation of the blackout rule places added emphasis on the reliability of the dc power sources that are the normal power sources for the (UPS) power for the VIBs in most plants.

IE Bulletin 79-27<sup>22</sup> is a related previous action to ensure the adequacy of plant procedures for accomplishing cold shutdown upon loss of power to any bus (Class 1E or non-Class 1E) that supplies power for instruments and controls. This item is relevant to the concerns of GI-48 but involves the loss of only one power bus. GI-48 deals with the added possibility of losing more than one vital bus at the same time.

Regulatory Guide 1.153,<sup>35</sup> "Criteria for Power, Instrumentation and Control Portions of Safety System," December 1985, is another action relating to GI-48. However, this regulatory guide is to be implemented for construction permit applications docketed after November 1985 and is not, therefore, relevant to existing plants.

## 4. TECHNICAL FINDINGS

### 4.1 Generic Issue 48

The designation "Vital Instrument Bus" is not precisely defined, and is interpreted differently for different plants. In this evaluation, the term Vital Instrument Buses (VIBs) applies to the 120-Vac buses that are important because they provide power-instrumentation and controls for Engineered Safety Features (ESF) Systems and the Reactor Protection System (RPS).

VIBs are designed to provide continuous power during postulated events that involve the loss of normal off-site power sources. Usually, VIBs are energized continuously by a battery/inverter arrangement. Some plants use an alternate arrangement that utilize a motor-generator set instead of an inverter. Either arrangement provides power to energize the VIBs that is not interrupted by loss of off-site power. These power sources are commonly known as Uninterruptible Power Sources (UPS); off-site power sources are often identified as Interruptible Power Sources (IPS).

Past activities and efforts to resolve GI-48 have produced a considerable amount of relevant information relating to this issue. The following summarizes some of the pertinent information.

1. The GI-48 issue is not uniformly generic to all operating reactors. The VIBs and the systems powered by the VIBs exist in a variety of configurations. There are a number of different failure modes following power failure, depending on the configurations.
2. At recently licensed PWR plants, the VIBs are normally supplied power from battery-backed inverters, but VIBs at some older plants are normally supplied power from IPS sources backed up by emergency diesel generators. The failure modes on loss of a VIB for control systems are generally preselected to ensure that no

control action occurs or that the action is in a safe direction consistent with the assumptions of the safety analysis. With the loss of more than one VIB, other failure modes appear to be possible, e.g., initiation or prevention of ESF action.

3. There are operating plants in which continuous operation is permitted with more than one VIB energized from an IPS.
4. VIBs that are supplied power from an IPS backed up by emergency generator power are subject to temporary interruption (presumed to be 10 seconds upon loss of incoming power). The consequences of the interruption are dependent on the plant designs and may have safety implications.
5. Initially, operating BWR plants were excluded from consideration under GI-48. There have been fewer problems reported for these plants. In some BWR plants, motor generators (MG) are used instead of inverters. These plants also differ in that the MG sets are normally powered by an IPS that switches automatically without interruption to battery or diesel generator power upon failure of incoming (IPS) power. While this system has been more reliable it is vulnerable to events similar to those identified for PWR plants.

An effort has been made to conduct probability-risk-assessment (PRA) evaluations on this issue. Unfortunately, the diversity of the plant VIB configurations and equipment failure modes render true generic analysis by the PRA method impractical. Valid plant-specific PRA analysis would require consideration of numerous plant-specific variations. However, a PRA type evaluation relating to this issue was conducted by Lawrence Livermore National Laboratory (LLNL)<sup>15</sup> for a typical Westinghouse reactor and specific accident sequence. The LLNL study is based on assumptions that are too narrow to be generically applicable. Nevertheless, the study does have significance. Conclusions from the LLNL study are summarized in Section 2.1 of this report.

Another PRA study with limited relevance to GI-48 was conducted by the Brookhaven National Laboratory and is documented in their report<sup>36</sup> dated April 1983. This report does not provide useful results for resolving this issue but concludes that more detailed study is needed to draw generic conclusions on the risk significance of inverter losses.

If it were possible, it would be helpful to obtain statistical information on the amount of time that existing operating reactors have operated with one or more UPSs out of service. However, this is not a reportable event; therefore, it is not available from any of the established event reporting information systems. There is, however, considerable statistical information<sup>38,39,40,41</sup> on events relating to the VIBs and the UPS equipment which are typically used to energize the VIBs.

All nuclear plants are presumably designed to withstand the failure of at least one VIB, but several undesirable plant conditions have resulted from such failures. Among those identified are the following:

1. Severe system transients, including reactor cooling transients.
2. Challenges to plant operators and the remaining functional equipment.
3. Inadvertent actuation of safety systems, including reactor protection and safety injection systems.
4. Improper control system responses, including systems provided for feedwater and steam generator level control.
5. Loss of redundancy for safety-related instrumentation channels and power supplies.

6. Loss of indicators that provide information concerning plant and safety systems.
7. Damage to mechanical equipment.

There has been an increasing number of events in recent years involving failures of instrument buses.<sup>37</sup> While GI-48 is specifically directed toward verifying or implementing LCOs that restrict the time that a UPS is permitted to remain out of service, the restriction will provide some incentive for licensees to improve the reliability of the UPS and inverters. There is a separate effort to reduce age related failures of inverters discussed in Section 2.1 of this report.

The number of VIB (or UPS) failures is an indicator of the potential for failure of more than one VIB at the same time. There are 251 VIB failures tabulated in NUREG/CR-4470<sup>38</sup> of which 56% occurred during steady state operation. Many of these failures (43%) were caused by inverter failure. Human error and failure of DC source power were also identified as significant causes.

The NRC case study report, AEOD/C605,<sup>41</sup> "Operational Experience Involving Losses of Electrical Inverters," dated December 1986, includes the review of 94 licensee event reports (LERs), totaling 107 events involving inverter losses that occurred during 1982 through 1984. The study includes 35 additional events from the Nuclear Plant Reliability Data System (NPRDS) that occurred in the same timeframe. These 142 events occurred at 51 distinct plants: 26 designed by Westinghouse, 11 by General Electric, 9 by Combustion Engineering, 4 by Babcock & Wilcox, and 1 by General Atomic.

#### 4.2 Generic Issue 49

This issue deals primarily with the adequacy of procedural and administrative controls that are used to monitor and provide assurance that the tie breakers between redundant Class 1E divisions of electrical power and multi-units are always open during plant operation. Such controls are necessary to provide assurance that the Class 1E power buses are not compromised.



There is also a related concern involving electrical interlocks to prevent out-of-synchronization interconnections of a diesel generator to either the offsite power source or another diesel generator. This possibility exists while a tie breaker is closed, unless it is prevented by interlocks. Conversely, inadequately designed interlocks may prevent startup and loading of a diesel generator. Tie breaker interlocks to prevent manual paralleling of diesel generators are recommended by Regulatory Guide 1.6, position 4(d). Regulatory Guide 1.6 also specifically recommends against the use of any automatic paralleling of standby power sources, automatic connecting of load groups, or transferring of loads between redundant power sources and calls for interlocks to prevent paralleling of standby power sources through operator error.

Present licensing practice, as stated in Section 8.3.1, III 2.b of the Standard Review Plan, requires two physically separated tie breakers, in series, between redundant Class 1E buses. The purpose of this requirement is to satisfy the single failure criterion and to provide physical independence between the buses. Interlocks are also required to open these tie breakers automatically upon an accident concurrent with the loss of off-site power. In addition, the Standard Technical Specifications for new plants require tie breakers between redundant buses to be open as a Limiting Condition of Operating (LCO). Some plants have resolved the issue completely by eliminating tie breakers from their designs.

#### 4.3 Alternatives for Resolution of GI 48 and 49

Several alternatives have been considered for resolving these two issues. The advantages and disadvantages of each possible alternative action are similar for both issues. An integrated description of the possible alternative actions for both issues is summarized in the following:

- A. Require all plants to incorporate appropriate LCOs in their plant technical specifications.

- B. Initiate no new action. Provide justification for closing the issues based on evaluations of the issues and the results of other NRC actions.
- C. Issue a special notice to licensees with no response required that calls attention to the concerns of these two issues.
- D. Initiate or require new PRA studies to further assess the risk of the concerns. Follow-on action would be developed from the results of the PRA studies.
- E. Initiate an information request to all plants. The information request would contain questions (to be answered by the licensees) designed to selectively identify the plants at risk. Follow-up action would be developed as required, based on the responses to the information request.

#### Discussion of Alternatives

- A. The first alternative (require appropriate LCOs in plant technical specification) would constitute an acceptable resolution for these issues. However, universal imposition of such LCOs may not allow for special situations or variations in plant configuration. This approach may, therefore, impose excessive burdens on plants that are not at risk or do not have the problem. It would probably be necessary to adapt the LCOs to the specific plant configuration on a case-by-case basis. While this approach would provide an acceptable resolution for these issues, it is probably not the most cost effective.
- B. No action on these issues could be considered as a possible adequate resolution of the issues. Such an approach could conceivably be justified by a combination of other NRC actions and an evaluation of the residual risk following such actions. This approach was considered but found to be inadequate because the evidence strongly indicates that some action is required to avoid a significant safety risk on some plants.

- C. The issuance of special notices to direct attention to these issues has also been considered as a possible adequate resolution of the issues. There have been some special notices issued that are relevant to these issues. The primary disadvantage of this approach is that there is no adequate way to measure the success or to evaluate the response to the notice. Evaluation of the issues indicates that a more positive action is necessary to resolve the issues.
- D. Additional PRA studies on these issues have been considered but a complete PRA study has been ruled out as impractical because of the diversity of plant configurations. A limited PRA study was completed for GI-48 for a "typical Westinghouse plant." A more comprehensive PRA study was started but was aborted when it became evident that a meaningful study would require a different PRA study for each plant.
- E. The alternative of issuing an Information Request to all plants is judged to be the most promising alternative for obtaining a cost-effective resolution of the issues. The Information Request should be designed primarily to identify plants in which the single failure criterion is violated for lack of appropriate administrative controls (LCOs) relating to these issues. It should also be designed to make licenses of deficient plants aware of any obvious need to upgrade administrative controls to meet requirements of their original license.

## 5. CONCLUSIONS

A basic objective of the resolution of GI-48 and -49 is to assure that all plants meet the requirements necessary to cope with the design basis events identified in the plant safety analysis report. This assurance is currently suspect, because some plants evidently have VIBs that under some operating conditions are vulnerable to simultaneous failures due to a single initiating event (loss of incoming power for GI-48 and a common bus fault for GI-49). The root problem is that some plants may operate in violation of the design basis criteria (10 C.F.R. 50, Appendix A, GDC 17, 21, 34, and 35).

Selection of Alternative E will provide reasonable assurance that the plants will not be operated under identified conditions that are in violation of the single fault criterion. It is proposed that an Information Request composed to resolve these issues be sent to all operating licensed plants. The Information Request should include questions designed to require plants to reveal the existence of permissible plant operating conditions in which the single failure criteria are not met. Since this is an existing licensing requirement for all plants, it is expected that plants admitting noncompliance will voluntarily submit a description of proposed action to resolve the problem. Current licensing practice includes a resolution of these concerns for all plants recently or not yet licensed.

The most common reaction anticipated from plants needing action is the implementation of appropriate LCOs. This assumption is based on the fact that it is probably the simplest and cheapest resolution, as well as the recommended action by the staff. This does not rule out exceptions where either a different action or no action may be justified based on unique plant configurations.

It is expected that plant responses to the Information Request will be evaluated by the NRC staff on a plant-by-plant basis. Licensee submittals could be considered acceptable if reasonable assurance is provided that

operation is limited (except for short periods of time) to conditions that meet the design basis criteria.

It should be noted that the proposed resolution does not include a recommendation regarding the verification of the tie breaker interlocks. The interlocks raised as a concern by AEOD was to help protect against the potential for an operator committing an error and inadvertently closing a tie breaker between either:

- (1) two operating diesel generators which are potentially out-of-phase or
- (2) an operating diesel generator and an incoming feeder line which are potentially out-of-phase.

Although such interlocks can provide an additional degree of assurance for some infrequent situations, we believe that such interlocks can also have a potential negative impact on safety. For example, in some emergency situations (such as loss of offsite power and failure or unavailability of a divisional diesel generator, or a station blackout) an operator may need to cross connect power (via the tie breakers) to an opposite division. In such instances, a failure in the interlocking circuit could inhibit him from taking such action. PRA analyses have shown that cross connecting can allow for options that can prove to be beneficial (SECY 89-058<sup>42</sup>). In addition, there is some protection provided for inadvertent out-of-phase connections by the normal protective relaying and breaker coordination. If the protective relaying actuates, equipment would be protected and manual restart could be undertaken.

### 5.1 Estimated Cost

The licensee cost of this proposed action is dependent on the time requirement to collect and document the requested information. This effort is estimated to average 100 man-hours which based on \$50 per hour would result in a cost to the licensee of \$5000.



The cost for those plants that have to take additional action to implement the new technical specification provisions include the cost of developing and implementing the required LCOs. An estimate of this cost, based on information in NUREG/CR-4568,<sup>43</sup> is between \$24K and \$40K.

The proposed plan includes administrative controls that would become part of the existing plant procedures. There is, therefore, no significant continuing cost to the licensee associated with this action.

NRC resources is estimated to require 2 man-weeks to review the responses from each plant that does not provide verification of appropriate LCOs. If 50 plants are found to be in this category, 100 man-weeks would be required.

## 7. REFERENCES

1. NUREG-0933, A Prioritization of Generic Safety Issues, Revision 5, March 1987.
2. EGG-NTA-8197, Revision 1, "Technical Findings for Generic Issue 128 (Issue A-30) Adequacy of Safety Related DC Power Supplies," March 1989, R. O. Haroldsen and A. C. Udy.
3. Letter, W. O. Parker, Jr., Duke Power Co., to J. P. O'Reilly, NRC, June 6, 1980, Transmitting Reportable Occurrence Report, RO-287/80-8.
4. Letter, W. O. Parker, Jr., Duke Power Co., to J. P. O'Reilly, NRC, June 20, 1980.
5. LER Report 312-80028 for Rancho Seco, June 9, 1980 by R. W. Colombo, Sacramento Municipal Utility District.
6. Letter, J. J. Mottimor, Sacramento Municipal Utility District, to R. H. Engelken, NRC, June 19, 1980.
7. Memorandum, C. Michelson, AEOD, to H. R. Denton, NRR, "Operational Restrictions for Class 1E 120 Vac Vital Instrument Buses," July 15, 1980.
8. Memorandum, J. T. Beard, ORAB, to G. Lainas, "Operational Restrictions for Class 1E 120 Vac Vital Instrument Buses," July 24, 1980.
9. Memorandum, H. R. Denton, NRR, to C. Michelson, AEOD, "LCO for Class 1E Vital Instrument Buses in Operating Reactors," September 29, 1980.
10. Memorandum, G. Lainas, DL, to T. Novak, DL, "Operational Restrictions for Class 1E 120 Vac Vital Instrument Buses," August 7, 1981.
11. Standard Technical Specifications, Westinghouse, NUREG-0452, Revision 4.
12. Standard Technical Specifications, Combustion Engineering, NUREG-0212, Revision 3.
13. Standard Technical Specifications, General Electric, NUREG-0123, Revision 3.
14. Standard Technical Specifications, B&W, NUREG-0103, Revision 4.
15. UCID-19469, "Lawrence Livermore Laboratory Technical Evaluation Report on the 120 Vac Vital Instrument Buses and Inverter Technical Specifications, Issue B71," G. St. Leger-Barter and R. L. White, October 28, 1982.

16. WASH 1400, NUREG-75/014, U.S. Nuclear Regulatory Commission, "Reactor Safety Study," October 1975.
17. Memorandum, A. Thadani, RRAB, to M. Srinivasen, PSB, "Operational Restrictions for Class 1E 120 Vac Vital Instrument Buses (Generic Issue 48)," October 15, 1984.
18. Memorandum, M. Srinivasen, PSB, to F. Rosa, ICSB, "Operational Restrictions for Class 1E 120 V Vital Instrument Buses and Inverters (Generic Issue 48)," December 5, 1984.
19. Memorandum, F. Rosa, ICSB to M. Srinivasen, PSB, "Operational Restrictions for Class 1E 120 V Vital Instrument Buses and Inverters (Generic Issue 48)," December 14, 1984.
20. AEOD/C605 Case Study Report, "Operational Experience Involving Losses of Electrical Inverters," by F. Ashe, December 1986.
21. IE Information Notice 87-24, "Operational Experience Involving Losses of Electrical Inverters," June 4, 1987.
22. IE Bulletin 79-27, "Loss of Non-Class 1E Instrumentation and Control Power Bus During Operation," November 30, 1979.
23. IE Circular 79-02, "Failure of 120 Volt Vital AC Power Supplier," January 16, 1979.
24. NUREG/CR-4470, "Survey and Evaluation of Vital Instrumentation and Control Power Supply Events," August 1986.
25. NSAC-44, "Investigation of Failures in I&C Power Supply Hardware," Electric Power Research Institute, December 1981.
26. NSAC-48, "Workshop on Vital DC Power," Electric Power Research Institute, May 1982.
27. Brookhaven National Laboratory, "Analysis of Inverter Failures in Nuclear Power Plants," G. E. Bozoki and I. A. Papazoglou, April 1983.
28. NUREG/CR-4564, "Operating Experience and Aging-Seismic Assessment of Battery Chargers and Inverters," Gunther, Subudhi and Taylor, June 1986.
29. NUREG/CR-5051, "Detecting and Mitigating Battery Charger and Inverter Aging," Gunther, Lewis and Subudhi, August 1983.
30. Licensee Event Report, LER No. 80-005/03L0, Docket No. 05000301, Facility: Point Beach-2, Event Date: June 9, 1980.
31. Letter, C. Fay, Wisconsin Electric Power Company, to J. Keepler, NRC, "Docket No. 50-301, Point Beach Nuclear Plant Unit 2, Licensee Event Report No. 80-005/03L-0," June 27, 1980.

32. Memorandum, C. Michelson, Director, Office for Analysis and Evaluation of Operational Data, to H. R. Denton, Director, Office of Nuclear Reactor Regulation, "Tie Breakers Between Redundant Class 1E Buses - Point Beach Nuclear Plant, Units 1 and 2," August 27, 1980.
33. Memorandum, F. Schroeder, Acting Director, Division of Safety Technology, to D. Eisenhut, Director, Division of Licensing, "Request for Division of Licensing Action of Interlocks and LCOs for Tie Breakers Between Class 1E Buses (Point Beach Nuclear Plant, Units 1 and 2)," October 10, 1980.
34. Memorandum, H. R. Denton, Director, Office of Nuclear Reactor Regulation, to C. Michelson, Director, Office of Analysis and Evaluation of Operational Data, "Interlocks and LCOs for Redundant Class 1E Tie Breakers (Point Beach Nuclear Plant, Units 1 and 2)," October 16, 1980.
35. Regulatory Guide 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems," December 1985.
36. Brookhaven National Laboratory, "Analysis of Inverter Failures in Nuclear Power Plants," G. E. Bozoki and I. A. Papazoglou, April 1983.
37. Memorandum, C. J. Heltemes, Jr., AEOD, to Distribution, "Preliminary Case Study Report--Operational Experience Involving Loss of Electrical Inverter," June 17, 1986.
38. NUREG/CR-4470, "Survey and Evaluation of Vital Instrumentation and Control Power Supply Events," August 1986.
39. NSAC-44, "Investigation of Failures in I&C Power Supply Hardware," Electric Power Research Institute, December 1981.
40. NSAC-48, "Workshop on Vital DC Power," Electric Power Research Institute, May 1982.
41. AEOD/C605 Case Study Report, "Operational Experience Involving Losses of Electrical Inverters," by Frank Ashe, December 1986.
42. SECY-89-058, "Status Report and Preliminary Results of NUREG-1150", February 17, 1989.
43. NUREG/CR-4568, "A Handbook for Quick Cost Estimates," April 1986.



## APPENDIX I

### GI-48 and 49 SURVEY OF PLANT TECHNICAL SPECIFICATIONS SUMMARY OF APRIL 1987 SURVEY RESULTS

The survey was conducted by the staff in April 1987 utilizing available staff records. Plant specific information obtained by the survey is tabulated in Table 1. Highlight information is presented below.

#### LCOs for Power Sources for Vital Instrument Buses

The technical specification for 35 of the 113 plants surveyed have the same restrictions on operation with an unavailable preferred (uninterruptible) power source for a vital instrument bus as contained in the Westinghouse or CE Standard Technical Specifications. Thirteen plants have some restrictions but not as restrictive as the Westinghouse or CE Standard Technical Specifications. Sixty-five of the plants have no listed restrictions.

#### LCOs for Vital Instrument Buses

The technical specifications for 66 of the 113 plants surveyed have the same restrictions for operating with a vital instrument bus de-energizer as contained in the Westinghouse or CE Standard Technical Specifications. Sixteen plants have some restrictions but not as restrictive as the Westinghouse or CE Standard Technical Specifications. Thirty-one of the plants have no listed restrictions.

#### Tie Breakers LCOs

Of the 113 plant technical specifications surveyed, 77 have no stated restrictions on plant operations with tie breakers closed. Some of these plants may not have tie breakers. Thirty-six plants do have LCO restrictions on operation with the ac breakers closed. Of these, 27 also



have restrictions on operations with dc tie breakers closed. Some plants close dc tie breakers during periods when an equalizer charge is being applied to station batteries.

TABLE 1. SURVEY OF PLANT TECHNICAL SPECIFICATIONS

Plant	Vital Inst Bus LCOs			Power Supply LCOs for Vital Instrument Buses			Tie Breaker LCOs			Notes
	STS	ALT	None	STS	ALT	None	AC	DC	No Info	
ANO-1			✓			✓			✓	
ANO-2	✓					✓	✓			AC only
Arnold			✓			✓			✓	
Beaver Valley 1	✓					✓			✓	
D. Besse	✓					✓	✓			AC only
Braidwood 1 and 2	✓			✓					✓	
Browns Ferry 1		7 days				✓			✓	
Browns Ferry 2		7 days				✓			✓	
Browns Ferry 3		7 days				✓			✓	
Brunswick 1	✓					✓	✓	✓		No R check
Brunswick 2	✓					✓	✓	✓		No R check
Byron 1 and 2	✓			✓					✓	
Crystal River 3	✓				✓				✓	
Diablo Canyon 1 and 2	✓			✓					✓	
Callaway 1	✓			✓			✓	✓		
Calvert Cliffs 1	✓					✓	✓			AC only
Calvert Cliffs 2	✓					✓	✓			AC only
Catawba 1 and 2	✓			✓			✓			AC only
Clinton 1	✓			✓					✓	
Comanche Peak 1 and 2	✓			✓					✓	No tie breakers
D. C. Cook 1 and 2	✓					✓	✓	✓		MG sets
Cooper 1		✓			✓				✓	
Dresden 2 and 3			✓			✓			✓	

TABLE 1. (continued)

Plant	Vital Inst Bus LCOs			† Power Supply LCOs for Vital Instrument Buses			Tie Breaker LCOs			Notes
	STS	ALT	None	STS	ALT	None	AC	DC	No Info	
Farley 1	✓				✓	✓			✓	
Farley 2	✓			✓					✓	
Fermi 2	✓					✓	✓	✓		
Fitzpatrick 1		✓			✓				✓	MG sets
Ft. Calhoun	✓					✓			✓	
Ft. St. Vrain			✓			✓			✓	
Ginna			✓			✓			✓	
Grand Gulf 1			✓			✓			✓	
Haddamneck			✓			✓			✓	
S. Harris 1	✓			✓			✓	✓		
Hatch 1		✓			✓				✓	MG sets
Hatch 2	✓				✓		✓	✓		
Hope Creek	✓			✓					✓	
Indian Pt. 2			✓			✓			✓	
Indian Pt. 3		✓			✓				✓	
Kewaunee			✓			✓			✓	
LaSalle 1 and 2	✓					✓			✓	
Lacrosse	✓					✓	✓	✓		
Limerick 1 and 2			✓			✓			✓	
Maine Yankee			✓			✓			✓	
McGuire 1 and 2	✓			✓			✓			AC only
Millstone 1			✓			✓			✓	

TABLE 1. (continued)

Plant	Vital Inst Bus LCOs			Power Supply LCOs for Vital Instrument Buses			The Breaker LCOs			
	STS	ALT	None	STS	ALT	None	AC	DC	No Info	Notes
Millstone 2	/			/			/	/		
Millstone 3	/			/			/	/		
Monticello	/	/		/			/	/		
Nine Mile Pt. 1	/	/		/			/	/		
Nine Mile Pt. 2	/			/			/	/		
North Anna 1 and 2	/			/			/	/		
Oconee 1, 2 and 3	/	/		/	/		/	/		
Oyster Creek	/	/		/			/	/	a	
Palisades	/	/		/			/	/		
Palo Verde 1, 2, 3	/			/			/	/		
Peach Bottom 2 and 3	/	/		/			/	/		
Perry 1 and 2	/			/			/	/		
Pilgrim	/	/		/			/	/		
Pt. Beach 1 and 2	/	/		/			/	/		
Prairie Island 1 and 2	/	/		/			/	/		
Quad Cities 1 and 2	/	/		/			/	/		
Rancho Seco	/	/		/			/	/		
River Bend	/			/			/	/		
Big Rock Pt. 1	/	/		/			/	/		
Robinson	/	/		/			/	/		
Salem	/			/			/	/		
San Onofre 1, 2, 3	/	/		/			/	/		
Seabrook	/	/		/			/	/		

TABLE 1. (continued)

Plant	Vital Inst Bus LCOs			Power Supply LCOs for Vital Instrument Buses			Tie Breaker LCOs				Notes
	STS	ALT	None	STS	ALT	None	AC	DC	No Info		
Shoreham	✓					✓	✓	✓			
South Texas	✓			✓						✓	
St. Lucie 1	✓					✓				✓	
St. Lucie 2	✓			✓			✓	✓			
Summer	✓			✓			✓	✓			
Surry 1 and 2			✓			✓				✓	
Susquehanna 1 and 2	✓					✓	✓			✓	
TMI-1			✓			✓				✓	
Trojan	✓					✓	✓				AC only
Turkey Pt. 3 and 4			✓			✓				✓	
Vermont Yankee			✓			✓				✓	
Vogtle 1 and 2	✓			✓			✓	✓			
Waterford 3	✓			✓						✓	
Watts Bar 1	✓			✓			✓	✓			
WNP 2	✓					✓	✓	✓			
Wolf Creek 1	✓			✓			✓	✓			
Yankee Rowe	✓					✓	✓	✓			
Zion 1 and 2		✓			✓					✓	
TOTALS	113	66	16	31	35	13	65	36	27	77	

LCO - Limiting Condition of Operation  
 UPS - Uninterruptible Power Source  
 STS - Standard Technical Specification  
 ALT - Alternate  
 MIN - Minimal Requirements

a. Insufficient information. Some tie breaker restrictions.



NRC FORM 325  
(2-84)  
NRCM 1102  
3201, 3202

U.S. NUCLEAR REGULATORY COMMISSION

1 REPORT NUMBER (Assigned by NRC and Vol. No. (any))

BIBLIOGRAPHIC DATA SHEET

EGG-NTA-7727  
Revision 3

SEE INSTRUCTIONS ON THE REVERSE

2 TITLE AND SUBTITLE

TECHNICAL FINDINGS FOR PROPOSED INTEGRATED RESOLUTION OF  
GENERIC ISSUE 128 (ISSUE 48 AND ISSUE 49)

3 LEAVE BLANK

4 DATE REPORT COMPLETED

MONTH

YEAR

March

1989

5 DATE REPORT ISSUED

MONTH

YEAR

March

1989

3 AUTHOR(S)

R. O. Haroldsen

7 PERFORMING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)

EG&G Idaho, Inc.  
P. O. Box 1625  
Idaho Falls, ID 83415

8 PROJECT/TASK/WORK UNIT NUMBER

9 FIN OR GRANT NUMBER

D6025

10 SPONSORING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)

Division of Engineering  
Office of Nuclear Regulatory Research  
U.S. Nuclear Regulatory Commission  
Washington, DC 20555

11a TYPE OF REPORT

Technical Evaluation Report

b PERIOD COVERED (inclusive dates)

12 SUPPLEMENTARY NOTES

13 ABSTRACT (200 words or less)

This EG&G Idaho, Inc., Idaho National Engineering Laboratory report provides the technical findings for a proposed integrated resolution of Generic Issue 128 (Issue 48, LCOs for Class 1E Vital Instrument Braces in Operating Reactors, and Issue 49, Interlocks and LCOs for Class 1E Tie Breakers.)

14 DOCUMENT ANALYSIS -- KEYWORDS/DESCRIPTORS

15 IDENTIFIERS/OPEN ENDED TERMS

15 AVAILABILITY  
STATEMENT

Unlimited  
Distribution

16 SECURITY CLASSIFICATION

This page

Unclassified

This report

Unclassified

17 NUMBER OF PAGES

18 PRICE

ENCLOSURE 4

## Evaluation and Resolution of GI A-30

### Introduction

The resolution of GI A-30 includes a request for information pursuant to development of a staff position. Under the provisions of 10CFR50.54(f) a burden analysis has been performed. The information contained in this evaluation is intended to aid the CRGR in their review and includes information requested in the CRGR Charter (Revision 4 dated April 1987) Section III.A.(iii) for 50.54(f) requests. It also provides the information required by NUREG/BR-0058 Appendix A, "Analyses Required to Justify the Imposition of an Information Collection Requirement."

### Evaluation and Proposed Resolution for GI A-30

#### Background

GI A-30 "Adequacy of Safety Related DC Power Supplies" deals with a safety concern that some plants may not have adequate provisions for assuring that these power supplies are available and capable of performing their function.

Safety-related dc power is used for the overall operation of the safety-related portions of the electrical system including circuit breaker control for the ac power. It is typically also a source of vital ac power (via the vital inverters) for safety-related instrumentation and logic systems as well as operator indications. During normal operation, the battery chargers supply the load requirements and maintain the batteries fully charged to be available during loss of offsite power. For a loss of offsite power event, battery power is particularly important during the time period when the diesel generators are starting and immediately thereafter, because the circuit breaker control to sequence loads and the excitation of the generator field windings is entirely dependent on dc power.

Under a postulated Station Blackout (USI A-44) the batteries would be the only source of electrical power available. DC power, during this postulated event, is needed for operability of the steam driven auxiliary feedwater system in PWRs and for the RCIC and HPCI systems in BWRs. These are typically the only systems available to mitigate a station blackout event. All of these systems require dc power for operation of valves and for system control. Further, instrumentation to inform the plant operators of plant status and to allow them to diagnose and correct the cause of the station blackout would be entirely dependent on the dc power supply system.

The proposed resolution of GI A-30 involves a number of recommended provisions for tests and maintenance and a number of provisions for monitoring the dc power supply status. Many of these provisions may have already been implemented at a large number of plants. A more detailed discussion of this issue is contained in Idaho National Engineering Laboratory (INEL) Report EGG-NTA-8197, Revision 1, "Technical Findings, Generic Issue 128 (Issue A-30), Adequacy of Safety Related DC Power Supplies," March 1989.

### Safety Benefit

Risk analyses have been performed on some typical plant configurations that indicate that failure of a dc power system could represent a significant contribution to the unreliability of shutdown cooling. Plants must provide for some redundancy in the safety-related dc power system to meet the GDC. Operating experience over the years has highlighted some types of common cause events that may lead to the loss of more than one division of safety-related dc power. Information taken from LER data indicates that there have been a substantial number of reportable events that involved the safety-related dc systems.

Of particular concern has been the apparent lack of sufficient battery maintenance and surveillance. This concern, coupled with some lack of adequate monitoring of the condition of the dc power sources, has led to a number of actions by both NRC and INPO. Industry standards have been revised and current Standard Technical Specifications (STS) and licensing practice now include provisions for improved battery maintenance, testing and monitoring. Recommendations for similar improvements have been issued in notifications to all plant licensees. The staff believes that a significant number of plants have made improvements. Since most of the revised industry standards were not issued as requirements, the staff is unable to determine whether or not all plants have implemented all the recommended improvements.

The staff and its contractor made a survey of the technical specifications of 113 plants in the area of battery surveillance. It was found that 37 plants utilize the Standard Technical Specification.

### Proposed Resolution

The staff believes that the most cost-effective approach to resolve the A-30 issue is for the staff to request certain information from all plants (pursuant to 10 CFR 50.54(f)) in order that the NRC can establish that adequate measures have been or will be taken at all facilities. Only a portion of the measures would be reflected in a plant's technical specifications. The responses may indicate that in some cases improvements in dc system surveillance, maintenance and procedures are necessary.

### Information Required by CRGR

The CRGR Charter (Revision 4 dated April 1987) identifies the information necessary for CRGR evaluation for information requests that may lead to a new staff position. The applicable required information is listed in Section III.A.(iii) as follows:

- (a) A problem statement that describes the need for the information in terms of potential safety benefit.
- (b) The licensee actions required and the cost to develop a response to the information request.
- (c) An anticipated schedule for NRC use of the information.

The description of the A-30 problem and the potential safety benefit is contained in the previous section.

The proposed request for information is in accordance with the provisions of 10CFR50.54(f). The purpose of the request is to determine the extent of implementation of the recommended A-30 actions previously submitted to licensees by the NRC and other industry groups. The request will gather information that may lead to the development of a new staff position which would extend the A-30 provision implemented on current plants to include previously licensed plants. However, if the information request verifies that these provisions have already been adequately implemented, then no further NRC action will be needed.

#### Costs

The proposed request contains several multi-part questions. Licensees who have acted on past bulletins, notices and industry communications, as well as more recently licensed plants, will be able to provide adequate responses with a minimum amount of effort. For conforming plants, the licensee effort is not expected to exceed 100 man-hours. Assuming \$50/man-hour, the cost would be \$5000. Other plants may require additional effort. However, the proposed plan imposes no action on licensees beyond responding to the request for information.

Implementation of the proposed plan will require review for all plants not initially found to be in compliance. Total NRC resources estimated for this plan based on 50 plant reviews is 100 man-weeks.

#### Schedule

The proposed plan allows 180 days for licensee response to the request for information. It is expected that NRC evaluation of licensee responses will be completed within 2 years after the licensee's submittals.

#### Future Plants

The staff has identified a number of Regulatory Guides and Standard Review Plan changes which should be made to address this issue for all future plants. Since no new applications are under review, this can be pursued as a separate effort.



ENCLOSURE 5

Enclosure

DRAFT GENERIC LETTER

TO: ALL HOLDERS OF OPERATING LICENSES

SUBJECT: RESOLUTION OF GENERIC ISSUE GI A-30 "ADEQUACY OF SAFETY-RELATED DC POWER SUPPLIES"

The NRC staff has completed the evaluation of Generic Issue A-30, which focuses on safety-related dc systems. Attachment 1 to this Generic Letter provides a brief description and history of this GI. Additional details are provided in the reference. As a result of its evaluation, the Staff concludes that certain maintenance, surveillance and monitoring provisions are appropriate for establishing the adequacy of safety-related dc systems. The Staff believes that most plants have already implemented a major portion of these provisions because of a number of actions taken by the Staff and industry. Details of these actions are provided in the reference.

In order to determine whether any further Staff actions are necessary to assure implementation of these recommended maintenance, surveillance and monitoring provisions at your plant, we request, pursuant to 10 CFR 50.54(f) and Section 182 of the Atomic Energy Act, that you provide the NRC with a response to the questions in the attachment within 180 days of the date of this letter. This information should be submitted to NRC, signed under oath and affirmation.

This request is covered by Office of Management and Budget Clearance Number 3150-0011, which expires December 31, 1989. The estimated average burden hours is 100 man-hours per licensee response, including assessment of the questions, searching data sources, gathering and analyzing the data, and preparing the required reports. Comments on the accuracy of this estimate and suggestions to reduce the burden may be directed to the Office of Management and Budget, Room 3208, New Executive Office Building, Washington, D.C. 20503, and to the U. S. Nuclear Regulatory Commission, Records and Reports Management Branch, Office of Administration and Resources Management, Washington, D. C. 20555

If you have any questions, please contact your project manager.

Sincerely,

Attachment: 10 CFR 50.54(f) Request - GI A-30 "Adequacy of Safety-Related dc Power."

Reference: EGG-NTA-8197, Revision 1, "Technical Findings for Generic Issue 128 (Issue A-30), "Adequacy of Safety Related DC Power Supplies"

## ATTACHMENT

### 10 CFR 50.54(f) REQUEST - GI A-30 "ADEQUACY OF SAFETY-RELATED DC POWER SUPPLIES"

#### Background

The specific area of concern of Generic Issue A-30 is the adequacy of the safety-related dc power in operating nuclear power plants, particularly with regard to multiple and common cause failures. Risk analysis and past plant experience support conclusions that failure of the dc power supplies could represent a significant contribution to the unreliability of shutdown cooling. Analysis indicates that inadequate maintenance and surveillance and failure to detect battery unavailability are the prime contributors to failure of the dc power systems.

During the development of plans to resolve Generic Issue A-30, it was observed that several previously issued notices, bulletins and letters submitted to licensees include recommendations similar to those that have been identified to resolve Issue A-30. More specifically, it has been determined that recommendations contained in notifications IEN 85-74, IEB 79-27, the Institute of Nuclear Power Operations' Significant Operating Experience Report (SOER) 83-5, and separate actions being taken to resolve Generic Issue 49 include the elements necessary to resolve Generic Issue A-30. It is therefore concluded that licensees that have adequately implemented these recommendations and actions will have resolved Generic Issue A-30.

The response to the questions that follow is necessary to provide the staff with information to determine whether any further action is required for your facility. If licensees have adequately addressed previous notifications, further action will not be necessary.

#### Questions

Licensees are requested to provide the following information for each unit at each site:

1. Unit \_\_\_\_\_
2. a. The number of independent redundant divisions of Class 1E or safety-related dc power for this plant is \_\_\_\_\_. (Include any separate Class 1E or safety related dc, such as any dc dedicated to the diesel generators.)  
b. The number of functional safety-related divisions of dc power necessary to attain safe shutdown for this unit is \_\_\_\_\_.
3. Does the control room at this unit have the following separate, independently annunciated alarms and indications for each division of dc power?
  - a. alarms
    1. Battery disconnect or circuit breaker open? \_\_\_\_\_

2. Battery charger disconnect or circuit breaker open (both input ac and output dc)? \_\_\_\_\_
3. dc system ground? \_\_\_\_\_
4. dc bus undervoltage? \_\_\_\_\_
5. dc bus overvoltage? \_\_\_\_\_
6. Battery charger failure? \_\_\_\_\_
7. Battery discharge? \_\_\_\_\_

b. Indications

1. Battery float charge current? \_\_\_\_\_
2. Battery circuit output current? \_\_\_\_\_
3. Battery discharge? \_\_\_\_\_
4. Bus voltage? \_\_\_\_\_

c. Does the unit have written procedures for response to the above alarms and indications? \_\_\_\_\_

4. Does this unit have indication of bypassed and inoperable status of circuit breakers or other devices that can be used to disconnect the battery charger from its ac power source during maintenance or testing?  
\_\_\_\_\_
5. If the answer to any part of question 3 or 4 is no, then provide information supporting the adequacy of the existing design features of the facility's safety-related dc systems.
6. a. (1) Have you conducted a review of maintenance and testing activities to minimize the potential for human error causing more than one dc division to be unavailable? \_\_\_\_\_ and (2) do plant procedures prohibit maintenance or testing on redundant dc divisions at the same time? \_\_\_\_\_
- b. Do maintenance and test procedures for this plant include provisions for rotation of qualified personnel and systematic verification of activities completed by other qualified personnel for maintenance and testing of the safety-related dc systems? \_\_\_\_\_
7. Are maintenance, surveillance and test procedures regarding station batteries conducted routinely at this plant? Specifically:
  - a. At least once per 7 days are the following verified to be within acceptable limits:

1. Pilot cell electrolyte level? \_\_\_\_\_
  2. Specific gravity or charging current? \_\_\_\_\_
  3. Float voltage? \_\_\_\_\_
  4. Total bus voltage on float charge? \_\_\_\_\_
  5. Physical condition of all cells? \_\_\_\_\_
- b. At least once per 92 days, or within 7 days after a battery discharge, overcharge, or if the pilot cell readings are outside the 7-day surveillance requirements are the following verified to be within acceptable limits:
1. Electrolyte level of each cell? \_\_\_\_\_
  2. The average specific gravity of all cells? \_\_\_\_\_
  3. The specific gravity of each cell? \_\_\_\_\_
  4. The average electrolyte temperature of a representative number of cells? \_\_\_\_\_
  5. The float voltage of each cell? \_\_\_\_\_
  6. Visually inspect or measure resistance of terminals and connectors (including the connectors at the dc bus)?  
\_\_\_\_\_
- c. At least every 18 months are the following verified:
1. Low resistance of each connection (by test)? \_\_\_\_\_
  2. Physical condition of the battery? \_\_\_\_\_
  3. Battery charger capability to deliver rated ampere output to the dc bus? \_\_\_\_\_
  4. The capability of the battery to deliver its design duty cycle to the dc bus? \_\_\_\_\_
  5. Each individual cell voltage is within acceptable limits during the service test? \_\_\_\_\_
- d. At least every 60 months, is capacity of each battery verified by performance of a discharge test? \_\_\_\_\_
- e. At least annually, is the battery capacity verified by performance discharge test, if the battery shows signs of degradation or has reached 85% of the expected service life? \_\_\_\_\_



8. If the answer to any part of question 6 or 7 is no, then provide your basis for not performing the maintenance, surveillance and test procedures described.
9. Does this plant have operational features such that following loss of one safety-related dc power supply or bus:
  - a. Capability is maintained for ensuring continued and adequate reactor cooling? \_\_\_\_\_
  - b. RCS integrity and isolation capability are maintained?  
\_\_\_\_\_
  - c. Operating procedures, instrumentation (including indicators and annunciators), and control functions are adequate to initiate systems as required to maintain adequate core cooling? \_\_\_\_\_

ENCLOSURE 6



**Idaho  
National  
Engineering  
Laboratory**

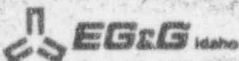
*Managed  
by the U.S.  
Department  
of Energy*

EGG-NTA-8197  
March 1989  
Revision 1

**TECHNICAL EVALUATION REPORT**

TECHNICAL FINDINGS FOR GENERIC ISSUE 128  
(ISSUE A-30) ADEQUACY OF SAFETY RELATED  
DC POWER SUPPLIES

R. O. Haroldsen  
Alan C. Udy



*Work performed under  
DOE Contract  
No. DE-AC07-76ID01570*

*Prepared for the  
U.S. NUCLEAR REGULATORY COMMISSION*

TECHNICAL FINDINGS  
GENERIC ISSUE 128 (ISSUE A-30)  
ADEQUACY OF SAFETY RELATED DC POWER SUPPLIES

R. O. Haroldsen  
Alan C. Udy

Published March 1989

Idaho National Engineering Laboratory  
EG&G Idaho, Inc.  
Idaho Falls, Idaho 83415

Prepared for the  
U.S. Nuclear Regulatory Commission  
Washington, DC 20555  
Under DOE Contract No. DE-AC07-76ID01570570  
FIN No. D6025

## ABSTRACT

This Idaho Nuclear Engineering Laboratory report provides the technical findings and conclusions for resolving Generic Issue A-30, "Adequacy of Safety Related DC Power Supplies."



## FOREWORD

This report is supplied as part of a program to resolve Generic Issue A-30, "Adequacy of Safety Related DC Power Supplies." This work is being conducted by EG&G Idaho, Inc., for the U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Research, Division of Engineering.

The NRC Task Manager for this project is D. F. Thatcher of the Engineering Issues Branch, Division of Safety Issues Resolution, Office of Nuclear Regulation Research.

The U.S. Nuclear Regulatory Commission funded this work under authorization B&R 9-60-19-50010, FIN No. D6025.

## CONTENTS

ABSTRACT .....	ii
FOREWORD .....	iii
1. INTRODUCTION .....	1
2. BACKGROUND .....	3
3. OTHER RELATED ISSUES .....	7
4. TECHNICAL FINDINGS .....	9
4.1 PREVIOUSLY PROPOSED RECOMMENDATIONS .....	9
4.2 OTHER RELATED ACTIONS .....	15
5. CONCLUSIONS .....	19
5.1 Estimated Cost .....	23
9. REFERENCES .....	23

## TABLES

1. CORRELATION OF GENERIC ISSUE A-30 RECOMMENDATIONS .....	20
APPENDIX 1, SURVEY OF PLANT TECHNICAL SPECIFICATIONS .....	25

TECHNICAL FINDINGS  
GENERIC ISSUE 128 (ISSUE A-30)  
ADEQUACY OF SAFETY RELATED DC POWER SUPPLIES

1. INTRODUCTION

A number of generic safety issues in the area of electric power systems have been identified over a period of years. These issues are listed and prioritized in NUREG-0933.<sup>1</sup> Three of these issues, because of their interrelationship, have been selected for integrated action. These are:

- |                    |  |
|--------------------|--|
| Generic Issue A-30 | "Adequacy of Safety-related DC Supplies"                         |
| Generic Issue 48   | "LCOs for Class 1E Vital Instrument Buses in Operating Reactors" |
| Generic Issue 49   | "Interlocks and LCOs for Redundant Class 1I Tie Breakers"        |

These three issues taken together are identified as Generic Issue 128. This report is a part of the action to resolve Generic Issue 128, but is specifically directed toward resolving Issue A-30.

The purpose of this report is to (1) provide background information, (2) state the recommendations that have been identified as sufficient to resolve this issue, (3) identify and correlate the elements of relevant past plant notifications with those identified in the recommendations, (4) document information as available, on actions that may have resolved part or all of the concerns of this issue on specific plants and (5) provide a recommended plan of action to close this issue.

It has been determined that some of the notifications previously submitted to plant owners regarding other concerns, contain elements of the recommendations identified for resolving Generic Issue A-30. Those

plants that have taken adequate action in response to these notifications may have resolved all or part of the relevant concerns. Most if not all plants that have adopted current standard technical specifications have met the recommendations regarding maintenance.

It is proposed that an information request be submitted to all licensees of operating plants to determine if the concerns of this issue have been addressed. The information obtained from this effort is expected to identify problem plants for which further action may be necessary.

## 2. BACKGROUND

This issue was first identified in April 1977, when a nuclear consultant questioned the Advisory Committee on Reactor Safeguards (ACRS) about the adequacy of the safety-related DC power systems.<sup>2</sup> The specific area of concern was the adequacy of the minimum design requirements for DC power systems, particularly with regard to multiple and common cause failures.

The NRC staff reviewed the adequacy of safety-related DC power supplies at operating nuclear power plants. Typical plants were reviewed for design, operating experience, and decay heat removal capability with respect to a DC power system failure. A preliminary assessment of accident scenario probabilities was made using data from WASH-1400.<sup>3</sup> The results of the initial staff assessment of the safety-significance of this issue were reported in NUREG-0305 in July 1977.<sup>4</sup>

NUREG-0305 recommended that a quantitative reliability assessment of the DC power systems be performed to identify and provide a basis for any changes in licensing criteria deemed necessary. Accordingly, a task action plan was developed. This task, identified as Generic Issue A-30, was chartered to determine the adequacy of the safety-related DC power system. The results of this study are documented in NUREG-0666.<sup>5</sup>

NUREG-0666 contains a probabilistic safety analysis of plant designs to assess the adequacy of the plant DC power system. The analysis utilized design information that conservatively enveloped the differences in plant design. It also utilized information from operational experience as reflected in Licensee Event Reports (LERs).

The supporting technical bases of NUREG-0666 included an analysis of the two-division DC power systems that evaluated the effectiveness of each proposed improvement in reducing the probability of the dominant DC power system failure modes. The analysis showed that there are two types of failures that dominate DC power system unreliability: common-cause failure of the batteries to provide sufficient power to the buses upon loss of AC



power to the battery chargers; and operational, test, or maintenance errors that cause the loss of both DC divisions (a bus tie may or may not be closed for this type of failure).

In the first failure mode, battery unavailability was dominated by inadequate maintenance practices and failure to detect and correct battery unavailability due to bus connection faults. In the second failure mode, most failures involved procedural errors either during periods when a tie breaker was closed or when both divisions were undergoing maintenance simultaneously (both compromise divisional independence).

The NUREG-0666 report concludes that failure of the minimum DC power system could represent a significant contribution to the unreliability of shutdown cooling. It also concludes that this contribution could be substantially reduced through the use of various design and operational improvements. Recommendations were made to augment both the minimum design criteria and procedural requirements.

Information taken from LER data indicates that there have been a substantial number of reportable events that involved the reliability of the safety-related DC systems. NUREG-0666 includes some statistics on events of this type that were listed in LERs prior to mid-1978. There are more than 1000 events listed. More than 100 events directly involved DC power and 87 events involved the batteries. Twelve of these events were identified as failure of a single DC bus. Twenty-four events were identified as battery charger failures. Four events were identified as possible battery common cause failures.

NUREG/CR-4470<sup>6</sup> contains a survey of events involving loss of vital AC instrument power through 1984. The vital instrument buses are normally powered by inverters from DC power. A total of 251 events were cataloged in the report of which more than 50 involved malfunctions of the DC power supply. Many of these events were caused by operator error or errors in maintenance procedures. Nine of these events caused operational transients.

There have been 3 events that merit special attention. These were:

1. An event at the Palisades power plant on January 6, 1981, caused by human error, resulted in the output breakers of both batteries being opened.

This event had limited consequence because the battery charger remained available to supply the DC power requirements. It is significant because power from both batteries was lost simultaneously.

2. An event at Millstone Unit 2 on January 2, 1981,<sup>7</sup> caused by operator error, resulted in the loss of one of the two redundant independent DC buses.

This event precipitated a variety of consequences, including a loss of operability of important switching equipment and annunciators. The event was made more complicated by the failure of an emergency diesel generator nine minutes into the event.

3. An event at Zion Unit 2 on September 19, 1976,<sup>7,8</sup> caused by a switching error resulted in the loss of one of the safety-related DC buses.

In this event, the loss of the DC bus was the start of a series of events that caused the reactor to trip without the usual annunciation. The reactor trip was followed by actuation of the emergency safeguards equipment and a fire that severely damaged one of the emergency diesel generators. The event left the plant in a natural circulation mode of operation. Although this event happened many years ago, it continues to be a valuable source of information relevant to Generic Issue A-30. It demonstrated that some operating reactor facilities may not provide sufficient operational information on the status of the safety-related DC system in the control room. It also suggested that more attention should be given to the design and review of the annunciator system in nuclear power plants.

The event at Zion Unit 2 resulted in a proposed multi-unit action to require licensees of operating reactors to review their design and to propose revisions, as necessary, to ensure that:

1. The plant annunciators and monitoring systems pertaining to the status of all DC buses in the plant are available to the control room operator at all times.
2. The plant bypass indication system include indication of the position of the station battery output breaker or fused disconnect switches (if provided) and the charger input and output breakers.

This multi-unit action was not implemented. Instead it was held in abeyance because of the direct relationship to the A-30 issue. For the purposes of this report, the recommendations of the proposed multi-unit action is considered to be a part of the A-30 generic issue.

### 3. OTHER RELATED ISSUES

Generic Issue A-30 is interrelated with several other generic issues. These include:

1. A-17 -- Systems Interactions
2. A-25 -- Non-safety Loads on Class 1E Power Source
3. A-44 -- Station Blackout
4. A-45 -- Decay Heat Removal
5. A-47 -- Safety Implications of Control Systems
6. GI-46 Loss of 125 Volt DC Bus
7. GI-48 -- LCOs for Class 1E Vital Instrument Buses in Operating Reactors
8. GI-49 -- Interlocks and LCOs for Redundant Class 1E Tie Breakers
9. GI-76 -- Instrumentation and Control Power Interactions

The first six issues are affected by, or involve, the loss of DC power in which operation of some systems (or several different systems) could be unavailable, such as: Control room annunciators and indicators, turbine-driven auxiliary feedpumps, reactor core isolation cooling pumps, and high pressure safety injection pumps, diesel-generator start valves and control power, vital instrument power, main generator stop valves, turbine trip and switchyard circuit breakers.

The guidelines for station blackout (A-44) include a plant requirement for a coping duration to be defined by the availability of alternate AC power. During the coping period, the plant is dependent on battery power to

achieve and maintain safe shutdown. This requirement places additional dependence on the capacity and reliability of the plant DC systems.

Generic Issue A-30 involves the power source to the inverters for the vital 120 VAC instrument power supplies which are related to Generic Issues 48 and 49. The NUREG-0666 recommendation prohibiting bus tie breakers that could compromise division independence is also related to A-30 and GI-49. This concern is expected to be resolved by actions pending on GI-49. In addition, A-30 is related to GI-76, because a loss of 120 VAC vital instrument power could challenge emergency safeguards systems. Loss of the vital instrument power could cause, for example, reactor trips, loss of feedwater, loss of emergency core and containment cooling systems and the loss of the post-accident monitoring instrumentation necessary for the operator to assess unit conditions.

In addition to the related generic issues listed above, there are ongoing investigations directed toward extending the life of batteries, battery chargers and other components. A description of some of this effort is reported in NUREG/CR 4457<sup>9</sup>, NUREG/CR 4564<sup>10</sup> and NUREG/CR 5051<sup>11</sup>. These investigations provide useful information on methods that may extend the life of batteries and battery chargers. They have no direct impact upon the proposed action to resolve generic issue A-30 because this issue is specifically directed toward assuring the availability of DC power and does not extend into the area of aging of components.



## 4. TECHNICAL FINDINGS

### 4.1 PREVIOUSLY PROPOSED RECOMMENDATIONS

The NRC has considered resolving this issue in various ways, including implementing a Branch Technical Position, revising the Standard Review Plan, and issuing a generic letter or an information notice. Among these alternatives was a Branch Technical Position proposed by the Power System Branch which provided a set of guidelines applicable to all Class IE DC power supplies, based on the recommendations of NUREG-0666. These guidelines have been identified by the staff as sufficient to resolve the concern of Generic Issue A-30. They are used in current licensing practice and provide the basis for relevant sections of the current Standard Technical Specifications. These guidelines are summarized as follows:

1. Where electrical interconnections between redundant divisions of the safety-related DC power systems are provided, the following practices will reduce the potential common cause failure of the DC power systems to a relatively low level.
  - a. Interconnections, where allowed, must be made by manual means and only with strict administrative controls.
  - b. The use of any tie breaker interconnection of redundant divisions should be restricted to cold shutdown or refueling modes of operation by use of strict administrative controls.
  - c. Interconnections should be designed and implemented such that single failure or inadvertent closure of interconnecting devices does not compromise division independence.
  - d. Surveillance requirements and limiting conditions of operation should be provided in the technical specifications for the use of interconnections, including interconnections between safety-related DC power systems for multi-unit stations.

2. The following control room indications for safety-related DC power systems are important and effective in enhancing the reliability of the DC power systems.
  - a. A battery trouble alarm in the control room that monitors the following abnormal conditions is important and effective in enhancing the reliability of the DC power systems.
    - (1) Battery disconnect or circuit breaker open
    - (2) Battery charger disconnect or circuit breaker open (both input AC and output DC)
    - (3) DC system ground
    - (4) DC bus undervoltage
    - (5) DC bus overvoltage
    - (6) Battery charger failure
    - (7) Battery discharge
  - b. Battery float charge current
  - c. Battery circuit output current
  - d. Battery charger output current

Additional alarms and indications may also be incorporated and the failure of one DC division should not cause a total loss of the control room annunciator system.

3. Bypassed and inoperable status indication should be provided for circuit breakers or other devices that can be used to disconnect

the battery or the battery charger from its DC bus or the battery charger from its AC power source during maintenance or testing.

4. The following practices will reduce the likelihood of accidental degradation of safety-related DC systems and associated distribution systems:
  - a. Performance of an independent review of all maintenance procedures and testing activities to help minimize the potential for human error causing more than one DC division to be unavailable. Procedures should prevent maintenance or testing activities from occurring on redundant DC divisions at the same time.
  - b. Adherence to adequately written procedures and administrative controls for maintenance, testing, and operational activities. Procedures should include a provision for the rotation of qualified personnel and the systematic verification of activity completion by other qualified personnel.
  
5. The following surveillance and maintenance activities provide assurance that the DC power system operates with high reliability.
  - a. At least once per 7 days, verification of the pilot cell electrolyte level, the specific gravity (or charging current) and float voltage, the total bus voltage on float charge, and the physical conditions of all cells.
  - b. At least once per 92 days, or within 7 days after a battery discharge, overcharge, or if the pilot cell readings are outside of 7-day surveillance requirements, verification of the electrolyte level of each cell, the average specific gravity of all cells, the specific gravity of each cell, the average electrolyte temperature of a representative number of cells, the float voltage of each cell, and the visual

inspection (or measured resistance of) terminals and connectors (including connectors at the DC bus).

- c. At least once per 18 months, verification of low resistance of each connection, the physical condition of the battery, each battery charger's capability to deliver rated ampere output to the DC bus, the capability of the battery to deliver its design duty cycle to the DC bus (service test), and each individual cell voltage during the service test.

Resistance measurements must be taken consistently and with an instrument of sufficient accuracy and resolution to measure resistance changes in the micro-ohm range.

Individual cell voltage readings should be taken between respective posts of like polarity of adjacent cells, so as to include the voltage drop of the intercell connections.

- d. At least once per 60 months, verification of the capacity of each battery by a performance discharge test. If the battery shows signs of degradation or has reached 85% of the service life expected for the application, verify the capacity annually by a performance discharge test. Degradation is indicated when the battery capacity drops more than 10% of its rated capacity from its average on previous performance tests, or is below 90% of the manufacturer's rating.
6. Plant design and operational features should be such that following the loss of one DC power supply or bus: (a) redundant capability is maintained for ensuring continued and adequate reactor core cooling; (b) RCS integrity and isolation capability are maintained; and (c) operating procedures, instrumentation, and control functions are adequate to initiate systems as required to maintain adequate core cooling. In essence, reactor core cooling capability should be maintained regardless of reactor trip

following the loss of any one DC power supply or bus and a single independent active failure in any other system required for shutdown cooling.

#### Discussion of Recommendations

The proposed power systems branch technical position stated that the following considerations and assumptions should be used to determine the adequacy of the design and operational features:

- a. DC power bus losses ranging from momentary to several hours duration should be considered. The length of the DC power bus outage should be the result of a comprehensive failure modes and effects analysis (FMEA) that has been performed. The FMEA should use reasonable assumptions, including credible failures (human and hardware related) and an evaluation of the repair actions and time necessary to complete restoration. An equivalent evaluation could be used instead.
- b. The transient conditions and interactions caused by the DC power bus loss and individual single failures, which may affect the ability to maintain adequate reactor core cooling, should be considered.
- c. Systems and components which become unavailable, or attain an undesired operating state due to the DC power bus loss, should be considered unavailable and should not be considered as single independent failures.
- d. Single failures affecting the availability of DC power supplies in addition to the initial DC power bus loss need not be considered for those DC power systems or subsystems in which the requirements of Recommendations 1, 4, and 5 above have been satisfied.



- e. Systems and components available to accomplish shutdown cooling should be (1) safety grade, or (2) used regularly during plant operation, or (3) subject to routine operability checks.
- f. Single failure should be interpreted to mean single active failures, except where further clarification is provided in a through e above.

#### 4.2 Other Related Actions

This section provides information on other independent actions and recommendations by the NRC and other organizations that may contribute to the resolution of Generic Issue A-30.

##### Standard Technical Specifications

Essentially all of the A-30 recommendations relating to maintenance and surveillance are included in the current standard technical specifications.<sup>12</sup> Recently licensed plants and some older plants have incorporated the relevant provisions into their plant technical specification. A survey of plant specific technical specifications was conducted by the staff in March 1987 to identify as far as possible (from available staff records) which plants have adopted the relevant provisions. The results of the survey are summarized in the appendix of this report.

##### Generic Issue 49

Action to resolve Generic Issue 49, "Interlocks and LCOs for Class 1E Tie Breakers," will be taken as part of the Integrated Generic Issue 128. The actions proposed will:

1. Restrict the closure of any bus tie breakers (between redundant division of AC or DC power and between units at the same site) to periods when the reactor is shutdown.
2. Ensure that provisions in the plant technical specifications prohibit plant startup unless all tie breakers are open.

The proposed plan for resolving Generic Issue 49 will accomplish all the actions in A-30 Recommendation Number 1 (listed in Section 4.1). It should be noted, however, that complete protection from compromising division independence by a single failure or inadvertent closure of a single tie breaker can only be obtained by racking out and physically removing the tie breaker. Therefore, current licensing practice discourages the use of tie breakers between independent division of power and requires redundant tie breakers when used.

#### Significant Operating Experience Report 83-5

The Institute of Nuclear Power Operations (INPO) issued Significant Operating Experience Report (SOER) 83-5<sup>13</sup> on May 27, 1983. This report, titled "DC Power System Failures," had eight recommendations concerning hardware, procedures, maintenance and training.

The hardware recommended includes: (1) alarms for DC bus under/over voltage, DC system ground fault, battery charger trouble and battery and battery charger input and output breaker position, and (2) battery capacity (ampere hour) monitor. The report recommended a review or test of plant behavior on loss of each vital DC bus. Should significant transients be possible, design and procedural changes were recommended to ensure that the transients were manageable. The report also recommended an evaluation of procedural requirements for specific gravity measurements and a review to determine that components supplied power from the Class 1E DC power system are not subjected to more than their design rated voltage, especially when performing an equalizing charge.

Procedural changes were also recommended as necessary to: (a) prevent the simultaneous maintenance of redundant DC divisions, (b) control the operation of tie breakers between redundant divisions or between units of multi-unit stations, (c) prevent the simultaneous testing of redundant DC divisions where the reliability of the DC system would be increased by testing each division separately, (d) monitor battery capacity when chargers are not in service, (e) clearly and correctly specify the transfer between float and equalizing charge, (f) clearly and correctly specify, if

permitted, the crosstying between electrical divisions and between units of multi-unit stations, (g) clearly and correctly specify the transfer between normal and standby battery chargers, and (h) ensure that procedures address initial and follow-up actions for the loss of any vital DC bus.

The report also recommends preventive maintenance procedures to ensure clean battery cell terminals, cell interconnections and bus connections, and routine battery cell case inspections. Operator training for DC power system operation, plant response to loss of Class 1E DC power and proper switching operation was also recommended.

The SOER 83-5 report was submitted to each INPO affiliated station. Depending on the licensee's response to the INPO recommendations, several of the A-30 recommendations may have been implemented. The INPO report adequately addresses the following A-30 recommendations (identified in Section 4 of this report): 1.d (including multi-unit stations), 2.a, 2.b, c & d (provided by battery capacity monitors instead of current meters), 4.a, and specific gravity and physical conditions of 5.a & b. It also would have licensees study plant behavior following the loss of DC power, partially satisfying Recommendation 6.

#### IE Information Notice No. 85-74

The NRC issued IE Information Notice 85-74, "Station Battery Problems," on August 29, 1985. It recommended the use of Regulatory Guide 1.129, Revision 1, and IEEE Standards 450-1975 and 1980 for guidance in the maintenance of station batteries. This information notice, if heeded by licensees, would provide the testing identified in Recommendation Number 5 (Section 4.1).

#### IE Bulletin No. 79-27

The NRC issued IE Bulletin No. 79-27, "Loss of Non-Class 1E Instrumentation and Control Power System Bus During Operation," on November 30, 1979. One of the requirements of this bulletin is the preparation or review of emergency procedures to be used by control room

operators to achieve cold shutdowns upon loss of any Class 1E or non-Class 1E bus supplying power to safety and non-safety related instrument and control systems. Implementation of the requirements of this bulletin should have verified the existence of the emergency procedures recommended by Recommendation Number 6C.

#### IEEE Standard 603-1980

IEEE Standard 603-1980, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,"<sup>14</sup> is endorsed with certain exceptions by Regulatory Guide 1.153.<sup>15</sup> This Regulatory Guide is effective for construction permits issued after November 1985. Section 5.8.3, "Indication of Bypasses," states that if the protective actions of a part of a safety system has been bypassed or rendered inoperative, a continuous indication of this fact should be provided in the control room. It should be automatically actuated if the bypass or inoperative conditions occurs more than once per year and is expected to occur when the affected system is required to be operable. This means that if a circuit breaker or fused disconnect is operated so that a DC bus is disconnected from its battery or battery charger, or if the battery charger is disconnected from its AC power source, this condition should be automatically indicated in the control room as an operating bypass.

While these requirements do not extend directly to all currently licensed plants, earlier less specific but similar requirements endorsed by the NRC are stated in IEEE Standards 279<sup>16</sup> and 308.<sup>17</sup> These requirements meet some of the actions stated in Recommendations 2 and 3 (Section 4.1).

#### A-30 Recommendations Not Addressed in Previous Notifications to Licensees

In this review we have found that almost all of the proposed recommendations for resolving Generic Issue A-30 are included in notices, bulletins and letters that have been previously submitted to all licensees. Two possible exceptions are included in Recommendations Numbers 4b and 6a (Section 4.1).

The first of these would require procedures that assure that maintenance and tests are performed properly by rotation of qualified personnel and by systematic verification of work by separate independent qualified personnel. This requirement could introduce new human factor related risks by having excess personnel in the battery rooms and by increasing the possibility that work may be conducted on redundant systems at the same time. We view this as a matter of competing risks. The rotation of personnel and verification of work would help reduce the possibility of common-cause human-error. However, with extra workmen in a somewhat small area, each with tools and ability, there is an additional potential for accidental degradation of the DC power system. Therefore, we find that this recommendation could be dropped.

The second item (6a) depending on interpretation could require 3 independent divisions of DC power. Some older plants currently have only 2 divisions.

General Design Criteria (GDC) 34 (Residual Heat Removal)<sup>18</sup> and 35 (Emergency Core Cooling)<sup>19</sup> require redundancy such that system functions can be accomplished assuming a single failure and that either the offsite electric power system or the onsite electric power system is not available. GDC 17<sup>20</sup> lists the criteria for electric power systems. The batteries are considered to be part of the onsite electric power supplies. Recommendation 6a implies an added requirement for maintaining all redundant DC powered functions operational following loss of a DC power bus. This may be a stringent requirement that cannot be met by some existing plants. Item d in the guidelines (Section 4.1) states that single failures affecting the availability of DC power supplies in addition to the initial loss of the DC power bus, need not be considered for those DC power systems or subsystem in which Recommendations Numbers 1, 4 and 5 have been satisfied.



## 5. CONCLUSIONS

From our review of Generic Issue A-30, we conclude that the action recommended by NUREG-0666, and further developed by the Power System Branch remains valid. These recommendations are reasonably well reflected in current versions of Standard Technical Specifications.<sup>12</sup> Plant responses to NRC Information Notice 85-74, "Station Battery Problems," August 29, 1985 may have brought about voluntary implementation of some of the recommended provisions of NUREG-0666 in some older plants. Other relevant independent recommendations have been submitted to plant owners by the Institute of Nuclear Power Operation. These also may have encouraged some plants to implement some of the recommendations of NUREG-0666.

It has been determined that most, if not all, of the elements of the recommendations identified to resolve this issue have been included in the various past notifications submitted to licensees. Those plants that have taken adequate action in response to these notifications may have resolved all of the concerns of the issue. A correlation between the recommendations included in the past notifications and the A-30 recommendations are summarized in Table 1.

The adequacy of implementation of these recommendations is unknown except in recently licensed plants or as reflected in plant specific technical specifications. We therefore, conclude that the adequacy of implementation of the recommendations can best be verified through a information request directed to all plant licensees. The results of this survey will provide the basis for any further actions and identify specific plants that may require further action.

TABLE 1. CORRELATION OF GENERIC ISSUE A-30 RECOMMENDATIONS

<u>A-30 Recommendations</u>	<u>Standard Tech Specs</u>	<u>GI-49</u>	<u>SOER 83-5</u>	<u>IEN 85-74</u>	<u>IEB 79-27</u>
1. Inter Division Ties					
(a) Operated manually under administrative control	x	x	x		
(b) Operation restricted to shutdown/fuel handling	x	x			
(c) Prevent single failure or inadvertent closure from compromising Division independence		x			
(d) Tech Specs for LCOs and Surveillance	x	x	x		
2. Alarms and Monitors					
(a) Alarms					
(1) Battery disconnect			x		
(2) Charger disconnect			x		
(3) DC ground			x		
(4) DC undervoltage			x		
(5) DC overvoltage			x		
(6) Charger failure			x		
(7) Battery discharge			x		
(b) Battery Float Charge Current			x		
(c) Battery Circuit Output			x		
(d) Charge Output Current			x		
3. Charger and Battery Input Disconnect Indication During Maintenance	See note below				

Note: IEEE Standard 279 (Section 4.1.3) states that if the protective actions of some part of the safety system have been bypassed or deliberately rendered inoperative for any purpose, this fact shall be continuously indicated in the Control room. This requirement is more precisely stated in IEEE Standard 603 Section 5.8.3.

TABLE 1. CORRELATION OF GENERIC ISSUE A-30 RECOMMENDATIONS

A-30 RECOMMENDATIONS	Standard Tech Specs	GI-49	SOER 83-5	IEN 85-74	IEB 79-27
4. Procedures and Administrative Controls					
(a) Independent maintenance and testing of redundant DC divisions			x		
(b) Procedures to ensure maintenance and testing is done correctly			Note: See Section 4.2 for discussion of this item.		
5. Surveillance and Testing					
(a) Weekly	x		x	x	
(b) Quarterly	x		x	x	
(c) 18 Months	x			x	
(d) 60 Months	x			x	
6. Design and Operational Features Following Loss of One DC Supply					
(a) Redundant capability for core cooling			Note: See Section 4.2 for discussion of this item		x (no redundancy requirement)
(b) RCS integrity and isolation capability maintained					x
(c) Procedures, instruments and control functions adequate for core cooling					x
Note: SOER 83-5 recommended review of the items in item 6.					

### 5.1 Estimated Cost

The licensee cost is dependent on the time requirement to collect and document the requested information. This effort is estimated to average 100 man-hours which based on \$50 per hour would result in a cost to the licensee of \$5000.

NRC resources is estimated to require 2 man-weeks to review the justification provided by each plant which does not respond with affirmative verification. If 50 plants are found to be in this category, 100 man-weeks would be required.

## 6. REFERENCES

1. NUREG-0933, A Prioritization of Generic Safety Issues, Revision 5, March 1987.
2. NRC Memorandum, R. F. Fraley to E. G. Case, "Reliability of Power Supplies" (Attachment B in Reference 4).
3. NRC Report WASH-1400, NUREG-75/014 "Reactor Safety Study," NTIS, October 1975.
4. NUREG-0305, "Technical Report on DC Power Supplies in Nuclear Power Plants," Office of Nuclear Reactor Regulation, July 1977.
5. NUREG-066F, "A Probabilistic Safety Analysis of DC Power Supply Requirements for Nuclear Power Plants," Office of Nuclear Regulatory Research, April 1981.
6. NUREG/CR-4470, "Survey and Evaluation of Vital Instrumentation and Control Power Supply Events," Oak Ridge National Laboratory, August 1986.
7. NSAC/48, EPRI Report, "Workshop on Vital DC Power," May 1982.
8. NRC Memorandum, D. G. Eisenhut to K. G. Goller, "Zion Station, Unit 2, Loss of Annunciators Due to Loss of 125-Volt DC Bus Voltage (TAC No. 6464)," July 13, 1977.
9. NUREG/CR-4457, "Aging of Class 1E Batteries in Safety Related Systems of Nuclear Power Plants", July 1987.
10. NUREG/CR-4564, "Operating Experience and Aging-Seismic Assessment of Battery Chargers and Inverters", June 1986.
11. NUREG/CR-5051, "Detecting and Mitigating Battery Charger and Inverter Aging", August 1988.
12. Standard Technical Specifications, Westinghouse, NUREG-0452, Revision 4; B&W, NUREG-0103, Revision 4; Combustion Engineering, NUREG-0212, Revision 3; General Electric, NUREG-0123, Revision 3.
13. INPO SOER 83-5, "DC Power System Failures," May 27, 1983. (Note: This document is not publically available.)
14. IEEE Standard 603-1980, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," IEEE Power Engineering Society, 1980.
15. Regulatory Guide 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems," Office of Nuclear Regulatory Research, NRC, December 1985.
16. IEEE Standard 279-1971, "IEEE Standard Criteria for Protection Systems for Nuclear Power Generating Stations."



17. IEEE Standard 308-1974, "IEEE Standard Criteria for Class IE Power System for Nuclear Power Generating Stations."
18. General Design Criterion 34, "Residual Heat Removal," of Appendix A, "General Design Criteria for Nuclear Power Plants," of 10 CFR 50.
19. General Design Criterion 35, "Emergency Core Cooling," of Appendix A, "General Design Criteria for Nuclear Power Plants," of 10 CFR 50.
20. General Design Criterion 17, "Electrical Power Systems," of Appendix A, "General Design Criteria for Nuclear Power Plants," of 10 CFR 50.

APPENDIX  
 TABLE 2. SURVEY OF PLANT TECHNICAL SPECIFICATIONS

<u>Plant</u>	<u>DC System Surveillance</u>				<u>Tie Breaker LCOs</u>		<u>No Info</u>	<u>Notes</u>
	<u>SIS</u>	<u>Alt</u>	<u>Min</u>	<u>None</u>	<u>AC</u>	<u>DC</u>		
ANO-1			x				x	
ANO-2	x				x			AC only
Arnold			x				x	
Beaver Valley	x						x	
Davis Besse	x				x			AC only
Braidwood 1 & 2	x						x	
Browns Ferry 1			x				x	
Browns Ferry 2			x				x	
Browns Ferry 3			x				x	
Brunswick 1	x*				x	x		*no R check
Brunswick 2	x*				x	x		*no R check
Byron 1 & 2	x						x	
Crystal River 3		x					x	
Diablo Canyon 1 & 2	x						x	
Callaway 1	x				x	x		
Calvert Cliffs 1		x			x			AC only
Calvert Cliffs 2		x			x			AC only
Catawba 1 & 2	x				x			AC only
Clinton 1	x						x	
Comanche Peak 1 & 2	x						x	No tie breakers
D. C. Cook 1 & 2		x			x	x		
Cooper 1		x					x	
Dresden 2 & 3			x				x	

APPENDIX  
TABLE 2. (Continued)

<u>Plant</u>	<u>DC System Surveillance</u>				<u>Tie Breaker LCOs</u>		<u>No Info</u>	<u>Notes</u>
	<u>STS</u>	<u>Alt</u>	<u>Min</u>	<u>None</u>	<u>AC</u>	<u>DC</u>		
Farley 1	x						x	
Farley 2	x						x	
Fermi 2	x				x	x		
Fitzpatrick 1			x				x	
Ft Calhoun			x				x	
Ft. St Vrain				x			x	
Ginna			x				x	
Grand Gulf 1	x						x	
Haddam Neck				x			x	
S. Harris	x				x	x		
Hatch 1 <sup>™</sup>			x				x	
Hatch 2		x			x	x		
Hope Creek	x						x	
Indian Point 2			x				x	
Indian Point 3			x				x	
Kewaunee			x				x	
La Salle 1 & 2	x						x	
La Crosse		x			x	x		
Limerick 1 & 2	x						x	
Maine Yankee			x				x	
McGuire 1 & 2	x				x		AC only	
Millstone 1			x				x	
Millstone 2		x			x	x		

APPENDIX  
TABLE 2. (Continued)

<u>Plant</u>	<u>DC System Surveillance</u>				<u>Tie Breaker LCOs</u>		<u>No Info</u>	<u>Notes</u>
	<u>STS</u>	<u>Alt</u>	<u>Min</u>	<u>None</u>	<u>AC</u>	<u>DC</u>		
Millstone 3	x						x	
Monticello			x				x	
Nine Mile Point 1			x				x	
Nine Mile Point 2	x				x	x		
North Anna 1 & 2		x			x	x		
Oconee 1, 2 & 3		x					x	
Oyster Creek			x				x*	*Insufficient info. Some tie breaker restrictions.
Palisades			x				x	
Palo Verde 1, 2, 3	x				x	x		
Peach Bottom 2 & 3			x				x	
Perry 1 & 2	x						x	
Pilgrim			x				x	
Point Beach 1 & 2			x				x	
Prairie Island 1 & 2			x				x	
Quad Cities 1 & 2			x				x	
Rancho Seco			x				x	
River Bend	x						x	
Big Rock Point 1			x				x	
Robinson			x				x	
Salem		x					x	
San Onofre 1, 2, 3	x						x	

APPENDIX  
TABLE 2. (Continued)

<u>Plant</u>	<u>DC System Surveillance</u>				<u>Tie Breaker LCOs</u>		<u>No Info</u>	<u>Notes</u>
	<u>STS</u>	<u>Alt</u>	<u>Min</u>	<u>None</u>	<u>AC</u>	<u>DC</u>		
Seabrook	x						x	
Shoreham	x				x	x		
South Texas	x						x	
St. Lucie 1	x						x	
St. Lucie 2	x				x	x		
Summer	x				x	x		
Surrey 1 & 2		x					x	
Susquehanna 1 & 2	x				x	x		
TMI-1			x				x	
Trojan		x			x	AC only		
Turkey Point 3 & 4			x				x	
Vermont Yankee		x					x	
Vogtle 1 & 2	x				x	x		
Waterford 3	x						x	
Watts Bar 1	x				x	x		
WNP 2	x				x	x		
Wolf Creek 1	x				x	x		
Yankee Rowe		x			x	x		
Zion 1 & 2		x					x	

LCO - Limiting condition of operation.

STS - Standard Technical Specification

ALT - Alternate

MIN - Minimal Requirements



APPENDIX  
TABLE 2. (Continued)

---

Note 1: DC Bus Surveillance

Of the 113 plant technical specification surveyed, 54 include surveillance requirements that are essentially the same as are included in the Standard Technical Specifications. Thirty-five plants have alternate (always less rigorous) requirements. Several of these are GE plants with substantially different configurations which include MG sets. Twenty-Two plants have surveillance requirements which are substantially less rigorous than are required by the Standard Technical Specifications. Only 2 plants have technical specifications (Ft. St. Vrain and Haddam Neck) that do not have any surveillance requirements on their DC buses.

Note 2: Tie Breakers LCOs

Of the 113 plant technical specifications surveyed, 77 have no stated restrictions on plant operations with tie breakers closed. Some of these plants are known to not have tie breakers (Comanche Peak). Thirty-six plants do have LCO restrictions on operation with the AC breakers closed. Of these, 27 also have restrictions on operations with DC tie breakers closed. Some plants operate with closed DC tie breakers during periods of equalizer charger.

---

NRC FORM 325 (2-84) NRCM 1102 100-1002		U.S. NUCLEAR REGULATORY COMMISSION		1. REPORT NUMBER (Assigned by TIIC add vol. no. if any)	
<b>BIBLIOGRAPHIC DATA SHEET</b>				EGG-NTA-8197 Revision 1	
2. TITLE AND SUBTITLE TECHNICAL FINDINGS FOR GENERIC ISSUE 128 (ISSUE A-30) ADEQUACY OF SAFETY-RELATED DC POWER SUPPLIES				3. LEAVE BLANK	
5. AUTHOR(S) R. O. Haroldsen Alan C. Udy				4. DATE REPORT COMPLETED MONTH: March      YEAR: 1989	
7. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code) EG&G Idaho, Inc. P. O. Box 1625 Idaho Falls, ID 83415				6. DATE REPORT ISSUED MONTH: March      YEAR: 1989	
10. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code) Division of Engineering Office of Nuclear Regulatory Research U.S. Nuclear Regulatory Commission Washington, DC 20555				8. PROJECT/TASK/WORK UNIT NUMBER	
12. SUPPLEMENTARY NOTES				9. PIN OR GRANT NUMBER  D6025	
11. TYPE OF REPORT Technical Evaluation Report				10. PERIOD COVERED (inclusive dates)	
13. ABSTRACT (200 words or less)  This EG&G Idaho, Inc. Idaho National Engineering Laboratory report provides the technical findings for a proposed integrated resolution of Generic Issue 128, (Issue A-30), Adequacy of Safety-Related DC Power Supplies.					
14. DOCUMENT ANALYSIS - KEYWORDS/DESCRIPTORS				15. AVAILABILITY STATEMENT Unlimited Distribution	
16. IDENTIFIERS/OPEN ENDED TERMS				18. SECURITY CLASSIFICATION This report: Unclassified This report: Unclassified	
				17. NUMBER OF PAGES	
				18. PRICE	

3701



UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
WASHINGTON, D. C. 20555

APR 8 1989

MEMORANDUM FOR: Edward Jordan, Chairman  
Committee to Review Generic Requirements

FROM: Eric S. Beckjord, Director  
Office of Nuclear Regulatory Research

SUBJECT: FINAL RESOLUTION OF USI A-47 "SAFETY IMPLICATIONS OF  
CONTROL SYSTEMS IN LWR NUCLEAR POWER PLANTS"

The staff has completed its resolution of Unresolved Safety Issue A-47, "Safety Implications of Control Systems in LWR Nuclear Power Plants." Results of the staff evaluation and the proposed implementation are presented in the enclosed documents.

The draft staff NUREG reports (NUREG 1217 and 1218) which included the proposed resolution received CRGR concurrence on May 10, 1988, and were issued for public comment on May 27, 1988. The enclosed documents represent the final resolution of this issue and includes the staff discussion of the public comments that were received. The changes to the NUREG reports and to the generic letter are editorial in nature and are intended to clarify the staff requirements.

The public comments and the staff's responses are documented in Appendix C to NUREG-1217. Difference of opinion between the NRC staff and two industry commenters remain, and are highlighted here for your information:

- (1) Duke Power Company believes that the requirement to include provisions in the Technical Specifications for periodic verification for the steam generator overflow protection system is not consistent with NRC policy statement on the content of the technical specifications. The staff however maintains that this requirement is compatible with the new technical specification policy. (See comment 31 in Appendix C.)
- (2) Baltimore Gas and Electric Company (Calvert Cliffs Plant) believes that our cost estimates for overflow protection for their plant is low by a factor of 2, and therefore they conclude that the stated design modifications to provide steam generator overflow protection are not cost effective. Although the staff agrees that the actual costs may be closer to the Calvert Cliff estimates, the sensitivity study provided in Appendix B of NUREG 1218 indicates that the cost benefit for the modifications requested are still justified. (See comment 15 of Appendix C to NUREG-1217.)

9004120026

APR 3 1989

The safety issue in USI A-47 is the concern that, in LWR nuclear power plants, there may be failures initiated or aggravated by non-safety related control systems that could lead to plant upsets or events that significantly impact the health and safety of the public.

To address this safety concern an evaluation was performed on non-safety related control systems that are typically used during normal plant operation. Four nuclear steam system (NSS) plants were evaluated, a General Electric Company designed BWR, a 3-loop Westinghouse Company PWR design, a once-through steam generator PWR designed by Babcock and Wilcox Company, and a Combustion Engineering PWR design. Tasks were established to identify control systems whose failure could (1) cause transients or accidents to be potentially more severe than previously analyzed, (2) adversely affect any assumed or anticipated operator action during the course of transients or accidents, (3) cause technical specification safety limits to be exceeded, or (4) cause transients or accidents to occur at a frequency in excess of those established for abnormal operational transients and design basis accidents. A study was also conducted to determine the generic applicability of the results of the specific plants analyzed to each class of plants.

A set of limitations and assumptions was developed to confine the USI A-47 investigation to a manageable scope and to focus attention on the more safety significant potential control system failures. The limitations and assumptions are itemized below:

- (1) A minimum number of safety-related protection systems would be available to trip the reactor and initiate overpressure protection systems or emergency core cooling (ECC) systems, if needed, during transients initiated by failures in the control systems.
- (2) Control system failures resulting from common cause events such as earthquakes, floods, fires, and sabotage, or operator errors of omission or commission are not addressed in this review. A study of selected multiple control system failures in non-safety related equipment was, however, performed to evaluate some effects of common mode failures.
- (3) Transients resulting from control system failures during limited conditions of operation (LCOs) or anticipated transient without scram (ATWS) events are not addressed in this review.
- (4) The plant-specific designs were assumed to have been appropriately modified to comply with the requirements of IE Bulletin 79-27 and NUREG-0737.

The A-47 program has addressed the safety implications of non-safety related control systems with a number of different approaches. One approach utilized failure mode and effects analysis to identify control system failures that could potentially impact plant safety. Another approach utilized thermal

APR 3 1989

hydraulic analyses to evaluate plant transients resulting from single and multiple non-safety related control system failures. Another approach was the evaluation of operating experience on control system failures reported by the utilities. On the basis of the findings identified during this review, a number of alternatives for possible regulatory action were evaluated. The selection of the resolution is based on consideration of the safety benefits derived from these alternatives in terms of risk reduction and the cost of implementation. The regulatory analysis of the alternatives considered is presented in NUREG-1218 .

The staff has concluded that certain non-safety related control systems and the technical specifications for selected systems should be upgraded. In addition, selected emergency procedures should be reevaluated and modified, if necessary, to assure that plant transients resulting from non-safety related control system failures do not compromise safety.

The resolution of A-47 provides a generic letter to be issued to all plants (See Enclosure 1). The generic letter includes four actions and provides guidance to the licensees to reduce efforts needed to prepare their responses. These actions are:

- (1) Provide the results of the staff's generic analyses. Licensees are expected to review this information for applicability and to consider action only if the staff's analyses do not bound their specific plant design.
- (2) Request that all PWR plants provide automatic steam generator overflow protection, all BWR plants provide automatic reactor vessel overflow protection, and the technical specifications include provisions to periodically verify the overflow protection system operability.
- (3) Request that certain Babcock and Wilcox plants provide automatic initiation of auxiliary feedwater in the event of loss of power to the non-safety related feedwater control system.
- (4) Request that certain Combustion Engineering plants reassess their emergency procedures and training to assure safe shutdown during any postulated small break loss of coolant accident.

It has been determined that these actions are backfits. Justification for the backfit is presented in NUREG-1218. In order to minimize the staff's efforts and expedite the schedule for the review of the licensees' response to the generic letter, a model SER (Enclosure 4) is attached for internal use by NRR. This document will be used as guidance for the project managers of each plant to expedite the review of the overflow protection and assure that the required actions have been implemented.

As part of the CRGR package we are also enclosing for guidance to NRR a copy of the proposed revision to the Babcock and Wilcox and to the Combustion Engineering Standard Technical specifications (STS) (Enclosure 5). These (STS) sections have been updated to reflect changes for overflow protection. These changes are commensurate with the STS requirements for other systems that initiate safety actions. The STS for Westinghouse and for the General Electric plant designs currently include requirements for overflow protection and therefore no changes to those STS are required.



APR 3 1989

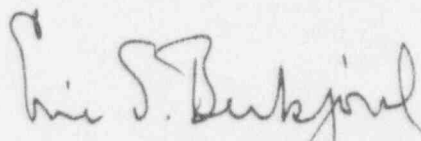
Other on-going staff programs that are related to, but are outside the scope of, USI A-47 are discussed in Appendix A, in NUREG 1217. Any action developed as part of these programs will be imposed independently of USI A-47.

Discussions were also held with the ACRS regarding the resolution of USI A-47. The ACRS agreed with the proposed resolution but expressed concerns regarding the scope of A-47 and identified some areas of concern that were not completely reviewed by this program and where additional work was still needed. These areas are now being identified and described by ORNL in a separate program entitled Multiple System Responses Program (MSRP). The MSRP program is intended to define specific bounds for these and other concerns in order to allow the NRC staff to prioritize these activities.

This enclosed package has been reviewed and concurred by NRR, AEOD and OGC.

Since no substantive changes were made to this package during the public comment period, the staff does not believe that a formal CRGR review is needed. We will however be available to brief the committee, if needed. Subject to a favorable recommendation by CRGR, the A-47 resolution would be implemented by forwarding the generic letter and the supporting enclosures to NRR. We have identified USI A-47 as a Category 2 action.

For further information on this subject, contact Andrew Szukiewicz, USI A-47 Task Manager (x23914).



Eric S. Beckjord, Director  
Office of Nuclear Regulatory Research

Enclosures:

1. Generic Letter
2. NUREG-1217 "Safety Implications of Control Systems in LWR Nuclear Power plants, Technical Findings Related to Unresolved Safety Issue A-47
3. NUREG-1218 Regulatory Analysis for Resolution of USI A-47
4. Model SER
5. Revised STS for B&W and CE plants

cc: w/o enclosures  
T. Speis  
W. Houston  
W. Minners  
R. Baer  
D. Thatcher  
A. Szukiewicz  
J. Conran

GENERIC LETTER  
(REFERENCE USI A-47)

TO: All Licensees of Operating Reactors, Applicants for Operating Licenses and Holders of Construction Permits for Light Water Reactor Nuclear Power Plants.

GENTLEMEN:

SUBJECT: 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)  
(Generic Letter \_\_\_\_\_)

As a result of the technical resolution of USI A-47, "Safety Implications of Control Systems in LWR Nuclear Power Plants," the NRC has concluded that protection should be provided for certain control system failures and that selected emergency procedures should be modified to assure that plant transients resulting from control system failures do not compromise public safety.

The NRC is taking four actions with respect to all licensees and applicants of LWR nuclear power plants. The first action provides to all licensees and applicants the results of the analyses conducted for this review. During the A-47 review a number of different designs for reactor vessel and steam generator overfill protection were evaluated. The staff concluded, with only a few exceptions, that no significant safety benefit could be gained by providing additional redundant level sensors and trip logic to terminate main feedwater on plants that already have automatic overfill protection. Plant specific features such as: power supply interdependence, sharing of sensors between control and trip logic, operator training, and designs for indication and alarms available to the operator were considered in developing risk estimates associated with failures of the feedwater trip system. This information, including the analysis for other events evaluated, such as overheat and overcool events, are provided for information only. It is expected that each licensee and applicant will review the information for applicability to its facility and conduct a plant specific analysis and make modifications, as needed, if the staff analysis and the conclusions do not bound their specific plant design. The results of the analyses and the technical bases for the NRC conclusions are documented in the references listed in Enclosure 1.

The second action recommends that all PWR plants provide automatic steam generator overfill protection and all BWR plants provide automatic reactor vessel overfill protection and that technical specifications include provisions to verify periodically the operability of the overfill protection and to assure that automatic overfill protection is available to mitigate main feedwater overfeed events during reactor power operation. The Technical Specifications recommendations are consistent with the criteria and the risk considerations of the Commission Interim Policy Statement on Technical Specification Improvement. In addition, the staff recommends that all BWR recipients reassess and modify, if needed, their operating procedures and operator training to assure that the

operators can mitigate reactor vessel overfill events that may occur via the condensate booster pumps during reduced system pressure operation. Enclosure 2 describes the requested action.

Enclosure 2 outlines a number of designs that satisfy the objectives for overfill protection and provides guidance for an acceptable design. The staff believes that a significant number of plants already provide satisfactory designs for overfill protection; many plants also have technical specifications dealing with overfill protection system surveillance which were previously approved by the staff. To reduce the documentation associated with the response regarding overfill protection and to facilitate NRC review, the licensee/applicant ~~should~~ <sup>shall</sup> submit a letter of confirmation explicitly stating compliance with the guidance of Enclosure 2. *confirm or justify*

The third action is to recommend that certain Babcock and Wilcox plants provide either automatic initiation of auxiliary feedwater on low steam generator level or another acceptable design to prevent steam generator dryout on a loss of power to the control system. Most B&W plants have already incorporated automatic initiation circuits for this purpose. Enclosure 2 identifies the plants that have not, and describes the requested action.

The fourth action is to recommend that certain Combustion Engineering plants reassess their emergency procedures and operator training to assure safe shutdown of the plants during any postulated small break loss of coolant accident. Enclosure 2 identifies these plants and describes the requested action.

On the basis of the technical studies the staff requests that these actions be taken by all LWR plants to enhance safety. These actions result from the staff interpretation of General Design Criteria 13, 20, and 33, identified in 10CFR50, Appendix A.

The implementation schedule for actions on which commitments are made by licensees or applicants in response to this letter should be prior to start-up after the first refueling outage beginning nine (9) months following receipt of the letter. *provide flexibility*

In order to determine whether any license or construction permit for facilities covered by this request should be modified, suspended or revoked, we request, <sup>require</sup> pursuant to Section 182 of the Atomic Energy Act and 10 CFR 50.54(f), that you provide the NRC, within <sup>90</sup> ~~90~~ days of the date of this letter, a statement as to whether you will ~~comply~~ <sup>comply</sup> with the ~~requested~~ <sup>requested</sup> actions in Enclosure 2 and, if so, that you provide a schedule for implementation of the items in Enclosure 2 and the basis for the schedule. This information should be submitted to the NRC, signed under oath and affirmation. The licensee should retain, ~~on site~~, <sup>in accordance with the records</sup> the documentation associated with the actions ~~for possible future inspection~~. Technical specification applications must, however, include a summary of design information and all other necessary documentation for staff review and also satisfy all appropriate regulations, in particular 10CFR50.91 covering potential significant hazards considerations. *MS*

*confirm or justify*

This request is covered by Office of Management and Budget Clearance Number 3150-0011 which expires December 31, 1989. The estimated average burden hours is 240 man-hours per licensee response, including assessment of the new recommendations, searching data sources, gathering and analyzing the data, and the required reports. These estimated average burden hours pertain only to these identified response-related matters and do not include the time for actual implementation of the requested actions. Comments on the accuracy of this estimate and suggestions to reduce the burden may be directed to the Office of Management and Budget, Room 3208, New Executive Office Building, Washington, D.C. 20503, and to the U.S. Nuclear Regulatory Commission, Records and Reports Management Branch, Office of Administration and Resources Management, Washington, D.C. 20555.

If you have any questions on this matter, please contact your project manager.

Sincerely,

Steven A. Varga, Acting  
Associate Director for Projects  
Office of Nuclear Reactor Regulation

Enclosures:

1. Enclosure 1 and 2 to the generic letter
2. NUREG-1217 "Safety Implications of Control Systems in LWR Nuclear Power Plants" - Technical Findings Related to Unresolved Safety Issue A-47
3. NUREG-1218 "Regulatory Analysis for Resolution of USI A-47"

REFERENCE

LIST OF SIGNIFICANT  
INFORMATION RELATED TO  
RESOLUTION OF USI A-47

1. NUREG-1217 "Evaluation of Safety Implications of Control Systems in LWR Nuclear Power Plants" - Technical Findings Related to USI A-47.
2. NUREG-1218 "Regulatory Analysis for Resolution of USI A-47."
3. NUREG/CR-4285 "Effects of Control System Failures on Transients, Accidents and Core-Melt Frequencies at a Westinghouse PWR."
4. NUREG/CR-4386 "Effects of Control System Failures on Transients, Accidents and Core-Melt Frequencies at a Babcock and Wilcox Pressurized Water Reactor."
5. NUREG/CR-4387 "Effects of Control System Failures on Transients, Accidents and Core-Melt Frequencies at a General Electric Boiling Water Reactor."
6. NUREG/CR-3958 "Effects of Control System Failures on Transients, Accidents and Core-Melt Frequencies at a Combustion Engineering Pressurized Water Reactor."
7. NUREG/CR-4326 "Effects of Control System Failures on Transients and Accidents at a 3 Loop Westinghouse, Pressurized Water Reactor." Vol. 1 and 2.
8. NUREG/CR-4047 "An Assessment of the Safety Implications of Control at the Oconee 1 Nuclear Plant-Final Report."
9. NUREG/CR-4262 "Effects of Control System Failures on Transients and Accidents At A General Electric Boiling Water Reactor." Vol. 1 and 2.
10. NUREG/CR-4265 "An Assessment of the Safety Implications of Control at the Calvert Cliffs - 1 Nuclear Plant" Vol. 1 and 2.
11. Letter Report ORNL/NRC/  
LTR-86/19 "Generic Extensions to Plant Specific Findings of the Safety Implications of Control Systems Program."



CONTROL SYSTEM DESIGN AND PROCEDURAL MODIFICATION  
FOR RESOLUTION OF USI A-47

As part of the resolution of USI A-47, "Safety Implications of Control Systems," the staff investigated control system failures that have occurred, or are postulated to occur, in nuclear power plants. The staff concluded that plant transients resulting from control system failures can be adequately mitigated by the operator, provided that the control system failures do not also compromise operation of the minimum number of protection system channels required to trip the reactor and initiate safety systems. A number of plant-specific designs have been identified, however, that ~~do not provide adequate protection from~~ transients leading to reactor core overheating or reactor vessel or steam generator overfill.

*need improvement*

Reactor vessel or steam generator overfill can affect the safety of the plant in several ways. The more severe scenarios could potentially lead to a steamline break and a steam generator tube rupture. The basis for this concern is the following: (1) the increased dead weight and potential seismic loads placed on the main steamline and its supports should the main steamline be flooded; (2) the loads placed on the main steamlines as a result of the potential for rapid collapse of steam voids resulting in water hammer; (3) the potential for secondary safety valves sticking open following discharge of water or two-phase flow; (4) the potential inoperability of the main steamline isolation valves (MSIVs), main turbine stop or bypass valves, feedwater turbine valves, or atmospheric dump valves from the effects of water or two-phase flow; and (5) the potential for rupture of weakened tubes in the once-through steam generator on B&W nuclear steam supply system (NSSS) plants due to tensile loads caused by the rapid thermal shrinkage of the tubes relative to the generator shell. These concerns ~~have not been adequately~~ addressed in plant designs, because overfill transients normally have not been analyzed.

To minimize some of the consequences of overfill, early plant designs provided commercial-grade protection for tripping the turbine or relied on operator action to control water level manually in the event the normal-water-level control system failed. Later designs, including the most recent designs, provide overfill protection which automatically stops main feedwater flow on vessel high-water-level signals. These designs provide various degrees of coincident logic and redundancy to initiate feedwater isolation and to ensure that a single failure would not inhibit isolation. A large number of plants provide safety-grade designs for this protection.

On the basis of the technical studies conducted by the staff and its contractors, the staff recommends that certain actions should be taken by some plants to improve plant safety. These actions are described in the material that follows, and include design and procedural modifications to ensure that (1) all plants provide overfill protection, (2) all plants provide technical specifications for periodic surveillance of the overfill protection, (3) certain Babcock and Wilcox plants provide an acceptable design to prevent steam generator dryout on

a loss of power to the control system, and (4) certain Combustion Engineering plants reassess their emergency procedures and operator training to ensure safe shutdown during any postulated small break loss of coolant accident.

(1) GE Boiling-Water-Reactor Plants

- (a) It is recommended that all GE boiling-water-reactor (BWR) plant designs provide automatic reactor vessel overflow protection to mitigate main feedwater (MFW) overfeed events. The design for the overflow-protection system should be sufficiently separate from the MFW control system to ensure that the MFW pump will trip on a reactor high-water-level signal when required, even if a loss of power, a loss of ventilation, or a fire in the control portion of the MFW control system should occur. Common-mode failures that could disable overflow protection and the feedwater control system, but would still result in a feedwater pump trip, are considered acceptable failure modes.

It is recommended that plant designs with no automatic reactor vessel overflow protection be upgraded by providing a commercial-grade (or better) MFW isolation system actuated from at least a 1-out-of-1 reactor vessel high-water-level system, or justify the design on some defined basis.

In addition, it is recommended that all plants reassess their operating procedures and operator training and modify them if necessary to ensure that the operators can mitigate reactor vessel overflow events that may occur via the condensate booster pumps during reduced pressure operation of the system.

- (b) It is recommended that technical specifications for all BWR plants with main feedwater overflow protection include provisions to verify periodically the operability of overflow protection and ensure that automatic overflow protection to mitigate main feedwater overfeed events is operable during power operation. The instrumentation should be demonstrated to be operable by the performance of a channel check, channel functional testing, and channel calibration, including setpoint verification. The technical specifications should include appropriate limiting conditions for operation (LCOs). These technical specifications should be commensurate with the requirements of existing plant technical specifications for channels that initiate protective actions. Previously approved technical specifications for surveillance intervals and limiting conditions for operation (LCOs) for overflow protection are considered acceptable. Justification should be included to demonstrate that the changes to the technical specifications are commensurate with previously approved designs.

Designs for Overflow Protection

Several different designs for overflow protection have already been incorporated into a large number of operating plants. The following discussion identifies the different groups of plant designs and provides guidance for acceptable designs.

Group I: Plants that have a safety-grade or a commercial-grade overfill protection system initiated on a reactor vessel high-water-level signal based on a 2-out-of-3 or a 1-out-of-2 taken twice (or equivalent) initiating logic. The system isolates MFW flow by tripping the feedwater pumps.

The staff concludes that this design is acceptable, provided that (1) the overfill protection system is separate from the control portion of the MFW control system so that it is not powered from the same power source, not located in the same cabinet, and not routed so that a fire is likely to affect both systems and (2) the plant technical specifications include requirements to periodically verify operability of this system and identify the LCOs. Licensees of plants that already have these design features that have been previously approved by the staff should state this in their response.

Group II: Plants that have safety-grade or commercial-grade overfill-protection systems initiated on a reactor vessel high-water-level signal based on a 1-out-of-1, 1-out-of-2, or a 2-out-of-2 initiating logic. The system isolates MFW flow by tripping the feedwater pumps.

The staff concludes that these designs are acceptable provided conditions (1) and (2) stated for Group I are met. Licensees of plants that already have these design features that have been previously approved by the staff should state this in their response. Plant designs with a 1-out-of-1 or a 1-out-of-2 trip logic for overfill protection should provide bypass capabilities to prevent feedwater trips during channel functional testing when at power operation.

Group III: Plants without automatic overfill protection.

It is ~~requested~~ <sup>recommended</sup> that the licensee have a design to prevent reactor vessel overfill and justify the adequacy of the design. The justification should include verification that the overfill protection system is separated from the feedwater control system so that it is not powered from the same power source, not located in the same cabinet, and not routed so that a fire is likely to affect both systems. Common-mode failures that could disable overfill protection and the feedwater control system, but would still result in a feedwater pump trip, are considered acceptable failure modes. The staff review identified three plants; i.e., Big Rock, LaCrosse (permanently shutdown), and Oyster Creek; that fall into this group. If any of these plants wish to justify not including overfill protection, part of the requested justification should demonstrate that the risk reduction in implementing an automatic overfill protection system is significantly less than the staff's generic estimates of risk reduction. In determining the risk reduction, specific factors such as low plant power and population density should be considered. Other applicable factors that are plant unique should also be addressed.

(2) Westinghouse-Designed PWR Plants

- (a) It is ~~requested~~ that all Westinghouse plant designs provide automatic steam generator overfill protection to mitigate MFW overfeed events. The design for the overfill protection system should be sufficiently separate

from the MFW control system to ensure that the MFW pump will trip on a reactor high-water-level signal when required, even if a loss of power, a loss of ventilation, or a fire in the control portion of the MFW control system should occur. Common-mode failures that could disable overfill protection and the feedwater control system, but would still result in the feedwater pump trip, are considered acceptable failure modes.

- (b) It is ~~requested~~ that technical specifications for all Westinghouse plants include provisions to periodically verify the operability of the MFW overfill protection and ensure that the automatic overfill protection is operable during reactor power operation. The instrumentation should be demonstrated to be operable by the performance of a channel check, channel functional testing, and channel calibration, including setpoint verification. The technical specifications should include appropriate LCOs. These technical specifications should be commensurate with existing plant technical specification requirements for channels that initiate protective actions. Plants that have previously approved technical specifications for surveillance intervals for overfill protection are considered acceptable. Justification should be included to demonstrate that the changes to the technical specifications are commensurate with previously approved designs. *JFK*

#### Designs for Overfill Protection

Several different designs for overfill-protection are already provided in most operating plants. The following discussion identifies the different groups of plant designs and provides guidance for acceptable designs.

Group I: Plants that have an overfill-protection system initiated on a steam generator high-water-level signal based on a 2-out-of-4 initiating logic which is safety grade, or a 2-out-of-3 initiating logic which is safety grade but uses one out of the three channels for both control and protection. The system isolates MFW by closing the MFW isolation valves and tripping the MFW pumps.

The staff concludes that the design is acceptable, provided that (1) the overfill protection system is sufficiently separate from the control portion of the MFW control system so that it is not powered from the same power source, not located in the same cabinet, and not routed so that a fire is likely to affect both systems, and (2) the plant technical specifications include requirements to periodically verify operability of this system and identify the LCOs.

Group II: Plants with a safety-grade or a commercial-grade overfill protection system initiated on a steam generator high-water-level signal based on either a 1-out-of-1, 1-out-of-2, or 2-out-of-2 initiating logic. The system isolates MFW by closing the MFW control valves.

The staff finds that only one early plant (i.e., Haddam Neck) falls into this group; therefore, a risk assessment was not conducted. Considering the successful operating history of the plant regarding overfill transients (i.e.,



no overflow events have been reported), this design may be found acceptable, provided that (1) justification for the adequacy of the design on a plant-specific basis is included and (2) technical specifications are modified to include requirements to periodically verify operability of this system and identify the LCOs. As part of the justification, it is requested that the licensee include verification that the overflow-protection system is separate from the feedwater-control system so that it is not powered from the same power source, not located in the same cabinet, and not routed so that a fire is likely to affect both systems. Common-mode failures that could disable overflow protection and the feedwater-control system, but would still cause a feedwater pump trip, are considered acceptable failure modes.

Group III: Plants without automatic overflow protection.

It is ~~requested~~ that the licensee have a design to prevent steam generator overflow and justify the adequacy of the design. The justification should include verification that the overflow-protection system is separated from the feedwater-control system so that it is not powered from the same power source, not located in the same cabinet, and not routed so that a fire is likely to affect both systems. Common-mode failures that could disable overflow protection and the feedwater-control system, but would still result in a feedwater pump trip, are considered acceptable failure modes. The staff's review identified two plants; i.e., Yankee Rowe and San Onofre 1; that fall into this category. If either of these plants wish to justify not including overflow protection, part of the requested justification should demonstrate that the risk reduction in implementing an automatic overflow protection system is significantly less than the staff's generic estimates of risk reduction. In determining the risk reduction, specific factors such as low plant power and population density should be considered. Other applicable factors that are plant unique should also be addressed.

(3) Babcock and Wilcox-Designed PWR Plants\*

- (a) It is ~~requested~~ that all Babcock and Wilcox plant designs have automatic steam generator overflow protection to mitigate MFW overfeed events. The design for the overflow-protection system should be sufficiently separate from the MFW control system to ensure that the MFW pump will trip on a steam generator high-water-level signal (or other equivalent signals)

---

\* On December 26, 1985, an overcooling event occurred at Rancho Seco Nuclear Generating Station, Unit 1. This event occurred as a result of loss of power to the integrated control system (ICS). Subsequently, the B&W Owners Group initiated a study to reassess all B&W plant designs including, but not limited to, the ICS and support systems such as power supplies and maintenance. As part of the USI A-47 review, failure scenarios resulting from a loss of power to control systems were evaluated; and the results were factored into the A-47 requirements. However, other recommended actions for design modifications, maintenance, and any changes to operating procedures (if any) developed for the utilities by the B&W owners group is being resolved separately.



when required, even if a loss of power, a loss of ventilation, or a fire in the control portion of the main feedwater control system should occur. Common failure modes that could disable overfill protection and the feedwater-control system, but would still result in a feedwater pump trip, are considered acceptable failure modes.

It is ~~requested~~ that plants that are similar to the reference plant design (i.e., Oconee Units 1, 2, and 3) have a steam generator high-water-level feedwater-isolation system that satisfies the single-failure criterion. An acceptable design would be to provide automatic MFW isolation by either (1) providing an additional system that terminates MFW flow by closing an isolation valve in the line to each steam generator (this system is to be independent from the existing overfill protection which trips the main feedwater pumps on steam generator high-water level); (2) modifying the existing overfill-protection system to preclude undetected failures in the trip system and facilitate online testing; or (3) upgrading the existing overfill-protection system to a 2-out-of-4 (or equivalent) high-water-level trip system that satisfies the single-failure criterion.

- (b) It is ~~requested~~ that technical specifications for all B&W plants include provisions to periodically verify the operability of overfill protection and ensure the automatic main feedwater overfill protection is operable during reactor power operation. The instrumentation should be demonstrated to be operable by the performance of a channel check, channel functional testing, and channel calibration, including setpoint verification. Technical specifications should include appropriate LCOs. These technical specifications should be commensurate with the requirements of existing technical specifications for channels that initiated protective actions. Justification should be included to demonstrate that the changes to the technical specifications are commensurate with previously approved designs. ] *for*
- (c) It is ~~requested~~ that plant designs with no automatic protection to prevent steam generator dryout upgrade their design and the appropriate technical specifications and provide an automatic protection system to prevent steam generator dryout on loss of power to the control system. Automatic initiation of auxiliary feedwater on steam generator low-water level is considered an acceptable design. Other corrective actions identified in Section 4.3(4) of NUREG-1218 could also be taken to avoid a steam generator dryout scenario on loss of power to the control system. The staff believes that only three B&W plants, i.e., Oconee 1, 2, and 3, do not have automatic auxiliary feedwater initiation on steam generator low water level).

#### Designs for Overfill Protection

Several different designs for overfill protection are already provided on most operating plants. The following discussion identifies the different groups of plant designs and provides guidelines for acceptable designs.

Group I: Plants that provide a safety-grade overfill-protection system initiated on a steam generator high-water-level signal based on either a 2-out-of-3 or a 2-out-of-4 (or equivalent) initiating logic. The system isolates main feedwater (MFW) by (1) closing at least one MFW isolation valve in the MFW line to each steam generator and (2) tripping the MFW pumps.

The staff concludes that this design is acceptable, provided that (1) the overfill protection system is sufficiently separated from the feedwater control system so that it is not powered from the same power source, not located in the same cabinet, and not routed so that a fire is likely to affect both systems (common-mode failures that could disable overfill protection and the feedwater control system, but still result in a feedwater pump trip are considered acceptable failure modes) and (2) the plant technical specifications include requirements to verify operability of this system periodically and identify LCOs.

Group II: Plants that have a commercial-grade overfill-protection system initiated on a steam generator high-water level based on coincident logic that minimizes inadvertent initiation. The system isolates MFW by tripping the MFW pumps.

This design may be found acceptable, provided that (1) the overfill-protection system is sufficiently separate from the feedwater control system so that it is not powered from the same power source, not located in the same cabinet, and not routed so that a fire is likely to affect both systems and (2) the design modifications are implemented per the guidelines identified in the second paragraph of item (3)(a) above and that the plant technical specifications include requirements to periodically verify operability of this system and identify LCOs.

It is requested that plant designs that provide a separate 1-out-of-1 or a 1-out-of-2 trip logic to close the feedwater isolation valves for additional overfill protection provide bypass capabilities to prevent feedwater trips during channel functional testing when at power or during hot-standby operation. These technical specifications should be commensurate with existing plant technical specification requirements for channels that initiate protection actions. } *fer*

(4) Combustion Engineering-Designed PWR Plants

- (a) It is requested that all Combustion Engineering plants provide automatic, steam generator overfill protection to mitigate main feedwater (MFW) over-feed events. The design for the overfill-protection system should be sufficiently separate from the MFW control system to ensure that the MFW pump will trip on a steam generator high-water-level signal when required, even if a loss of power, a loss of ventilation, or a fire in the control portion of the MFW control system should occur. Common failure modes that could disable overfill protection and the feedwater control system, but would still result in a feedwater pump trip, are considered acceptable failure modes.

- (b) It is ~~requested~~ that technical specifications for all Combustion Engineering plants include provisions to verify periodically the operability of overfill protection and ensure that automatic MFW overfill protection is operable during reactor power operation. The instrumentation should be demonstrated to be operable by the performance of a channel check, channel functional testing, and channel calibration, including setpoint verification, and by identifying the LCOs. These technical specifications should be commensurate with existing plant technical specifications requirements for channels that initiate protection actions. Justification should be included to demonstrate that the changes to the technical specifications are commensurate with previously approved designs. } *for*
- (c) It is ~~requested~~ that all utilities that have plants designed with high-pressure-injection pump-discharge pressures less than or equal to 1275 psi reassess their emergency procedures and operator training programs and modify them, as needed, to ensure that the operators can handle the full spectrum of possible small-break loss-of-coolant accident (SBLOCA) scenarios. This may include the need to depressurize the primary system via the atmospheric dump valves or the turbine bypass valves and cool down the plant during some SBLOCA. The reassessment should ensure that a single failure would not negate the operability of the valves needed to achieve safe shutdown.

The procedure should clearly describe any actions the operator is required to perform in the event a loss of instrument air, or electric power prevents remote operation of the valves. The use of the pressurizer PORVs to depressurize the plant during an SBLOCA, if needed, and the means to ensure that the R<sub>NDT</sub> (reference temperature, nil ductility transition) limits are not compromised should also be clearly described. Seven plants have been identified that have high pressure injection pump discharge pressures less than or equal to 1275 psi that may require manual pressure-relief capabilities using the valves to achieve safe shutdown. They are: Calvert Cliffs 1 and 2, Fort Calhoun, Millstone 2, Palisades, and St. Lucie 1 and 2.

#### Designs for Overfill Protection

CE-designed plants do not provide automatic steam generator overfill protection that terminates MFW flow. Therefore, it is requested that licensees and applicants for CE plants provide a separate and independent safety-grade or commercial-grade steam generator overfill-protection system that will serve as backup to the existing feedwater runback, control system. Existing water-level sensors may be used in a 2-out-of-4 initiating logic to isolate MFW flow on a steam generator high-water-level signal. The proposed design should ensure that the overfill protection system is separate from the feedwater-control system so that it is not powered from the same power source, is not located in the same cabinet, and is not routed so that a fire is likely to affect both systems (common-mode failures described above are considered acceptable) and the plant technical specifications should include requirements to periodically verify operability of the system and identify the LCOs. The information that is requested to be addressed in the technical specifications is provided in item (4)(b) above.

---

# Evaluation of Safety Implications of Control Systems in LWR Nuclear Power Plants

Technical Findings Related to  
Unresolved Safety Issue A-47

Final Report

---

**U.S. Nuclear Regulatory  
Commission**

Office of Nuclear Regulatory Research

A. J. Szukiewicz



---

# Evaluation of Safety Implications of Control Systems in LWR Nuclear Power Plants

Technical Findings Related to  
Unresolved Safety Issue A-47

Final Report

---

Manuscript Completed: November 1988  
Date Published: December 1988

A. J. Strukiewicz

Division of Engineering  
Office of Nuclear Regulatory Research  
U.S. Nuclear Regulatory Commission  
Washington, DC 20555





NUREG-1217

EVALUATION OF SAFETY IMPLICATIONS OF CONTROL SYSTEMS IN LWR  
NUCLEAR POWER PLANTS

DECEMBER 1988

## ABSTRACT

This report summarizes the work performed by the Nuclear Regulatory Commission (NRC) staff and its contractors, Idaho National Engineering Laboratory, Oak Ridge National Laboratory, and Pacific Northwest Laboratory, leading to the resolution of Unresolved Safety Issue (USI) A-47, "Safety Implications of Control Systems." The technical findings and conclusions presented in this document are based on the technical work completed by the contractors. The principal documents that contain the technical findings and conclusions of the contractors who worked on USI A-47 are summarized in Appendix B.

An in-depth evaluation was performed on non-safety-related control systems (see Section 1) that are typically used during normal plant operation on four nuclear steam supply system plants: a General Electric Company boiling-water reactor, a Westinghouse 3-loop pressurized-water reactor (PWR), a Babcock & Wilcox Co. (B&W) once-through steam generator PWR, and a Combustion Engineering PWR design. A study was also conducted to determine the generic applicability of the results to the class of plants represented by the specific plants analyzed. Generic conclusions were then developed.

Steam generator and reactor vessel overfill events and reactor vessel overcooling events were identified as major classes of events having the potential to be more severe than previously analyzed. Specific subtasks of this issue were to study these events to determine the need for preventive and/or mitigating design measures.

The impact of the Rancho Seco event (December 26, 1985), which involved a loss of power to the integrated control system is also discussed. This effort is closely coordinated with the USI A-47 effort, but is being evaluated separately by the B&W Owners Group and the NRC staff. Any requirements developed will be imposed independently of USI A-47.

This report describes the technical studies performed by the laboratories, the NRC staff assessment of the results, the generic applicability of the evaluations, and the technical findings resulting from these studies.

This final report contains the staff's responses to, and resolution of, the public comments that were solicited and received before September 16, 1988 in response to the draft reports issued for public comment on May 27, 1988.

# CONTENTS

	<u>Page</u>
ABSTRACT .....	iii
ACKNOWLEDGEMENTS .....	vii
ABBREVIATIONS .....	viii
<b>1 STATEMENT OF THE ISSUE .....</b>	<b>1</b>
<b>2 APPROACH .....</b>	<b>3</b>
2.1 Selection of Plants .....	3
2.2 Limitations and Assumptions of the Study .....	3
2.3 USI A-47 Program Overview .....	4
2.4 Review Procedures .....	6
2.4.1 Criteria Development .....	6
2.4.2 Systems Level Failure Mode and Effects Analyses .....	7
2.4.3 Thermal-Hydraulic Transient Analyses .....	7
2.4.4 Literature Search .....	8
2.4.5 Failure Analyses of Significant Control System Failures .....	8
<b>3 RESULTS OF THE INEL AND ORNL STUDIES .....</b>	<b>12</b>
3.1 Potentially Significant Control System Failure Scenarios .....	12
3.1.1 GE BWR Plant .....	12
3.1.2 W 3-Loop PWR Plant .....	12
3.1.3 B&W PWR Plant .....	12
3.1.4 CE PWR Plant .....	13
3.2 Literature Search .....	13
3.2.1 GE BWR Plants .....	13
3.2.2 W PWR Plants .....	13
3.2.3 B&W PWR Plants .....	13
3.2.4 CE PWR Plants .....	14
<b>4 GENERIC APPLICABILITY .....</b>	<b>26</b>
4.1 GE BWR Plants .....	27
4.1.1 Overfill Events at Power Resulting From Failures in the Reactor Vessel High-Water-Level Feedwater Trip System .....	27
4.1.2 Overfill and Overcooling Events During Low-Pressure Startup and Shutdown Operations .....	28
4.2 W PWR Plants .....	28
4.2.1 Overfill Events Resulting From a Sustained Operation of the Auxiliary Feedwater Flow .....	29
4.2.2 Overfill Events Resulting From Failures in the Steam Generator High-Water-Level Feedwater Trip System .....	30
4.2.3 Overcooling Events During Hot Shutdown and Full-Power Operation .....	30
4.2.4 Overpressure Events During Low-Temperature and Low-Pressure Shutdown or Startup Operating Conditions .....	32
4.2.5 Control System Failures Aggravating a Steam Generator Tube Rupture Event .....	33
4.3 B&W PWR Plants .....	33
4.3.1 Overfill Events Resulting From Failures in the Steam Generator High-Water-Level Main Feedwater Trip System .....	34

4.3.2	Overheating Events Resulting From Steam Generator Dryout .....	35
4.4	CE PWR Plants .....	35
4.4.1	Overfill Events Resulting From Operator Errors During a Steam Generator Overfeeding Event ..	36
4.4.2	Overheating Events and Possible Pressurized Thermal Shock Events Resulting From Operator Errors During Small-Break Loss-of-Coolant Accidents .....	36
5	SUMMARY AND CONCLUSIONS .....	38
6	REFERENCES .....	39
	APPENDIX A: OTHER RELATED STUDIES, PROGRAMS, AND ISSUES .....	41
	APPENDIX B: SUMMARY OF THE PRINCIPAL DOCUMENTS USED FOR USI A-47 STUDY .....	44
	APPENDIX C: STAFF RESOLUTION OF PUBLIC COMMENTS .....	46

## FIGURE

2.1	USI A-47 program overview .....	5
-----	---------------------------------	---

## TABLES

2.1	Control system screening criteria used by INEL to identify potentially significant control system failures .....	9
2.2	Control system screening criteria used by INEL to identify potentially significant control system failures on the <u>W</u> PWR reference plant design .....	10
2.3	Control system screening criteria used by ORNL to identify potentially significant control system failures on the B&W and CE PWR reference plant designs .....	11
3.1	Potentially significant failure scenarios in a representative GE BWR .....	15
3.2	Potentially significant failure scenarios in a representative <u>W</u> PWR .....	17
3.3	Potentially significant failure scenarios in a representative B&W PWR .....	21
3.4	Potentially significant failure scenarios in a representative CE PWR .....	24

## ACKNOWLEDGEMENTS

The technical findings relevant to Unresolved Safety Issue A-47, "Safety Implications of Control Systems," which are presented in this report, represent the combined efforts of staffs at the Nuclear Regulatory Commission (NRC), Idaho National Engineering Laboratory (INEL), Oak Ridge National Laboratory (ORNL) (and ORNL's subcontractor Science Applications Inc. [SAI]), and Pacific Northwest Laboratory (PNL). The following individuals deserve special mention for their participation and contributions:

N. Anderson	NRC/RES
W. Bickford	PNL
S. Bruske	INEL
W. Hodges	NRC/NRR
E. Lantz	NRC/NRR
A. McBride	SAI
C. Ransome	INEL
R. Stone	ORNL
A. Tabatabai	PNL



## ABBREVIATIONS

ACRS	Advisory Committee on Reactor Safeguards
ADV	atmospheric dump valve
AEOD	Office for Analysis and Evaluation of Operational Data
AFW	auxiliary feedwater
ATWS	anticipated transients without scram
B&W	Babcock & Wilcox Co.
BWOG	B&W Owners Group
BWR	boiling-water reactor
CE	Combustion Engineering
CFR	Code of Federal Regulations
CSF	control system failure
CSI	core spray injection
CSS	core spray system
ECC	emergency core cooling
ECCS	emergency core cooling system
EFW	emergency feedwater
FMEA	failure mode and effects analysis
FSAR	final safety analysis report
GDC	general design criteria
GE	General Electric Co.
HPI	high-pressure injection
IEEE	Institute of Electrical and Electronics Engineers
INEL	Idaho National Engineering Laboratory
LCO	limiting condition(s) for operation
LER	licensee event report
LOCA	loss-of-coolant accident
LPCI	low-pressure coolant injection
LTOP	low-temperature overpressure
MFW	main feedwater
MMS	modular modeling system
MSIV	main steam isolation valve
MSLB	main steamline break
NRC	U.S. Nuclear Regulatory Commission
NSS	nuclear steam system
NSSS	nuclear steam supply system
ORNL	Oak Ridge National Laboratory
PNL	Pacific Northwest Laboratory
PORV	power-operated relief valve
PRA	probabilistic risk analysis
PTS	pressurized thermal shock
PWR	pressurized-water reactor
RCS	reactor coolant system
SAI	Science Applications Inc.
SAR	safety analysis report
SBLOCA	small-break LOCA
SGTR	steam generator tube rupture
SIAS	safety injection actuation signal
SRV	safety/relief valve
TBV	turbine bypass valve
TMI	Three Mile Island
UCLA	University of California at Los Angeles
USI	unresolved safety issue
W	Westinghouse Corp.

## 1 STATEMENT OF THE ISSUE

Nuclear power plant instrumentation and control systems comprise safety-related protection systems and non-safety-related control systems. The safety-related protection systems are designed to satisfy the general design criteria (GDC) identified in 10 CFR Part 50 and are used to (1) trip the reactor whenever certain specific parameters exceed allowable limits, (2) protect the core from overheating by initiating the emergency core cooling systems, and (3) actuate other safety systems such as the closure of main steam isolation valves or opening of the safety or relief valves to maintain the plant in a safe condition. Non-safety-related control systems are used to maintain a nuclear plant within prescribed level, pressure, and temperature limits during shutdown, startup, and normal power operation. Non-safety-related control systems are not relied on to perform any safety functions during or following postulated accidents. They are used to control plant processes that could have a significant impact on the plant dynamics. Non-safety-related control systems include, but are not limited to: (1) reactivity control systems; (2) reactor coolant pressure, temperature, level, and flow control systems; and (3) inventory control systems (such as feedwater and borated water controls). In addition, they include secondary system pressure and flow controls (pressurized-water reactor [PWR]) as well as associated support systems, such as electric, hydraulic, and pneumatic power supply systems. The non-safety-related control systems are not required to be designed to satisfy the GDC.

During the licensing review processes, the U.S. Nuclear Regulatory Commission (NRC) performs an audit review on the non-safety-related instrumentation and control systems on a case-by-case basis. Although this audit review is not conducted to the same degree as the review of the safety systems, the review provides confidence that an adequate degree of separation and independence is provided between these non-safety-related systems and the safety-related protection systems. The audit review also provides confidence that misoperation or failure of non-safety-related control systems does not result in transient conditions more severe than conditions assumed in the bounding analyses reported in the plant safety analysis report (SAR).

Events that licensees are required to address are specified in Chapter 15 of the Standard Review Plan (NRC, NUREG-0800). These events include, but are not limited to:

- (1) feedwater system malfunctions that result in a decrease or an increase in the feedwater flow (including the loss of normal feedwater flow)
- (2) steam pressure regulator malfunctions or failures that result in an increase or a decrease in the steam flow (including the turbine trip event)
- (3) spectrum of reactivity addition events
- (4) chemical and volume control malfunctions that increase the reactor coolant inventory or decrease the boron concentration

Because non-safety-related control systems are only audited as part of the licensing review, there may exist some potential (which an audit review did not disclose) for accidents or transients developing into more severe events than previously analyzed, if compounded by non-safety-related control system failures.

These system failures or malfunctions may occur independently or as a result of an accident or transient. Concerns have previously been identified (NRC [AEOD], 1980; NUREG-0153) in which a failure or malfunction of the non-safety-related control system can (1) potentially cause a steam generator or reactor vessel to overfill (see AEOD report) or (2) can lead to a transient (in PWRs) in which the vessel could be subjected to severe overcooling (see NRC, SECY-82-465). In addition, the potential exists for a single failure (such as a loss of power supply, a short circuit, an open circuit, a control sensor failure) or for multiple failures resulting from a common-cause failure to cause a malfunction of one or more control systems which could lead to an undesirable control system response, or could provide misleading information to the plant operators.

The purpose of the Unresolved Safety Issue (USI) A-47 study is to perform a more in-depth review of the non-safety-related control systems and to (1) evaluate the need for modifying control systems in operating reactors, (2) verify the adequacy of current licensing requirements identified in Section 7.7 of the Standard Review Plan (NRC, NUREG-0800), and (3) evaluate the need for additional guidelines and criteria to ensure that non-safety-related control system failures do not pose unacceptable public risk. To this end, tasks were established to identify control systems whose failure could (1) cause transients or accidents to be potentially more severe than those identified in the final safety analysis report (FSAR) and previously analyzed, (2) adversely affect any assumed or anticipated operator action during the course of transients or accidents, (3) cause technical specification safety limits to be exceeded, or (4) cause transients or accidents to occur at a frequency in excess of those established for abnormal operational transients and design-basis accidents.

It should be noted that the focus of the USI A-47 review was directed to identify and evaluate control system failures that could cause transients or accidents to be potentially more severe than those identified in the FSAR. Control system failure-induced transients that were bounded by the FSAR analysis were not considered significant failures for this review. These transients were evaluated, but if they were determined to be adequately mitigated by safety-related systems or if sufficient time was available for the transients to be mitigated by subsequent operator action and not exceed the bounding analyses, they were not considered to pose an important risk to public health and safety.

Because control systems are an integral part of plant operations, failures in these systems have historically caused plants to shut down or to actuate safety systems. Challenges to the safety systems could represent a small but potentially significant fraction of the overall plant risk. This fact has been demonstrated in plant probabilistic risk assessments that have been performed to date. As a result of plant-specific analyses that have exposed unique vulnerabilities to severe accidents, some plants have modified their designs. Generally, undesirable contributions to risk have been reduced to acceptable levels by changing procedures or modifying designs. The Commission plans to formulate an integrated systematic approach to exam-

ine the design of each nuclear power plant now operating or under construction for significant risk contributors. Once NRC and the nuclear industry have developed a method of analysis, every nuclear power plant that has not yet been appropriately examined will be studied, and any changes that are needed will be made to ensure that no excessive risk is posed to public health and safety (NRC, NUREG-1070).

The section that follows, "Approach," describes (1) the approach used to review non-safety-related control systems, (2) the limitations and assumptions made, and (3) the methods developed and the activities performed. Section 3 describes the results of the individual plant reviews and identifies the control system failure scenarios determined to be potentially safety significant. Section 4 discusses the generic applicability of the plant-specific reviews of the reference plants, Section 5 presents the staff's conclusions, and Section 6 lists the references cited in this report. Appendix A provides a summary of other NRC and industry studies, programs, and issues related to USI A-47. In Appendix B, the principal documents underlying the resolution of USI A-47 are summarized. Appendix C contains the staff's responses to, and resolution of, the public comments that were solicited and received before September 16, 1988, in response to the draft reports issued for public comment on May 27, 1988.

## 2 APPROACH

### 2.1 Selection of Plants

Three pressurized-water-reactor (PWR) plant designs and one boiling-water reactor (BWR) plant design were selected for the review of non-safety-related control systems. These reference plants are specific designs from each of the four major nuclear steam supply system (NSSS) vendors: Babcock & Wilcox Co. (B&W), Westinghouse Corp. (W), Combustion Engineering Co. (CE), and General Electric Co. (GE). A major factor in the selection of the reference plants was the quality and quantity of plant-specific design information available to the NRC staff. In addition, the three PWR designs were already being evaluated in the study of USI A-49, "Pressurized Thermal Shock," and a significant amount of information obtained in that study could be utilized. The BWR plant was selected because a considerable amount of design information was available from other NRC projects. Also, an existing thermal-hydraulic computer model was available for this plant.

The reference plant designs were reviewed by two national laboratories. Two of the PWR plants, representing B&W and CE designs, were evaluated by Oak Ridge National Laboratory (ORNL) (NRC, NUREG/CR-3692, -4047, -4265 (Vols. 1 & 2), and -4449). The other two plant designs, a GE BWR and a W PWR design, were evaluated by Idaho National Engineering Laboratory (INEL) [NRC, NUREG/CR-4262 (Vols. 1 & 2), and -4326 (Vols. 1 & 2)]. The risk analyses for potentially significant control system failures were performed by Pacific Northwest Laboratory (PNL) (NRC, NUREG/CR-3958, -4385, -4386, and -4387). Appendix B summarizes the content of the principal documents used for this review.

### 2.2 Limitations and Assumptions of the Study

To perform a systematic review of control system failures, it became quickly evident that the scope of the review had to be confined. The type of events and the type, number, and combinations of possible control system failures were therefore limited. In order to keep the review at a manageable level, limitations and assumptions had to be made. These limitations and assumptions and their bases are discussed below.

- (1) Non-safety-related control system failures would not cause simultaneous failure of both redundant trains of safety-related protection systems. This assumption implies that a minimum number of safety-related protection systems would be available for

(a) actuation of the reactor trip system, (b) actuation of the overpressure protection system, and (c) initiation of the minimum number of required emergency core cooling (ECC) systems, if needed during a control system failure transient. This assumption is considered valid on the basis that adequate separation and independence is required to be provided between the non-safety-related control systems and the safety-related protection systems. Independence is provided by verifiable isolation devices located between safety-related and non-safety-related systems and/or by physically locating the safety systems in separate areas and routing the electrical cables in separate raceways throughout the plant. The staff audits the safety-related systems (audit reviews) as part of the licensing review process to ensure that an adequate degree of separation and independence has been provided. Also, as part of the A-47 program, a literature search was conducted to review the operating history of control system failures. The purpose of the review, in part, was to identify any control system failures that could cause a failure in both safety-related protection systems. The staff's review (see Section 3.2 of this report) did not identify any such failures. In addition, as part of the USI A-17 systems interactions program, spatial interactions between safety-related systems and non-safety-related systems were considered. Any identified interactions between safety-related systems and non-safety-related control systems were evaluated as part of that program and are not included in the scope of the USI A-47 review.

- (2) External events such as earthquakes, floods, fires, and sabotage have not been considered in this study. Multiple control system failures were evaluated to assess some effects of common-cause failures on the plant. However, the review was limited to selected combinations of control system failures. Not all control system failures that could occur as a result of these external events were reviewed in detail. An attempt was made to select those failure scenarios that would bound the dynamic effects of a number of control system failures. System failures were evaluated for automatic and manual modes of operation and at different reactor power levels that included low-, intermediate-, and full-power operation.

It should be noted that evaluations have been performed by the staff and the utilities to assess the plant's ability to achieve safe shutdown during these external events. Fire protection reviews for all operating plants have also been performed to

ensure conformance to 10 CFR Part 50, Appendix R, and to evaluate the plant's ability to cope with fires and flooding in different cable trays as well as in different areas of the plant. These reviews evaluated the effects of fires and flooding in control-grade as well as protection-grade equipment.

Also, as part of the USI A-46 activities, control-grade and protection-grade equipment are evaluated to assess their seismic ruggedness and ensure that plants have the ability to achieve safe shutdown after a design-basis seismic event (see item 2 in Appendix A to this report).

- (3) Operator errors of omission or commission were not addressed in this review. Operating procedures for the important transients were reviewed. An assessment was made to determine whether operating procedures (to mitigate the transients of concern) were written so that the operator could perform the task in the time allowed. An evaluation was also performed to determine whether there was sufficient information (i.e., alarms and/or indications) available in the control room for the operator to assess the conditions in the plant at the time of the event. In some cases, early recognition of transients was necessary. Given early recognition, there were actions that the operator could take to mitigate these events. For the purposes of developing the failure scenarios and analyzing resulting transients on the plant model, two of the four reviews assumed no operator action for the first 10 minutes into the transient. The other plant reviews evaluated operator action on the basis of available time for action during each transient. For the risk-analysis phase evaluating the core-melt frequency, operator action for all plants reviewed was determined on the basis of available time for action during each significant transient identified.
- (4) Transients resulting from control system failures during limiting conditions for operation (LCO) (for example, systems deliberately disabled for a short time for testing and/or maintenance) were not considered in the review.
- (5) The processes used to modify and to maintain control systems were not considered in this review.
- (6) Anticipated transients without scram (ATWS) were not considered in the review. A separate generic study (NRC, NUREG-0460) was conducted to address this issue. On July 26, 1984, Title 10 of the Code of Federal Regulations (CFR) was amended to include Section 50.62 (ATWS rule), which requires specific improvements in the design and operation of commercial nuclear power facilities to reduce the likelihood of failure to shut down the reactor follow-

ing anticipated transients and to mitigate the consequences of an ATWS event.

- (7) Control system failures that could lead to failures of liquid tanks located outside the containment and to fuel-handling accidents (for example, spent fuel or accidents involving waste disposal systems) were not considered in this review. These systems do not usually interact with control systems that are used during normal plant operations.
- (8) Individual utilities had to address IE Bulletin 79-27, "Loss of Non-Class 1E Instrumentation and Control Power System Bus During Operation," and to modify their plants appropriately in order to ensure that the operator would be able to achieve cold shutdown conditions after a loss of power of a single bus to instrumentation and controls in systems used in attaining cold shutdown. A reevaluation of IE Bulletin 79-27 regarding the consequences of a loss of power to the instrumentation and control systems is currently being performed for all B&W-designed operating plants (see item 5 in Appendix A to this report).
- (9) The items of NUREG-0737, "Clarification of TMI Action Plan Requirements" (November 1980), were implemented or committed to be implemented on individual plant designs, including but not limited to Items II.E.1.1, II.E.1.2, II.K.2.2, II.K.2.9, and II.G.1.

### 2.3 USI A-47 Program Overview

Figure 2.1 summarizes the A-47 program and identifies that program's major activities. Both INEL and ORNL concentrated on identifying control system failures that could lead to:

- (1) steam generator (reactor vessel) overfill events
- (2) reactor vessel overcooling events
- (3) reactor core overheating events
- (4) events or accidents that could be more severe than those previously analyzed in the FSAR

Steam generator and reactor vessel overfill and reactor vessel overcooling events have been identified previously as potentially significant transients that could lead to unacceptable consequences. Review of how control system failures contribute to these events was, therefore, a major part of the program. The methodology developed during this phase of the review was then applied to identifying and evaluating control system failures contributing to reactor core overheating events and events or accidents that could be more severe than those previously analyzed in the FSAR.



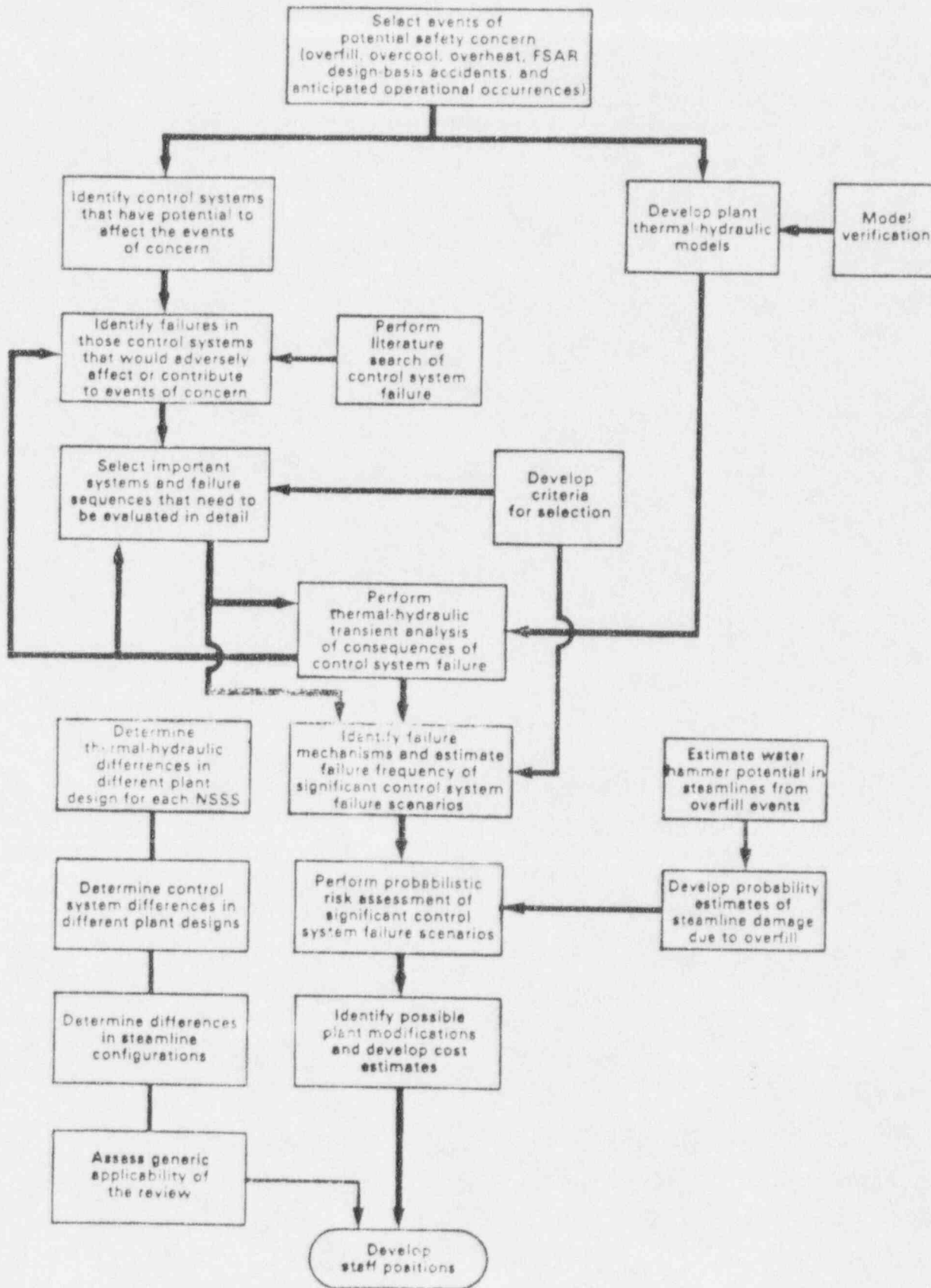


Figure 2.1 USI A-47 program overview

## Approach

The goal of the review was to identify the non-safety-related control systems whose failure or misoperation could:

- (1) cause transients or accidents identified in the FSAR analysis of the reference plants to be potentially more severe than previously analyzed
- (2) adversely affect any assumed or anticipated operator action during the course of a particular event
- (3) cause technical specification safety limits to be exceeded
- (4) cause transients or accidents to occur at a frequency in excess of the values established for abnormal operational transients and design-basis accidents
- (5) cause frequent challenges to the protection systems

INEL and ORNL developed similar approaches for evaluating control systems. Each approach consisted of several activities conducted in parallel:

- (1) Selection criteria for choosing important systems and important failure sequences were developed.
- (2) Failure mode and effects analyses were performed for all control systems in each reference plant to (a) identify systems that had the potential to affect the events of concern (for example, overfill, overcooling, overheating) and (b) identify the failure modes that would aggravate the events.
- (3) A literature search was conducted to review the operating history of selected plants and identify system failures that adversely affected plant safety.
- (4) Thermal-hydraulic computer models (for each reference plant design) were developed with sufficient detail of the plant systems and control systems design to simulate the dynamic responses of the plant during transient conditions.
- (5) Analysis was verified by comparing selected transient response calculations with actual plant data and other independent analyses using accepted and verified codes.

Credible combinations as well as some highly unlikely failure combinations of systems were analyzed to identify important control system failure sequences and to evaluate their consequences. Non-safety-related control system failures were evaluated for automatic and manual modes of operation and at different reactor power levels (low-, intermediate-, and full-power operations) in order to determine the bounding conditions. The sequences that satisfied the selection criteria were analyzed to identify component failures (including component failures in support systems). Failure mechanisms were identified

and estimates of failure frequencies were derived from generic failure-rate data. Estimates of failure frequencies were also related to specific plant failure data when available.

Safety-significant control system failures identified by INEL and ORNL are described in Section 3.

PNL performed a probabilistic risk analysis on all significant failure sequences that were identified. The importance of these sequences was determined according to their expected contribution to risk.

For the more risk-significant failure sequences, plant modifications were evaluated and the potential risk reduction and cost for these modifications were estimated. A typical steamline configuration was analyzed (insofar as stress) to evaluate the dynamic effects of overfill events. These studies were performed by INEL through its subcontractor CREARE R&D Inc.

Evaluations were made to assess the generic applicability of the review. This review was conducted in two steps: (1) assessing whether the thermal-hydraulic characteristic of different plants (of the same vendor) were similar to the reference plants and (2) assessing whether control and safety systems of different plants (of the same vendor) are sufficiently similar.

## 2.4 Review Procedures

INEL and ORNL employed similar methods and procedures to review the control systems. Differences were noted in the initiating mechanism for each type of transient evaluated, and in the number of control system failure combinations analyzed. These differences are attributed to the collective judgments made by the reviewers conducting the evaluations at each laboratory and the iterative process used to select the failure scenarios. These procedural differences are not significant.

### 2.4.1 Criteria Development

The following events for BWRs and PWRs were considered in identifying potentially significant control systems. These events were selected using the collective experience and judgment of the NRC staff and its consultants. Control systems whose failure could contribute to the listed events were identified by performing systems level failure mode and effects analyses (FMEAs) and were selected for detailed review as described in the following sections.

#### (1) BWR Events

- (a) increases and decreases in reactor coolant inventory

- (b) increases in reactor heat removal
- (c) increases in reactor vessel pressure
- (d) increases in reactor core positive reactivity
- (e) increases and decreases in reactor core recirculation flow

(2) PWR Events

- (a) increases and decreases in steam generator inventory
- (b) increases and decreases in heat removal by the secondary system
- (c) anomalies in reactivity and power distribution
- (d) decreases in reactor coolant system flow rate
- (e) increases and decreases in reactor coolant system inventory

Tables 2.1, 2.2, and 2.3 list the screening criteria used by INEL and ORNL to identify potentially significant control systems.

#### 2.4.2 Systems Level Failure Mode and Effects Analyses

A systems level FMEA was performed on all major plant systems for each reference plant design to identify systems and their failure modes that could potentially cause or contribute to the events listed above [Section 2.4.1(1) and (2)]. Systems that did not contribute to these events were deleted from further review. During this stage of review, both non-safety-related systems and safety-related systems were addressed. The criteria (Tables 2.1, 2.2, and 2.3) were interpreted broadly during the selection process to ensure that all systems that could contribute to the events of concern were identified, regardless of their relative effect. The effects of the failure of support systems (e.g., loss of air and loss of power supply) were also considered in this phase of the review.

#### 2.4.3 Thermal-Hydraulic Transient Analyses

Thermal-hydraulic transient analyses were conducted using computer models developed for each of the reference plant designs.

Computer models included the nuclear steam supply systems, the balance-of-plant systems, the safety-related reactor protection systems, and the major non-safety-related control systems designed to control pressure, temperature, flow, and flux. The control logic necessary to automatically actuate the safety-related and control-grade protection systems and/or components was included.

For the INEL analysis, RELAP 5/Mod 1.6 was used for both the GE and the W reference plant designs.

For the ORNL analysis, the computer model used for the B&W reference plant consisted of an analog model of the integrated control system coupled to a digital thermal-hydraulic model of the major reactor components and systems. This hybrid model (NRC, NUREG/CR-4449) used a number of different codes to model the various components and subsystems in the design. The codes most widely used were the RETRAN and RELAP codes.

For the CE reference plant design review, ORNL used the following plant models:

- (1) a RETRAN model of Calvert Cliffs Nuclear Power Plant, Unit 1 (developed principally by CE for the Baltimore Gas & Electric Company and modified by ORNL [NRC, NUREG/CR-4758] to include the necessary control and balance-of-plant system designs), and
- (2) a modular modeling system (MMS) computer code adapted to the Calvert Cliffs design.

The MMS model was developed as a backup in the event the RETRAN model might not be available. Subsequently, it was used for several transient simulations but was not needed for the design review.

Control system failures identified during the FMEA were represented in the thermal-hydraulic analysis. Single failures as well as multiple failures of systems such as loss of power to the control systems were evaluated to assess their effect on the transient behavior of the plant. It was not necessary in all cases to use the thermal-hydraulic model to evaluate the effects of every system failure identified by the FMEA. Engineering judgment limited the numbers and kinds of transients that were analyzed. Selection of the type and number of system failures evaluated was an iterative process. That is, the selection of system failures was highly dependent on the results of previous analyses. In selecting credible single-failure and multiple-failure scenarios for analysis, engineering judgment prevailed. In some cases (more extensively in the reviews of the GE and the W designs), highly unlikely combinations of multiple failures were selected for analysis. These combinations were chosen to select system failure combinations that could have the most significant

## Approach

effect on the events of concern. If these selected multiple failures resulted in acceptable plant transients, many other (less severe) failure combinations could be eliminated from consideration. Failure combinations were also selected to assess the effects of potential common-mode failures of the more important systems.

If unlikely failure combinations resulted in significant plant transients, the failure modes were then analyzed to determine how credible these failure combinations were and to estimate the frequency of such failures.

Combinations of system failures under various normal plant conditions (i.e., startup, shutdown, and power operation) and accident conditions were analyzed. Failures that were considered for selecting worst-case or bounding transients included the following:

- (1) single and multiple failure of safety-related protection systems (evaluated only on GE and W designs)

Some single failures in safety-related protection systems could produce more severe transients than those caused by combined failures of various non-safety-related control systems. In many cases, including the effects of safety-related protection, failures bounded the effects of a number of non-safety-related control system failure combinations and therefore minimized the number of non-safety-system failure combinations that needed to be analyzed by computer simulation.

- (2) single failures of non-safety-related systems
- (3) multiple dependent failures of safety-related protection systems and non-safety-related systems resulting from a single event such as loss of a support system
- (4) multiple independent system failures

Loss of ac and dc electric power supply systems and air systems was considered in the review. When multiple control system failures were identified that could occur as a result of a loss of a single electrical bus or a single air supply system or common sensing lines, they were analyzed. For certain systems, if it was not apparent from the available information whether or not they could fail simultaneously as a result of loss of power, multiple (dependent) failures were postulated. If these failures resulted in significant plant transients, the failure modes would then be analyzed to determine if these failures were credible.

For certain events, multiple independent failures of non-safety-related systems (and safety-related systems for the

GE and the W review) were also evaluated. These analyses were performed in part to verify the dynamic plant response to failures that were assumed in the FSAR analysis (that is, a single failure of a safety-related system concurrent with loss of a single non-safety-related system) and in part to assess combinations of control system failures that might occur on other plants as a result of a common-cause failure resulting from unique design configurations. The number of control system failure combinations that were analyzed were minimized by selecting only those combinations that would have the greatest impact on plant parameters (e.g., flow, pressure, and level). These combinations were judged to be the "worst case" scenarios. If these combinations resulted in acceptable plant transients, other (less severe) failure combinations could be eliminated from consideration.

### 2.4.4 Literature Search

The literature was searched to identify and evaluate transients or accidents initiated by failures related to control and instrument systems. Licensee event reports (LERs) and nuclear plant experience reports were reviewed to identify and select candidate scenarios for transient analysis. Control system failures from these reports were screened to identify those failures that could (1) adversely affect operator actions, (2) result in the actuation of protection systems, (3) cause technical specification safety limits to be exceeded, and (4) cause transients or accidents designated as moderate or infrequent events to occur more frequently than prescribed. Also, the LERs were used to assess if control system failures (shown by analysis not to be a problem on the reference plant) might be of concern at other plants. Data on control and instrument failures from 1969 through 1985 were reviewed by the laboratories. ORNL data were supplemented by additional data provided by the University of California at Los Angeles (UCLA) (Alter and Okrent, 1983). UCLA staff visited seven plant sites, gathering operating experience and reviewing station records.

### 2.4.5 Failure Analyses of Significant Control System Failures

Failures that met the selection criteria (refer to Tables 2.1, 2.2, and 2.3) were considered to be safety significant. Analyses were performed to identify the credible failure mechanisms that could cause the events of concern. Probability was also estimated for each identified failure mechanism and for the resulting failure scenarios that could cause the events of concern. The results of these reviews are described in Section 3.

Table 2.1 Control system screening criteria used by INEL to identify potentially significant control system failures on the GE BWR reference plant design

- 
- (1) Any control-grade system or component failure, either initiating or aggravating, that results in an undesired *increase in reactor coolant inventory* to the point at which moisture enters the main steamlines, will be selected for a detailed review. For this study, the point of overflow is defined as that level which, if exceeded, could cause significant water to carry over into the main steamlines.
  - (2) Any control-grade system or component failure, either initiating or aggravating, that results in an undesired *decrease in reactor vessel inventory* beyond the bounds of the Browns Ferry FSAR analysis, will be selected for a detailed review.
  - (3) Any control-grade system or component failure, either initiating or aggravating, that results in an undesired *increase in heat removal* beyond the bounds of the Browns Ferry FSAR analysis, will be selected for a detailed review. System failures that could lead to cooldown rates in excess of 100F° in an hour were identified as potentially significant failures during the transient analysis phase of the review.
  - (4) Any control-grade system or component failure, either initiating or aggravating, that results in an undesired *increase in reactor vessel pressure* beyond the bounds of the Browns Ferry FSAR analysis, will be selected for a detailed review.
  - (5) Any control-grade system or component failure, either initiating or aggravating, that results in an undesired *increase or decrease in reactor core coolant flow* beyond the bounds of the Browns Ferry FSAR analysis, will be selected for a detailed review.
  - (6) Any control-grade system or component failure, either initiating or aggravating, that results in an undesired *increase in positive reactivity* beyond the bounds of the Browns Ferry FSAR analysis, will be selected for a detailed review.
  - (7) Any control-grade system or component failures projected to cause transients identified as incidents of moderate frequency (anticipated operational occurrences) to occur more frequently than once a year, or failures which are projected to cause transients identified as infrequent incidents to occur more than once during the lifetime of a plant, or failures which are projected to cause limiting faults (design-basis accidents) will be selected for a detailed review.
  - (8) Any control-grade system or component failures that would adversely affect any assumed or anticipated operator action or operation of automatic protection systems during the course of a particular event, or that would result in frequent manual or automatic activation of engineered safety features, including the reactor protection system, or that would result in exceeding any technical specification safety limit, will be selected for a detailed review.
-



Table 2.2 Control system screening criteria used by INEL to identify potentially significant control system failures on the W PWR reference plant design

- 
- (1) Any control-grade system or component failure, either initiating or aggravating, that results in an undesired *increase in steam generator water level* to the point at which moisture enters the main steamlines, will be selected for a detailed review. For this study, the point of overflow is defined as that level which, if exceeded, could cause significant water to carry over into the main steamlines.
  - (2) Any control-grade system or component failure, either initiating or aggravating, that results in an undesired *increase or decrease in reactor coolant inventory* beyond the bounds of the H. B. Robinson FSAR analysis, will be selected for a detailed review.
  - (3) Any control-grade system or component failure, either initiating or aggravating, that results in an undesired *decrease in reactor coolant water temperature* beyond the bounds of the H. B. Robinson FSAR analysis, will be selected for a detailed review. System failures that could lead to cooldown rates in excess of 100F° in an hour were identified as potentially significant failures during the transient analysis phase of the review.
  - (4) Any control-grade system or component failure, either initiating or aggravating, that results in an undesired *increase in nuclear system pressure* beyond the bounds of the H. B. Robinson FSAR analysis, will be selected for a detailed review.
  - (5) Any control-grade system or component failure, either initiating or aggravating, that results in an undesired *decrease in reactor core coolant flow* beyond the bounds of the H. B. Robinson FSAR analysis, will be selected for a detailed review.
  - (6) Any control-grade system or component failure, either initiating or aggravating, that results in an undesired *increase in positive reactivity* beyond the bounds of the H. B. Robinson FSAR analysis, will be selected for a detailed review.
  - (7) Any control-grade system or component failure, aggravating a *steam generator tube rupture* causing a release of radioactive material to the atmosphere greater than the FSAR analysis calculated, will be selected for a detailed review.
  - (8) Any control-grade system or component failures projected to cause transients identified as incidents of moderate frequency (anticipated operational occurrences) to occur more frequently than once a year, or failures which are projected to cause transients identified as infrequent incidents to occur more than once during the lifetime of a plant, or failures which are projected to cause limiting faults (design-basis accidents) will be selected for a detailed review.
  - (9) Any control-grade system or component failures that would adversely affect any assumed or anticipated operator action during the course of a particular event, or that would result in frequent manual or automatic actuation of engineered safety features, including the reactor protection system, or that would result in exceeding any technical specification safety limit, will be selected for a detailed review.
-

Table 2.3 Control system screening criteria used by ORNL to identify potentially significant control system failures on the B&W and CE PWR reference plant designs

- 
- (1) Identify nuclear plant systems with potential to initiate or aggravate steam generator overfill. Such systems would be those whose failure or misoperation can introduce feedwater in amounts sufficient to fill the steam generator to the degree that water enters the steamlines.
  - (2) Identify nuclear plant systems with the potential to initiate or aggravate overcooling the primary system. Such systems would be those whose failure or misoperation can lead to uncontrolled primary heat removal at rates greater than the rate of heat production to the extent where safety limits are challenged. System failures that lead to extended cooldown rates in excess of 100F° in an hour were identified as potentially significant failures during the transient analysis phase of the review.
  - (3) Identify nuclear plant systems with potential to initiate or aggravate core damage through overheating.
  - (4) Identify nuclear plant systems with potential to degrade the performance of safety systems.
-

## 3 RESULTS OF THE INEL AND ORNL STUDIES

### 3.1 Potentially Significant Control System Failure Scenarios

Using the methods and screening criteria described in Section 2, potentially significant control system failure scenarios were identified for each reference plant design. The results are summarized in the sections that follow.

#### 3.1.1 GE BWR Plant

Three failure scenarios that could lead to reactor vessel overfill events were identified (NRC, NUREG/CR-4262, Vols. 1 & 2). Two of the three failure scenarios could also lead to overcooling events during low-pressure startup or shutdown operation. All other failure scenarios that were identified were determined to be bounded by the plant FSAR analyses.

For these events, an assumption was made that no operator action would be initiated for the first 10 minutes following any postulated failure. This guideline applies to operator response to a specific failure regardless of the time at which the failure occurs during the course of an event.

The onset of overfill was predicted to occur very quickly (i.e., between 20 and 300 seconds into the event). The reactor vessel was assumed to overfill when moisture entered the main steamlines and was sustained. Moisture carryover was defined as a significant change in steam quality and was indicated by the steamline vapor void fraction and the downcomer water level. The transient analyses were terminated after the vapor void fraction in the steamline continued to decrease at a steady rate, indicating that more water was entrained in the steam. Transients that resulted in the downcomer fluid temperature decreasing at a steady rate greater than  $100\text{F}^\circ$  in an hour were defined as overcooling transients. Table 3.1 summarizes the failure scenarios and the failure mechanisms that were identified as safety significant, and summarizes failure probabilities of control system failure sequences initiating the events of concern.

#### 3.1.2 W3-Loop PWR Plant

Eight failure scenarios were identified that could potentially lead to undesirable events (NRC, NUREG/CR-4326, Vols. 1 & 2). Two of these scenarios were identified as contributors to overfill events, two other scenarios contributed to overcooling events, and two contributed to reactor coolant system overpressure events. The remaining two failure scenarios contributed to a radiation release during a steam generator tube rupture, by causing

greater break flow conditions than were assumed in the FSAR accident analysis.

Transient studies showed that the limiting mode of operation for one of the two identified overcooling transients occurred during hot-shutdown conditions. The two overpressure transients occurred during cold-shutdown operation, and one of the overfill transients occurred during low-power operations. For the other failure scenarios, mid-range to full-power operation produced more rapid and severe transients.

For these events, an assumption was made that no operator action was initiated for the first 10 minutes following any postulated failure. This guideline applies to operator response to a specific failure regardless of the time at which the failure occurs during the course of the event.

Results of the thermal-hydraulic transient analysis indicated that:

- (1) The onset of overfill (via the main feedwater system) could occur very quickly (between 20 and 205 seconds).
- (2) Plant cooldown transients reached cooldown rates of  $100\text{F}^\circ$  within 125 to 230 seconds.
- (3) Overpressure limits (10 CFR Part 50, Appendix G curves) can be exceeded in 15 to 162 seconds.

Table 3.2 summarizes the failure scenarios and the failure mechanisms that were identified as safety significant, and summarizes the failure probabilities of control system failure sequences initiating the events of concern.

#### 3.1.3 B&W PWR Plant

Three potentially safety-significant failure scenarios were identified (NRC, NUREG/CR-3692, -4047, and -4449). One leads to a steam generator overfill event and two lead to a reactor core overheating event. The analysis indicates that the onset of overfill associated with main feedwater flow can occur very quickly (i.e., approximately 3 minutes) at power levels between 50 percent and 100 percent when both feedwater pumps are in operation. Overfill events associated with the auxiliary feedwater system and the startup feedwater system were predicted to occur at a much slower rate, so that the operator would be expected to have sufficient time to identify the event and terminate the flow before overfill conditions could occur. The onset of overfill was determined by a very low vapor void fraction fluid entering the steam generator downcomer and main steamlines. This guideline was similar to that discussed in Section 3.1.1 for the BWR review.

For the overheating events, it was predicted that the core could be severely damaged if the operator did not take proper corrective action within 30 to 60 minutes.

Other control system failure scenarios were identified in NUREG/CR-3692, -4047, and -4449, but were determined to be either bounded by transients or accidents analyzed in the FSAR, or it was determined that the operator would have sufficient time to terminate the event before it became a safety-significant event; therefore, they are not discussed here. Table 3.3 summarizes the failure scenarios and the failure mechanisms that were identified as safety significant, and summarizes failure probabilities of control system failure sequences initiating or contributing to the events of concern.

### 3.1.4 CE PWR Plant

Four potentially safety-significant failure scenarios were identified (NRC, NUREG/CR-4265). Two lead to overfilling the steam generator vessel via the main feedwater system; one leads to overheating the reactor core; and one overcooling event could lead to a possible pressurized thermal shock event in a plant with a vulnerable pressure vessel. Two categories of such overfill events were investigated: rapid and slow. Slow overfeeding transients occur via the feedwater bypass valves after the main feedwater-regulating valves are closed and were not considered safety significant because of the long time it took to overfill. Overfill with main feedwater systems was predicted to occur very quickly (that is, onset of overfill could occur in 2 minutes). Onset of overfill was assumed when low-quality steam entered the main steamlines. This guideline is similar to that discussed in Section 3.1.1 for the BWR review. For the other two failure scenarios, the analysis indicated that for a very narrow range of break sizes of small-break loss-of-coolant accidents (SBLOCAs), overheating of the core or possible pressurized thermal shock can occur if the operator fails to take the plant to safe-shutdown conditions. Other failure scenarios that were identified in NUREG/CR-4265 were determined to be bounded by the events analyzed in the FSAR accident analysis, or it was determined that the operator would have sufficient time to terminate the event. Therefore they are not discussed here.

Table 3.4 summarizes the failure scenarios and the failure mechanisms that were identified as safety significant, and summarizes failure probabilities of control system failure sequences initiating or contributing to events of concern.

## 3.2 Literature Search

Licensee event reports and nuclear plant experience reports were reviewed to identify control system failures that could (1) adversely affect operator actions, (2) result

in the actuation of protection systems, (3) cause technical specification safety limits to be exceeded, or (4) cause transients or accidents designated as moderate or infrequent events to occur more frequently than described. Data on control and instrument failures from 1969 through early 1985 were reviewed. The sections that follow summarize both that review and the conclusions.

### 3.2.1 GE BWR Plants

The literature review for BWR plants evaluated all reported events of control system failure for the Browns Ferry Nuclear Power Station, Units 1, 2, and 3, during a 3-year period (1980 through 1982). This review was expanded to include all other BWR plants for the same period. The data were further expanded to include potentially significant events occurring as early as 1970 (NRC, NUREG/CR-4262, Vols. 1 & 2).

Review of the operating experience did not identify any control system failures that satisfied the above criteria.

Three reactor overfill events did occur in the early 1970s. Two occurred at Dresden Nuclear Power Station, Units 2 and 3, and one at Nine Mile Point Nuclear Station, Unit 1. At the time of these events, the design did not provide a reactor vessel high-water-level feedwater trip system. A trip system was later incorporated.

Four overcooling events were also identified (Edwin I. Hatch Nuclear Plant, Unit 2 [1978]; Brunswick Steam Electric Plant, Unit 1 [1977]; Peach Bottom Atomic Power Station, Unit 3 [1979]; and Cooper Nuclear Station [1980]). These events were regarded as precursors to the transients evaluated in the plant model.

### 3.2.2 W PWR Plants

A similar review of the W PWR plants was conducted for the same 3-year period (1980 to 1982) (NRC, NUREG/CR-4326, Vols. 1 & 2). The review included the reference plant and five other W PWR plants. The review did not identify any control system failures that satisfied the criteria stated above.

### 3.2.3 B&W PWR Plants

A review of the operating experience was conducted for the reference plant and all other B&W PWR plants (NRC, NUREG/CR-4047). The period ranged from January 1975 through early 1985. On the basis of this review, no abnormal events were identified at the reference plant that led to potentially severe accidents or unsafe conditions. One steam generator overfill event occurred at Oconee Nuclear Station, Unit 3, in 1981.

The operating history data on other B&W PWR plants revealed the following:

## Results

- (1) Two steam generator overfill events occurred at Rancho Seco Nuclear Generating Station, Unit 1 (March 1978 and December 1985).
- (2) Operator errors could cause technical specifications to be violated.
- (3) Inadvertent malfunctions occurred infrequently.
- (4) Unnecessary scrams that challenge the protection system occur. B&W PWR plants have a lower-than-average industry record for the number of scrams (i.e., three per year).

### 3.2.4 CE PWR Plants

A review similar to the B&W review was conducted for CE PWR plants (NRC, NUREG/CR-4265).

A number of steam generator overfeeding events were identified; none progressed to an overfill condition. In all cases, the overfeeding events were terminated by the control system or by operator action. Maintenance and testing problems resulted in the most frequent challenges to the protection systems. The review did not identify any control system failures that satisfied the criteria stated in Tables 2.1, 2.2, and 2.3.



Table 3.1 Potentially significant failure scenarios in a representative GE BWR  
(Source: NUREG/CR-4262 and -4387)

Event	Failure scenario	Failure mechanism	Probability estimate (events/yr)
Overfill event #1	<p>Failure in the feedwater control system can cause an increase in feedwater flow and disable the feedwater trip system, <i>and</i> the operator fails to trip the feedwater pumps.</p> <p><u>Condition for Operation:</u> 67% full load operation.</p>	<p>A leak or rupture of the primary sensing line common to two of the three reactor vessel water-level sensors can cause false low-level signals.</p> <p>Common-cause failure (e.g., maintenance error) of two of the three reactor vessel level sensors (or sensor circuitry), can cause false low-level signals.</p> <p>Independent failures of two of the three level sensors (or sensor circuitry) can cause false low-level signals.</p> <p>A failure in the control circuit that regulates the feedwater pump speed and a second failure of two of the three high-level trips.</p>	3.4E-3*
Overfill event #2**	<p>Control system failure can cause an increase in the condensate flow <i>and</i> the operator fails to terminate condensate flow.</p> <p><u>Condition for Operation:</u> Low-pressure startup <i>or</i> reactor shutdown operation.</p>	<p>A single control system failure can cause any one of the three motor operated feedwater pump discharge valves to open, resulting in full condensate flow.</p> <p>A single failure of a startup feedwater low-pressure bypass valve (failing open) can cause an increase in the condensate flow rate.</p> <p>A single failure of a condenser bypass valve (failing closed) can cause an increase in the condensate flow rate.</p>	2.5E-5†

See footnotes at end of table.

Table 3.1 (Continued)

Event	Failure scenario	Failure mechanism	Probability estimate (events/yr)
Overfill event #3 <sup>*†</sup>	Failure in the protection system which results in inadvertent low-pressure coolant injection (LPCI) or core spray injection (CSI) and the operator fails to terminate flow.	Failure in a 1-out-of-2 taken-twice reactor low-water-level logic circuit.	1.6E-3 <sup>††</sup>
	<u>Condition for Operation:</u> Low-pressure startup or reactor shutdown operation.	Failure in one of the two high drywell pressure logic circuits.	
		Common-cause failure of two drywell pressure switches (failing closed).	
		Common-cause failure of two reactor vessel low-water-level switches (failing closed).	
		Two independent failures of drywell pressure switches or two independent reactor low-water-level switches (failing closed).	

\* Includes probability estimate (0.52/demand) that the operator fails to trip the feedwater in time to prevent overfill following a rapid overfeeding transient.

† This event can also cause an overcooling transient.

† Includes probability estimate (0.3/demand) that the operator fails to trip the condensate flow to prevent overfill.

†† Includes probability estimate (0.4/demand) that the operator fails to trip the LPCIs or CSIs.

Table 3.2 Potentially significant failure scenarios in a representative W PWR  
(Source: NUREG/CR-4326 and -4387)

Event	Failure scenario	Failure mechanism	Probability estimate (events/yr)
Overfill event #1	<p>A single control system failure can lead to excessive feedwater flow (e.g., overfeeding). When the feedwater flow is automatically terminated by the steam generator high-water-level trip system, the auxiliary feedwater system (which is automatically initiated when the main feedwater pumps are tripped) can cause a steam generator overfill condition if the operator does not take proper action to mitigate the transient.</p> <p><u>Condition for Operation:</u> Very-low-power operation (i.e., 5% power).</p>	<p>A false steam generator low-water-level signal to the feedwater controller can cause overfeeding of a steam generator.</p> <p>A leak or rupture in the primary sensing line of the controlling steam generator level instrument can cause overfill.</p> <p>A single failure can cause the feedwater regulating valve to open and cause an excessive overfeeding transient.</p> <p>A failure in the steam generator water-level controller circuitry can cause a steam generator overfeeding transient.</p>	1E-4*
Overfill event #2	<p>A control system failure can cause an increase in main feedwater flow <i>and</i> a second failure of a steam generator high-water-level trip system could cause an overfill event if the operator fails to terminate flow.</p> <p><u>Condition for Operation:</u> 67% full-power operation.</p>	<p>A failure in the controlling steam generator level instrument (causing it to indicate low) and a concurrent (or subsequent) second failure of another level channel (sticking or failing as is).</p> <p>A leak or rupture in the primary sensing line of the controlling steam generator level instrument <i>and</i> a second failure of another level channel (sticking or failing as is).</p> <p>A failure in the main feedwater valve (can cause it to open) <i>and</i> a failure of two of the three steam generator level instruments (fail in the mid-range position).</p>	3E-8**

See footnotes at end of table.

Table 3.2 (Continued)

Event	Failure scenario	Failure mechanism	Probability estimate (events/yr)
Overfill event #2 (cont'd)		<p>A failure of a steam generator level controller <i>and</i> a failure of two of the three steam generator water level instruments failing to respond to a high-water-level condition.</p> <p>The controlling steam generator level instrument fails low <i>and</i> the steam generator high-water-level trip logic circuitry fails to trip the feedwater pumps.</p> <p>A leak or rupture of the primary sensing line of the controlling level instrument (can cause the sensor to read low) <i>and</i> a failure of the high-water-level trip logic circuit.</p> <p>A failure of a feedwater valve (in the open position) <i>and</i> a failure of the high-water-level trip logic circuitry.</p> <p>Failure of the steam generator water-level controller and a failure of the high-water-level trip logic circuitry.</p>	
Overcool event #1	<p>A failure that results in an inadvertent steam dump operation with the reactor at power (all steam dump valves fail open <i>and</i> the operator fails to close the block valve).</p> <p><u>Condition for Operation:</u> 102% full-power operation (this failure scenario requires that the reactor trips during the early stage of the transient).</p>	<p>The <math>T_{avg}</math> temperature instrument fails high <i>and</i> a second failure occurs in the steam dump valve arming circuit.</p> <p>A single failure occurs in the temperature controller <i>and</i> a second failure occurs in the steam dump valve arming circuit.</p>	1.4E-8†
Overcool event #2	<p>Control system failure that results in inadvertent opening of the steam dump valves or steamline relief valves.</p> <p><u>Condition for Operation:</u> Hot shutdown (<math>T_{avg}</math> less than 547°F).</p>	<p>Single failure in the steam dump controller that sends a signal to one or more steam dump valves.</p> <p>A single failure in a steam dump valve that results in opening of the valve.</p>	1E-3†

See footnotes at end of table.

Table 3.2 (Continued)

Event	Failure scenario	Failure mechanism	Probability estimate (events/yr)
Overcool event #2 (Cont'd)		A single failure in the steam dump controller that sends an open signal to one or more PORV (atmospheric dump valves).	
		A steamline PORV control circuit (or switch) fails.	
Over-pressure event #1	A failure that results in a loss of letdown flow <i>and</i> a loss of pressure relief (both PORVs) and the operator fails to terminate the event.  <u>Condition for Operation:</u> Cold shutdown.	A loss of power that feeds both the letdown valve and one of the PORVs so that the pressurizer letdown valve goes to its closed position and renders the PORV inoperable <i>and</i> a second active failure of the other PORV.  Independent failure of a letdown valve in the closed position <i>and</i> failure of both PORVs to open.	2E-8††
Over-pressure event #2	A failure that results in inadvertent safety injection initiation when the reactor is being heated from cold shutdown. (During this operation both pressurizer PORV setpoints are shifted from the "low temperature" setpoint to the "normal" setpoint. If there is a failure causing inadvertent operation of safety injection, overpressure conditions can occur if the operator fails to terminate the event).  <u>Condition for Operation:</u> Heating up from cold shutdown.	A single failure in the logic circuit that results in the actuation of the safeguards sequence.  Independent failures that would initiate high-pressure safety injection <i>and</i> open the accumulator isolation valves.  A single failure in one of the two safety injection actuation pushbuttons (that actuates the safeguards sequence).	4E-5††
SGTR event #1	Failure that results in opening one of the steamline relief valves concurrent with a steam generator tube rupture in the affected steam generator.	A failure of a component in the steamline PORV control circuit can cause the valve to open and remain open.	2E-3 (7E-6 with an SGTR event)

See footnotes at end of table.



Table 3.2 (Continued)

Event	Failure scenario	Failure mechanism	Probability estimate (events/yr)
SGTR event #1 (Cont'd)	<u>Condition for Operation:</u> 102% power operation with one steam generator tube ruptured (adjacent to the cold-leg tube-sheet) <i>and</i> a simultaneous loss of offsite power.	A mechanical failure of a steamline PORV (i.e., atmospheric dump valve) can cause the valve to stick open.  A failure of a component in the steam dump controller can cause a steamline PORV to open and remain open.  A mechanical failure of a safety valve can cause it to stick open.	3E-3 (1E-5 with an SGTR event)
SGTR event #2	Failure that results in opening of steamline safety valves (SRVs) or steamline relief valves (PORVs) <i>and</i> a high feedwater rate concurrent with a rupture of a steam generator tube.  <u>Condition for Operation:</u> 102% power with one steam generator tube rupture (adjacent to the cold-leg tubesheet).	For PORV and SRV failure mechanisms, refer to SGTR event #1 above.  For feedwater overfeeding events, the following failure mechanisms were considered:  • A failure of a steam generator level instrument controlling the feedwater flow.  • A leak or rupture of the sensing line of the level instrument controlling the feedwater flow.  • Inadvertent opening of the feedwater control valve.  • A circuit failure of the steam generator water level controller.	

\*Includes probability estimate (0.1/demand) that the operator fails to terminate the auxiliary feedwater system to prevent overfill.

\*\*Includes probability estimate (0.5/demand) that the operator fails to terminate the flow.

†Includes probability estimate (0.05/demand) that the operator fails to initiate the block valve.

††Includes probability estimate (0.1/demand) that the operator fails to terminate the event.

Table 3.3 Potentially significant failure scenarios in a representative B&W PWR  
(Source: NUREG/CR-3692, -4047, and -4386)

Event	Failure scenario	Failure mechanism	Probability estimate (events/yr)
Overfill event	<p>Failure in the main feedwater control system (or valves) that could result in overfeeding one of the two steam generators <i>and</i> a concurrent (possibly long-present but undetected) failure of the main feedwater pump trip system which terminates feedwater flow on steam generator high-water level <i>and</i> a failure of the operator to detect and manually trip the main feedwater pumps or isolate the feedwater flow.</p> <p><u>Condition for Operation:</u> Normal power operations.</p>	<p>Failures that can cause main feedwater pump trip system to fail are:</p> <ul style="list-style-type: none"> <li>• Either of two high steam generator (operate range) level transmitters failing low.</li> <li>• Either of two steam generator level function generator modules failing.</li> <li>• Either of two multiplications modules failing.</li> <li>• Either of two signal monitors failing.</li> <li>• Feedwater pump trip relay (FTPX) failure.</li> <li>• Feedwater pump trip solenoid valve failures.</li> <li>• Feedwater pump turbine inlet intercept valve failures.</li> </ul> <p>Failures that can cause main feedwater overfeeding are:</p> <ul style="list-style-type: none"> <li>• Main feedwater control valves fail open or control valve signal fails demanding valve to open.</li> <li>• Miscellaneous failures of control modules associated with the feedwater control system.</li> </ul>	6E-3*

See footnotes at end of table.

Table 3.3 (Continued)

Event	Failure scenario	Failure mechanism	Probability estimate (events/yr)
Overheat event #1	<p>A loss of electric power to the integrated control system branch circuits "H" or "H1" when the control system is operating in the automatic mode would result in control stations for different control systems transferring to a manual mode of operation. This transfer could occur without upsetting plant operation. Power could be restored before any plant perturbations could occur. If, however, plant perturbations resulted in a reactor trip, feedwater overfeeding conditions could occur if the operator does not manually throttle the feedwater flow. The feedwater pumps would eventually trip on steam generator high-water level if the feedwater flow were allowed to continue and safe-shutdown operations would be initiated.</p> <p>If, however, the operator takes action early in the transient by throttling the feedwater to prevent overfeeding, but subsequently does not restore the necessary flow to the steam generator or initiate high-pressure injection (HPI), severe reactor core overheating can occur.</p> <p><u>Condition for Operation:</u> Normal operating range.</p>	A loss of "auto" power to integrated control system branch circuit "H" or "H1."	1.4E-6**
Overheat event #2	A failure of the "hand" power to the feedwater control system would result in the main feedwater pump run back to minimum speed. If the feed pumps were not tripped but allowed to operate at minimum speed, the steam generator water level would eventually be depleted. Unless the operator manually initiates the auxiliary feedwater system or restores the main feedwater flow, the steam generator would boil dry and steam generator cooling would be lost. The operator has about 30 minutes to reestablish the main or auxiliary feedwater flow. After	Loss of "hand" power to the integrated control system branch circuits (HX or H1X).	9E-6†

See footnotes at end of table.

Table 3.3 (Continued)

Event	Failure scenario	Failure mechanism	Probability estimate (events/yr)
	<p>30 minutes, establishing feedwater flow would not be effective to establish the necessary steam generator cooling. The high-pressure injection pumps would provide the necessary long-term core cooling if the operator manually initiates this system within 60 minutes.</p> <p><u>Condition for Operation:</u> Normal power operations.</p>		
	<p>*Includes probability estimate (0.7/demand) that the operator fails to trip the feedwater in time to prevent overfill following a rapid overfeeding transient.</p>		
	<p>**Includes probability estimate (0.03/demand) that the operator fails to reinstate main feedwater or initiate emergency feedwater within 30 minutes, and includes a probability estimate of 0.01/demand that the operator fails to initiate high-pressure injection within 60 minutes.</p>		
	<p>†Includes probability estimate (0.3/demand) that the operator fails to reinstate main feedwater or initiate emergency feedwater within 30 minutes, and includes a probability estimate of 0.01/demand that the operator fails to initiate high-pressure injection within 60 minutes.</p>		

Table 3.4 Potentially significant failure scenarios in a representative CE PWR  
(Source: NUREG/CR-3958 and -4265)

Event	Failure scenario	Failure mechanism	Probability estimate (events/yr)
Overfill event #1	<p>A single failure that causes the main feedwater regulating valve to fail in the "as is" or in the fully open position <i>and</i> the operator fails to terminate the overfeeding event.</p> <p><u>Condition for Operation:</u> Transient conditions following a reactor trip.</p>	<p>The following failures can cause the main feedwater regulatory valves to fail:</p> <ul style="list-style-type: none"> <li>• Loss of electrical bus (1Y09).</li> <li>• Air solenoid valve controlling air to the feedwater regulatory valve fails closed.</li> <li>• Mechanical failure of the main feedwater regulating valve.</li> <li>• Failure in the hand/auto station to the regulating valve.</li> <li>• Failure of the electrical to pneumatic convertor to the main feedwater regulating valve.</li> </ul>	9E-3*
Overfill event #2	<p>Given an overfeeding condition, if the turbine trip signal to the feedwater regulating circuit fails <i>and</i> the operator fails to terminate the feedwater flow, a system generator overfill event can occur (multiple failures would be required).</p> <p><u>Condition for Operation:</u> Normal power operation.</p>	<p>An overfeeding condition can occur if the feedwater demand signal fails high <i>and</i> the following failures occur to cause the turbine trip signal to fail to close the regulating valves:</p> <ul style="list-style-type: none"> <li>• Logic circuit failure.</li> <li>• Relay failure.</li> <li>• Cable failure.</li> </ul>	4E-4*

See footnotes at end of table.



Table 3.4 (Continued)

Event	Failure scenario	Failure mechanism	Probability estimate (events/yr)
Overheat event	<p>Given a specifically sized small-break loss-of-coolant accident (LOCA), a failure to initiate reactor coolant system cooldown via the steam generator, <i>and/or</i> depressurize the reactor via the pressurizer power-operated relief valve (PORV) <i>or</i> the auxiliary spray system can potentially cause core uncover.</p> <p><u>Condition for Operation:</u> Shutdown after a small-break LOCA.</p>	<p>A failure to initiate or maintain reactor coolant system cooldown can be caused by atmospheric dump valves (ADV's) and/or the turbine bypass valves (TBV's) failing to open on demand, or closing indirectly as a result of a safety injection actuation signal <i>and</i> an operator error.</p> <p>A failure of the instrument air system or a loss of power to bus Y09 can prevent the ADV's and TBV's from opening (these have much lower probabilities than the mechanism above).</p> <p>A failure to depressurize the reactor coolant system can result from the lack of procedural instructions to initiate this mode under saturated RCS conditions.</p>	9E-6**
Overcool event	<p>Given a small-break LOCA <i>and</i> reactor coolant system cooldown is initiated, if the operator fails to open either pressurizer PORV or initiate auxiliary spray, a pressurized thermal shock could result in damage to a vulnerable pressure vessel.</p> <p><u>Condition for Operation:</u> Shutdown after a small-break LOCA.</p>	Operator error <i>or</i> a failure of the pressurizer PORV's or auxiliary spray system.	1.5E-4†

\*Includes 0.1/demand probability that the operator fails to manually trip the main feedwater pumps in time to prevent overflow.

\*\*Includes multiple operator failure probabilities (that is, failure to initiate reactor coolant system (RCS) cooldown via the steam generator (0.01/demand) *and* failure to depressurize the RCS via pressurizer PORV's or auxiliary spray system (0.5/demand).

†Includes 0.01/demand probability that the operator fails to open the pressurizer PORV when indicated. It does not include the conditional probability of vessel failure due to pressurized thermal shock (PTS) conditions.

## 4 GENERIC APPLICABILITY

Reference plants were selected on the basis of (1) the quality and quantity of design information available to conduct a review and (2) the belief that any weaknesses in control system designs were more likely to be identified in older plants.

A number of control system failures having the potential for causing undesirable events were identified at the reference plants. To determine if the results obtained for the reference plants were applicable to other plants supplied by the same vendor, similarities in the thermal-hydraulic parameters and similarities in control systems of other plants were evaluated. This evaluation of control systems (similarity review) of other plants focused primarily on those design characteristics identified as contributing to the events of concern. Sensitivity studies were selectively performed to evaluate if the differences were significant. The significant transients analyzed for the reference plants were also evaluated to determine (1) if similar transients could occur in other plants and (2) if the transients analyzed for the reference plant represented a more severe or bounding transient.

Results of the review of the reference plants were considered generically applicable to the same vendor's other plants if:

- (1) Major fluid systems of other plants were functionally similar to the reference plant.
- (2) Ratio of power to volume and various ratios of volume to flow of other plants were similar to the reference plant.
- (3) Thermal-hydraulic transients analyzed at the reference plant were similar to or would bound transients on other plants of the same class.
- (4) Control systems at other plants were sufficiently similar to the reference plants so that any differences in the design were not significant enough to substantially alter the events of concern.
- (5) Reactor protection systems (that is, the reactor trip systems and the engineered safety features systems) at other plants are functionally similar to the reference plants so that any differences in the design of the reactor protection system were not significant enough to substantially alter the events of concern.

A large number of single and multiple control system failures were analyzed for the reference plants. It was not necessary or practical to evaluate all possible control system failure combinations that could occur in any one plant. Engineering judgment and the failure modes and effects analysis (FMEA) conducted on each plant were

used to limit the number and kind of transient analyses performed. Selection of the type and number of system failures evaluated for the plant model was an iterative process highly dependent on the knowledge gained from responses to the failure sequences simulated in previous analyses. In some cases, highly unlikely combinations of multiple failures were evaluated to assess worst-case or bounding scenarios. On the basis of the combinations and number of control system failures analyzed, it became apparent that as long as the protection systems were not compromised and performed their intended design functions, the events (except those noted below) induced by control failures were satisfactorily mitigated. On the basis of the number of credible and unlikely failures evaluated, the staff concluded that other control system failures that could occur at the reference plant (but have not been analyzed in this review) would also be mitigated by the protection systems. Since the designs of the reactor protection systems of other plants (of the same vendor) are functionally similar to the reference plant designs, the same degree of protection to mitigate multiple control system failures is provided in other plants.

It should be noted that a few plant designs vary significantly from the reference plant designs. These plants incorporate unique design features in major fluid systems and/or instrumentation and control systems, power systems, or reactor protection systems which have not been evaluated in detail. For BWRs these plants are: Oyster Creek Nuclear Power Plant, Unit 1; Big Rock Point Nuclear Plant; Nine Mile Point Nuclear Station, Unit 1; La Crosse Nuclear Generating Station; Millstone Nuclear Power Station, Unit 1; and Dresden Nuclear Power Station, Units 2 and 3. For the W PWRs, the plants are: Yankee Rowe Nuclear Power Station, Haddam Neck Plant, and San Onofre Nuclear Generating Station, Unit 1. For CE PWRs, the plants are: Arkansas Nuclear One, Unit 2; San Onofre Nuclear Generating Station, Units 2 and 3; Maine Yankee Atomic Power Plant; and Palo Verde Nuclear Generating Station, Units 1, 2, and 3. For B&W PWRs, the plants are Arkansas Nuclear One, Unit 1; Crystal River Nuclear Plant; Rancho Seco Nuclear Generating Station, Unit 1; and Davis-Besse Nuclear Power Station, Unit 1. The major differences in these designs and their effects on the significant events are discussed below. Most of the events identified during the Unresolved Safety Issue (USI) A-47 review were found to be generically applicable to most other reactors of the same class. Some events, however, were determined to be applicable only to the reference plant.

The following discussions assess the generic applicability of the events determined to be safety significant during the review. Design features of other plants that could

potentially modify failure scenarios or transients analyzed in this review are described and the criteria used to assess generic applicability are identified. This assessment is based on fundamental engineering principles, the generic evaluations conducted by ORNL and INEL (see NRC reports NUREG/CR-3991, -4047, -4262, -4265, -4326 and Letter Report ORNL/NRC/LTR-86-19), and staff judgment.

## 4.1 GE BWR Plants

Several control system failures that could contribute to reactor vessel overfill and reactor overcooling events were identified as potentially safety significant. All other control system failures that were evaluated were determined to be bounded by the FSAR analyses. The failure mechanisms contributing to these events are identified in Table 3.1. Major contributors to events that occur during power operation were multiple control system failures that initiated overfeeding transients and failed the automatic feedwater pump trip system. Major contributors to events that occur during startup or shutdown operation were single and multiple failures that initiated vessel overfeeding.

The discussions that follow summarize the design features of other plants and assess the generic applicability of the major events identified for the reference plant.

### 4.1.1 Overfill Events at Power Resulting From Failures in the Reactor Vessel High-Water-Level Feedwater Trip System

#### Control System Differences

Review of the plant-specific safety analysis reports (SARs) and the docket files identified variations in the reactor vessel high-water-level feedwater trip systems that terminate reactor vessel overfill events in BWRs during power operation.

Most operating BWR plants provide commercial non-safety-related reactor vessel overfill protection identical to the reference plant; that is, a 2-out-of-3, high-water-level trip system with separate and independent electrical power supplies for each level sensor. Several plants however have overfill protection designs with less independence and reliability. These designs vary from a 1-out-of-1 or a 1-out-of-2, to a 2-out-of-2 reactor high-water-level feedwater pump trip. At some plants, logic separation and electrical power independence could not be verified. More-recent designs provide improved flexibility and redundancy by including a four-level sensor logic system, that is, a 1-out-of-2 taken twice. Three plants (Big Rock Point, La Crosse, and Oyster Creek) have no automatic

isolation of feedwater on a reactor vessel high-water-level signal and rely solely on the operator to mitigate an overfeeding event.

The relative benefits of the different high-water-level trip logic provisions were evaluated using the reference plant as a model. The risk reduction associated with the different trip systems was estimated (NUREG/CR-4387).

Safety benefits gained by providing additional reactor vessel water-level redundancy and independence to some existing feedwater trip systems are not significant. The estimated reduction in frequency of overfill events between plants that have some sort of automatic reactor vessel high-water-level feedwater trip system was not significant. For plants with no automatic feedwater trip system, the overfill frequency was estimated to be about 15 times more likely than for plants with automatic feedwater trip systems. In actual practice, the three BWR plants with no trip system have demonstrated better reliability because of the operator's role in controlling feedwater. Results and conclusions of analyses of the reference plant apply to other BWR plants if they meet the following criteria with respect to control system design:

- (1) The plant must have an automatic reactor vessel high-water-level feedwater trip system.
- (2) The trip system must be operable during power operation or administrative procedures must be implemented to ensure that manual feedwater trip can be accomplished in time to prevent overfill when the automatic feedwater trip system is not operable.

#### Thermal-Hydraulic Differences

Most BWR plant systems that could contribute to reactor vessel overfeeding and vessel overfill events are functionally similar. Although variations in the design exist in some plants, such as the number, type, and capacity of valves or pumps and the size of reactor vessels, these variations are not significant when the overall size of the plant is considered. Major systems are designed with roughly similar proportions so that the time to overfill at other BWR plants is expected to be very similar to or bounded by the time predicted for the reference plant. Several BWR plants identified above (p. 26) incorporate designs that differ from the reference plant design. These differences include: (1) different recirculation flow systems, (2) use of isolation condensers, (3) different power supply designs, and (4) use of different reactor vessel capacities.

These design differences (except for vessel size) would not change the results of the overfill transients analyzed for the reference plant. Although reactor vessel capacity (i.e., size) can affect plant response for overfill events, the ratio of feedwater flow to reactor vessel volume for these plants is smaller than the ratio for the reference plant so that the overfill transients at plants with larger reactor

## Applicability

vessel volumes (like La Crosse) are expected to occur more slowly than predicted for the reference plant.

The following criterion was used to assess the generic applicability of this overflow event at other plants: Ratios of power to flow, power to volume, and reactor feedwater flow to reactor vessel volume for other plants should be similar to the ratios for the reference plant. If the ratios vary, they should vary in the direction that causes the overflow transients to occur more slowly.

Plants with thermal-hydraulic characteristics that satisfied this criterion were determined to be similar to the reference plant.

### Conclusions

- (1) Most BWR plants provide automatic feedwater pump trip systems on high reactor vessel high-water level. (Only three plants do not have automatic feedwater pump trip on reactor vessel high-water level).
- (2) Variations in the design of the control system for automatic overflow protection exist in other BWRs. For plants with automatic overflow protection systems, variations in the design do not significantly modify expected failure estimates to reduce the frequency of overflow events that could result from control system failures.
- (3) Overflow events at plants with no automatic overflow protection are estimated to be 15 times more likely than at plants with automatic overflow protection. Operator action can significantly reduce this estimate.
- (4) Ratios of power to flow, power to volume, and reactor feedwater flow to reactor vessel volume at other BWR plants are sufficiently similar to these ratios for the reference plant so that the analysis conducted on the reference plant is considered a bounding analysis and is generically applicable to other BWR plants.

### 4.1.2 Overflow and Overcooling Events During Low-Pressure Startup and Shutdown Operations

#### Control System Differences

Various failures in the condensate system and in the low-pressure coolant injection (LPCI) and core spray (CS) systems were identified that could cause reactor vessel overfeeding events during low-pressure startup and shutdown operations.

Most BWR plants provide LPCI, CS, and condensate systems similar to systems in the reference plant design. Although variations in some control system designs exist, all

plants rely on the operator to terminate flow from these systems once they are initiated.

#### Thermal-Hydraulic Differences

Several plants provide fluid system designs that are different from the reference plant design. These differences are discussed in Section 4.1.1.

The differences in the major fluid systems in these plants (except for reactor vessel size) do not affect the overflow transients analyzed for the reference plant. For plants with larger reactor vessels, because the ratio of condensate flow and/or emergency core cooling system (ECCS) flow to the reactor vessel volume is smaller than these ratios for the reference plant, overflow transients for these plants are expected to be slower and less severe than the transients predicted for the reference plant.

The following criteria were used to assess the generic applicability of this event on other plants:

- (1) Ratios of power to flow, power to volume, and condensate flow or low-pressure ECCS flow to reactor volume should be similar to the values for the reference plant.
- (2) The fill rate of the condensate system or the ECCS is less than or about equal to the reference plant flow rates.
- (3) Administrative procedures are implemented to help ensure that manual trip can be accomplished to terminate condensate or ECCS flow in time to prevent overflow.

Plants that had thermal-hydraulic characteristics and administrative procedures satisfying these criteria were determined to be similar to the reference plant.

The risk associated with control failures that could lead to overflow events (estimated for the reference plant) was small. Because the variations in control system design for other plants were not significant enough to substantially increase these estimates, sensitivity studies of control systems contributing to this event at other BWR plants were not performed.

#### Conclusion

Ratios of power to flow, power to volume, and condensate flow or low-pressure ECCS flow to reactor volume at other BWR plants are similar enough to the reference plant so that the analysis conducted on the reference plant is considered a bounding analysis and is generically applicable to other BWRs.

## 4.2 W PWR Plants

The review of a W PWR plant identified several control system failures that could contribute to steam generator



overflow, reactor vessel overcooling, and reactor overpressure events. Several failures were also identified that could contribute to undesirable release (i.e., releases in excess of those calculated in the FSAR analysis for steam generator tube rupture [SGTR]) of radioactivity during an SGTR. All other control system failures that were evaluated were determined to be bounded by the FSAR analysis. The failure mechanisms that contribute to these events are identified in Table 3.2. Overflow events could be caused by either sustained operation of the auxiliary feedwater system or the main feedwater system. Overcooling events could be caused by failures in the steam dump control systems (i.e., steamline atmospheric dump valves or condenser steam dump system). Overpressure events could be caused by failures in the pressurizer power-operated relief valve (PORV) control system, failures of the letdown valves, and failures in the ECCS circuitry. Failures in the steamline pressure relief control systems could also contribute to excessive release of radioactivity during an SGTR.

The discussions that follow summarize the generic applicability of other W PWR plants to the major events identified in the reference plant.

#### 4.2.1 Overflow Events Resulting From a Sustained Operation of the Auxiliary Feedwater Flow

##### Control System Differences

On all W PWR designs, auxiliary feedwater (AFW) flow is automatically initiated when the main feedwater pumps are tripped. There are no automatic interlocks to terminate AFW flow when the water in the steam generator reaches a high level (except for Virgil C. Summer Nuclear Station, Unit 1). An overflow event similar to the reference plant event can occur unless the operator manually terminates the AFW flow. Analysis performed on the reference plant predicts onset of overflow occurring rapidly, requiring quick operator response to terminate the AFW flow.

Results and conclusions of analysis performed on the reference plant apply to other W PWR plants if they do not meet the following criteria with respect to control system design.

- (1) Automatic reduction of the AFW flow on steam generator high-water level is provided, or
- (2) Administrative procedures are implemented to give reasonable assurance that the AFW valves can be manually throttled in time to prevent overflow.

If other W PWR plants meet the above criteria, the analyzed failure modes would be less severe than for the ref-

erence plant and should not result in a steam generator overflow.

##### Thermal-Hydraulic Differences

Variations exist in the design of the AFW systems in other W PWR plants that would change the time to overflow.

New 4-loop designs and some 3-loop designs have devices (orifices or throttling valves) installed in the AFW lines. These devices restrict the flow into the steam generators so that a less severe overfeeding transient would result than analyzed for the reference plant. In addition, most 4-loop designs have split AFW headers, so only 50 percent of total AFW could flow into the faulted steam generator instead of 100-percent flow for the 3-loop reference plant design.

The following criterion was used to assess the generic applicability of this event on other plants: The ratio of steam generator volume to main feedwater flow rate and the ratio of steam generator volume to the auxiliary feedwater flow rate should be similar to or greater than these ratios for the reference plant.

Plants with thermal-hydraulic characteristics satisfying this criterion were determined to be similar to the reference plant.

Some W PWR plants identified above (p. 26) incorporate designs that are different from the reference plant. These design differences include: (1) large cooling capacity of the reactor coolant system so that the ratio of the steam generator volume to the main or auxiliary feedwater flow is significantly greater than the reference plant design; (2) the use of charging pumps (i.e., high-pressure injection pumps) that have a higher pressure capability than the reference plant design; and (3) main steam systems that have no main steam isolation valves. These design differences would not change the results of the overflow events analyzed for the reference plant with the exception of plants with larger reactor vessel volumes. For those plants, less-severe overflow events are expected.

Although other differences, such as operator training and procedures, the design of the level-indication system, and alarms available to the operator, will alter the operator response time to address an overfeeding event, the review did not identify any plants that would have more-severe overflow transients.

##### Conclusions

- (1) Overflow events via the AFW system can occur at other W PWR plants under similar conditions analyzed in the reference plant (except for the Virgil C. Summer plant which has automatic termination of AFW).
- (2) The overflow transients via the AFW system at other W PWR plants are determined to be equal to or less



## Applicability

severe than those analyzed for the reference plant (except for the Virgil C. Summer plant which has automatic termination of AFW).

- (3) Ratios of steam generator volume to main feedwater flow rate and steam generator volume to AFW flow rate at other W PWR plants are so similar to reference plant ratios that the overfill analysis conducted at the reference plant is considered a bounding analysis applicable to other W PWR plants. Although several plants provide different designs, so that some of the thermal-hydraulic characteristics mentioned above are different from the reference plant, the differences are such that the transients would be equivalent to or less severe than the results of the overfill events analyzed for the reference plant.

### 4.2.2 Overfill Events Resulting From Failures in the Steam Generator High-Water-Level Feedwater Trip System

#### Control System Differences

All of the overfill-protection system designs at W PWR plants (except for three very early plant designs, i.e., Haddam Neck, Yankee Rowe, and San Onofre 1) have either a 2-out-of-3 or a 2-out-of-4 steam generator high-water-level trip system to terminate the feedwater flow during a feedwater overfeeding event. These systems are redundant and designed to satisfy safety requirements. The newer designs incorporate a more flexible and redundant 2-out-of-4 system that provides additional improvements for testing and fully satisfies all the prescribed safety requirements of IEEE Std. 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations." San Onofre 1 and Yankee Rowe plants do not have automatic overfill protection. The Haddam Neck plant provides an overfill-protection system consisting of a safety-related, 1-out-of-2 steam generator high-water-level interlock which automatically shuts the main feedwater control valves to the steam generator. Results and conclusions of the reference plant apply to other W PWR plants if they meet the following criteria with respect to control system design:

- (1) The plant must have an automatic steam generator high-water-level feedwater trip system similar to or better than the reference plant design has.
- (2) The trip system must be operable during power operation or administrative procedures must be implemented to provide reasonable assurance that a manual feedwater trip can be accomplished in time to prevent overfill when the automatic feedwater trip system is inoperable.

#### Thermal-Hydraulic Differences

The following criterion was used to assess the generic applicability of this event to other W PWR plants: The ratio of steam generator volume to main feedwater flow rate should be similar to or greater than that of the reference plant.

Plants with thermal-hydraulic characteristics satisfying this criterion were determined to be similar to or bounded by the reference plant.

Some W PWR plants identified above (p. 26) incorporate designs that differ from the reference plant. These differences would not adversely change the results of the overfill events analyzed for the reference plant. Less-severe overfill events are expected for plants with larger steam generator volumes. Although other differences, such as operator training and procedures, the design of the level indication system, and alarms available to the operator, can alter the operator response time to an overfeeding event, the review did not identify any plants that would have more severe overfill events.

#### Conclusions

- (1) Variations in the design of the automatic overfill-protection system exist in other W PWR plants. The designs are the same as or better than the reference plant design (except as noted for three very early plant designs).
- (2) Overfill transients in other W PWR plants are judged to be equal to or less severe than those analyzed for the reference plant.
- (3) The ratio of steam generator volume to main feedwater flow rate at other W PWR plants is so similar to the reference plant ratio that the overfill analysis conducted on the reference plant is considered a bounding analysis applicable to other W PWR plants. (Although several plants provide different designs so that some of the thermal-hydraulic characteristics discussed above are different from the reference plant characteristics, these differences do not change this conclusion.)

### 4.2.3 Overcooling Events During Hot Shutdown and Full-Power Operation

#### Control System Differences

Several control system failures were identified that could cause the steam dump valves to the condenser or the atmospheric dump valves (ADV) to open. These failures can result in reactor vessel overcool events during full-power operation or hot-shutdown conditions.

All W PWR plants utilize similar ADV and condenser-steam dump valve control systems. Although the number

of valves and valve capacities of these systems may differ at other W PWR plants, the overall valve capacity for 2-, 3-, and 4-loop plants is proportional to the plant's power level. Transients resulting from failures in these systems at other W PWR plants were determined to be similar to those analyzed for the reference plant.

A majority of operating plants and plants under review for an operating license (i.e., 37 out of 52 W PWR plants) have incorporated lead/lag-compensated steamline pressure measurement in the steamline-break-protection systems. This control system can terminate steam flow through the steam dump valves to the condenser by isolating the main steamlines on a low steamline pressure signal. This control design feature is not provided for the reference plant and represents an improvement over the reference plant design. For W PWR plants utilizing this feature, overcooling transients resulting from inadvertent opening of steam dump valves downstream of the main steam isolation valves (MSIVs) will be less severe than transients predicted for the reference plant.

In addition, most operating plants as well as plants of newer designs utilize arming circuits in the steam dump valve control system similar to circuits in the reference plant design. Multiple independent failures in these systems, similar to those postulated for the reference plant, are needed to cause all the steam dump valves to fail open. The initiating frequency for such failures is very low.

Although one plant design (San Onofre Nuclear Generating Station, Unit 1) does not have MSIVs or a lead/lag-compensated steamline pressure control system, it does utilize arming circuits similar to those of the reference plant to prevent inadvertent opening of the dump valves.

Results and conclusions of analyses of the reference plant apply to other W PWR plants if they meet the following criteria with respect to control system designs:

- (1) Must automatically terminate the steam flow through the steam dump valves to the condenser by isolating the main steamlines on low steamline pressure (that is, must have a lead/lag-compensated steamline pressure control system, or equivalent) or
- (2) Multiple independent control failures are needed to open all steam dump valves to the condenser (that is, provide arming circuits in the steam dump valve control systems similar to those in the reference plant).
- (3) Administrative procedures are implemented to ensure that (a) the ADVs can be manually isolated in time to prevent severe overcooling or (b) multiple independent failures are required to open more than one ADV.

### Thermal-Hydraulic Differences

Most W PWR plant systems that can contribute to reactor vessel overcooling transients are functionally similar. Although variations in the design exist at some plants (such as the number, type, and capacity of valves, and the number of steam generators), the variations are not significant when one considers the size of the plant. Major systems are sized in roughly the same proportions so that the overcooling transients on other W PWR plants are expected to be similar to or bounded by transients analyzed for the reference plant. Several W PWR plants identified above (p. 26) incorporate designs that differ from the reference plant. Plants that have larger reactor vessel and steam generator volumes, like Yankee Rowe Nuclear Power Station, have larger cooling capacities and larger ratios for reactor coolant system volume to atmospheric dump valve (or steam dump valve) capacity and steam generator volume to atmospheric dump valve (or steam dump valve) capacity. Overcooling transients resulting from inadvertent opening of the steamline PORV or steam dump valves to the condenser at these plants would be less severe than transients analyzed at the reference plant.

The following criteria were used to assess the generic applicability of this event at other W PWR plants: Ratios of (1) reactor coolant system volume to atmospheric or condenser-steam dump valve capacity and (2) steam generator volume to atmospheric or condenser-steam dump valve capacity ratios should be similar to or greater than these values for the reference plant.

Plants with thermal-hydraulic characteristics satisfying these criteria were determined to be similar to or bounded by the reference plant.

### Conclusions

- (1) All W PWR plants provide adequate control systems to prevent overcooling transients resulting from inadvertent opening of the steam dump valves to the condenser. Most plants provide overcooling transient protection that is better than that of the reference plant.
- (2) Transients that could occur as a result of inadvertent opening of the steam dump valves to the condenser or atmospheric dump valves are expected to be equal to or less severe than those analyzed for the reference plant.
- (3) Ratios of (a) reactor coolant system volume to atmospheric dump valve or (b) steam dump valve capacity and steam generator volume to ADV or steam dump valve capacity at other W PWR plants are sufficiently similar so that the overcooling analysis conducted for the reference plant is a bounding analysis applicable to other W PWR plants.

Although several plants provide such different designs that some of the thermal-hydraulic characteristic discussed above differ from those of the reference plant, the differences would cause less-severe transients and therefore do not adversely change the results of the overcooling events analyzed for the reference plant.

### 4.2.4 Overpressure Events During Low-Temperature and Low-Pressure Shutdown or Startup Operating Conditions

Several control system failures were identified that could prevent pressurizer PORVs from opening. These failures in conjunction with events that would increase reactor coolant system (RCS) pressure can result in reactor vessel overpressure events.

#### Control System Differences

Pressurizer PORV control systems at all W PWR plants are designed to conform to NRC Branch Technical Position RSB 5-2 (Denton, July 23, 1985) which requires the control systems for the pressurizer PORV valves to satisfy the single-failure criterion and to be powered from reliable independent power supplies (not necessarily Class 1E). Some new plants improve their control systems over the reference plant design by designing pressurizer PORV control systems that conform fully to all the requirements of safety-related systems, so that additional failures would be needed to produce the transients analyzed for the reference plant. Control system designs at other W PWR plants are, therefore, very similar to or better than the reference plant designs.

- (1) Results and conclusions of the analysis of the reference plant apply to other PWR plants if they meet the following criteria with respect to control system design:
  - (a) Pressurizer PORVs must be powered by reliable and independent power supplies and must be designed so that multiple independent failures are required to disable both PORVs.
  - (b) Administrative procedures are implemented to ensure that when one of the redundant pressurizer PORVs is rendered inoperable for a limited period of time during low-temperature operations, the remaining PORV can be opened manually.

Operator-induced procedural failures could also prevent both PORVs from opening during low-temperature and low-pressure conditions. These procedural failures are dependent on the adequacy of procedures used. Operating procedures at other plants were not reviewed to determine how many plants

may be susceptible to the kind of procedurally induced conditions analyzed in the reference plant review. Variations in procedures at other plants could affect the frequency and severity of this procedurally induced transient. The emphasis placed on PORV-related events since the TMI-2 accident, however, has made more operators more aware of this type of transient.

- (2) Results and conclusions of the analysis of the reference plant apply to other PWR plants if they meet the following criteria:
  - (a) The low-temperature overpressure (LTOP) system is removed from service during plant heatup before the RCS temperature is at or near the minimum pressurization temperature so that an LTOP condition can occur, or
  - (b) The ECCS is enabled during plant heatup before the RCS temperature is at or near the minimum pressurization temperature for the reactor vessel, or
  - (c) No other automatic pressure reduction capabilities exist to limit overpressure transients during low-temperature operations.

Under certain conditions, PWR plants are allowed to operate under limiting conditions for operation (LCO), wherein a redundant pressurizer PORV may be rendered inoperable for a finite period. If, during this time, the system is subjected to a pressure transient, the plant may be vulnerable to an overpressure event if a single failure in the available PORV control system can render the overpressure-protection system inoperable. This scenario has been identified as a safety issue. Generic Issue 94 was identified to reevaluate the existing LTOP designs and to assess the need for additional improvements to the low-temperature overpressure-protection system. This study is applicable to all PWRs that have PORVs (Denton, July 23, 1985). By resolving this issue, insights may be gained to warrant modifications.

#### Thermal-Hydraulic Differences

Because the major systems at W PWR plants are of roughly the same proportions, the overpressure transients at all W PWR plants are expected to be similar to or bounded by transients analyzed for the reference plant. Several W PWR plants identified (p. 26) incorporate some designs that differ from the reference plant design. These differences, discussed in Section 4.2.1 (except for plants that have high-capacity injection pumps), would not adversely change the results of the overpressure transients analyzed for the reference plant. For plants that utilize high-capacity injection pumps (higher than the reference plant design, like San Onofre Nuclear Generating Station, Unit 1), the overpressure transients induced by

inadvertent initiation of the high-pressure injection could produce a more-severe overpressure event than analyzed. Additional administrative procedures are used at these plants to lock out the isolation valves to the high-head pumps during shutdown conditions to preclude such events so that additional independent failures would be required to cause similar or more-severe events than analyzed for the reference plant. The following criteria were used to assess the generic applicability of these events to other W PWR plants:

- (1) The ratio of RCS volume to normal cold shutdown letdown flow rate should be similar to or greater than that of the reference plant.
- (2) Administrative procedures are implemented during startup or low-temperature, low-pressure operation to ensure that the pressurizer PORV low-pressure setpoint is not changed to the higher setpoint for normal operation before reaching the minimum pressurization temperature, or
- (3) Other automatic pressure-reduction capabilities exist to limit the overpressure transients during LTOP operation.

#### Conclusions

- (1) Most pressurizer PORV control system designs at other W PWR plants are very similar to designs of the reference plant. The designs provide similar electrical independence.
- (2) A few plants have better PORV control systems than the reference plant has, so additional multiple independent failures would be needed to produce similar scenarios analyzed for the reference plant.
- (3) The thermal-hydraulic analyses conducted for the reference plant are applicable to other W PWR designs.
- (4) Plants whose high-head injection pumps have a capacity higher than that of the reference plant provide additional lockout devices to prevent inadvertent initiation of the injection pumps during low-temperature operation.

#### 4.2.5 Control System Failures Aggravating a Steam Generator Tube Rupture Event

Several control system failures were identified that could cause inadvertent opening (or failure to close once challenged) of the atmospheric steamline dump valves during an SGTR event. An ADV that fails to reclose during an SGTR event can result in more severe transients than those previously analyzed by W for an SGTR event.

All W PWR plants provide steamline ADV designs similar to that of the reference plant design. They rely on the operator to isolate the flow through these valves should the valves fail to close during an SGTR event. Although the design of the ADVs may vary at other plants, these variations are not sufficient to modify the analysis performed for the reference plant design.

Results and conclusions of the analysis for the reference plant apply to other W PWR plants if they meet the following criteria with respect to control system design:

- (1) must have electrically initiated air-operated ADVs
- (2) require manual operator action to isolate flow through the ADVs

#### Conclusion

Transients at other W PWR plants that could occur as a result of inadvertent opening of the steamline ADVs are expected to be equal to or less severe than those analyzed at the reference plant.

### 4.3 B&W PWR Plants

The review of the B&W PWR reference plant identified potentially significant control system failures that could contribute to steam generator overfill events and reactor core overheating events. All other control system failures that were evaluated were determined to be bounded by the FSAR analysis. The failure mechanisms that contribute to these events are identified in Table 3.3.

The major contributors to these events were single and multiple control system failures that (1) initiated overfeeding transients and failed the automatic feedwater pump trip system that would have terminated an overfill event and (2) caused a loss of electrical power to various sections of the integrated feedwater control system resulting in a feedwater underfeeding condition that could lead to core overheating if proper operator action were not initiated.

It should be noted that about half of the B&W PWR plants currently operating incorporate an "820" integrated control system rather than a "721" integrated control system design utilized by the reference plant. Although these two control systems are functionally similar, they differ significantly in the power supply configuration. Design differences, such as providing additional independence and power supply separation, were implemented by the individual utilities on the 820 systems in order to improve system reliability on a loss of power. However, for this review, the 721 and the 820 systems were not compared in depth. To address the different transients resulting from a loss of power to the integrated control system (and other control systems), Bulletin 79-27 was issued by NRC's Office of Inspection



and Enforcement to all licensees. The bulletin required all licensees to take certain action to ensure the adequacy of plant procedures for accomplishing cold shutdown upon a loss of power to any Class 1E or non-Class 1E bus supplying power for instruments and controls in systems used in attaining cold shutdown. The licensee's response and design modifications to comply with Bulletin 79-27 were considered and evaluated in the review of the reference plant. The staff did not verify satisfactory compliance with this bulletin for all other plants.

The discussions that follow summarize the generic applicability of the major transients identified in the reference plant to other B&W PWR plants.

### 4.3.1 Overfill Events Resulting From Failures in the Steam Generator High-Water-Level Main Feedwater Trip System

#### Control System Differences

Review of the main feedwater control systems at all B&W operating PWR plants and all new B&W designs currently under review for operating licenses indicates that the 2-out-of-2 steam generator, high-water-level main feedwater trip system provided on the reference design is plant unique and not generically applicable. All other B&W operating PWR plants have installed or have committed to install safety-related overfill-protection systems that will satisfy the single-failure criterion. (Arkansas Nuclear One, Unit 1, implemented the new design in 1986; Rancho Seco Nuclear Generating Station, Unit 1, installed its system in 1988; Three Mile Island Nuclear Station, Unit 1, installed its system in 1987; and Crystal River Nuclear Plant, Unit 3, installed its system but has not yet implemented the trip system. It should also be noted that for the Bellefonte and WNP-1 plants overfill protection will be provided by high steam generator differential pressure (i.e., water level) when reactor power is below 31 percent and by excessive feedwater flow when reactor power is above 25 percent. Power dependence will be removed from the water level trip after a reactor trip is initiated.) The initiating logic for these designs is either a 2-out-of-4 or a 1-out-of-2 taken-twice, steam generator high-water-level main feedwater trip system. The trip system actuates redundant main feedwater isolation systems consisting of a main feedwater pump trip and a main feedwater isolation or control valve trip. One plant design currently under review for an operating license will use a safety-related 2-out-of-3, high-water-level main feedwater trip system. These plants provide (or will provide) additional redundancy, independence, and testing flexibility in their steam generator overfill-protection system and they are expected to represent a significant

improvement over the reference plant design when the installation is complete.

Results and conclusions of analyses of the reference plant apply to other B&W PWR plants if they meet the following criteria with respect to control system design:

- (1) The automatic overfill protection is at least as reliable as the reference plant design. A single failure in the overfill-protection system for the reference plant can negate the automatic overfill-protection system.
- (2) The main feedwater trip system must be operable during power operation, or administrative procedures must be implemented to ensure that manual feedwater trip can be accomplished in time to prevent overfill when the automatic feedwater trip system is not operable.

#### Thermal-Hydraulic Differences

Most B&W PWR plant systems that could contribute to steam generator overfeeding and overfill events are functionally similar. Variations in the designs exist at some plants, such as the type and capacity of main feedwater valves or pumps; these variations are not significant when considering the overall size of the plant. Major systems are sized in roughly the same proportions so that the time to overfill on other B&W PWR plants is expected to be very similar or is bounded by the time predicted for the reference plant.

The following criterion was used to assess the generic applicability of this event to other plants: The ratio of steam generator volume to main feedwater flow rate and the ratio of steam generator volume to the auxiliary feedwater flow rate should be similar to or greater than those of the reference plant.

Plants with thermal-hydraulic characteristics satisfying this criterion were determined to be similar to the reference plant.

#### Conclusions

- (1) Control systems for overfill protection for the main feedwater system for the reference plant is plant specific to Oconee Unit 1. The control systems for overfill protection are not as reliable as those provided or planned to be provided at all other B&W PWR plants.
- (2) All other B&W PWR plants provide (or have committed to provide) improved safety-related control systems for steam generator overfill-protection systems for the main feedwater system. These systems consist of either a 2-out-of-4 or a 1-out-of-2 taken twice or a 2-out-of-3 steam generator high-water-level trip. Although there are theoretical reliability



differences between these systems, these differences are outweighed by the improvements in overall reliability and operational flexibility allowed by such systems. All are thus adequate for overfill protection. It should be noted that until these modifications are completed some of the plants are currently operating with no overfill protection.

- (3) Ratios of steam generator volume to main feedwater flow rate and steam generator volume to auxiliary feedwater flow rate at other B&W PWR plants are similar to the reference plant ratios; thus the overfill analysis conducted on the reference plant is a bounding analysis applicable to other B&W PWR plants.

### 4.3.2 Overheating Events Resulting From Steam Generator Dryout

Several control system failure scenarios were identified that could result in steam generator dryout on a partial loss of electrical power to the feedwater control system. Such events could lead to reactor core overheating if adequate feedwater flow is not established within 30 minutes of a steam generator dryout and high-pressure injection (HPI) is not initiated within 60 minutes. Losses of electrical power to the "hand control" (i.e., manual control) circuit during the manual mode of operation or to the "auto control" circuit during the automatic mode of operation were identified as major contributors.

#### Control System Differences

Half of the operating B&W PWR plants have an 820 integrated control system rather than the 721 integrated control system used at the reference plant. Only four plants (Oconee Nuclear Station, Units 1, 2, and 3, and Three Mile Island Nuclear Station, Unit 1) use 721 systems. Electric power distributions in the 820 system are different from the distributions in the 721 system. The 820 system was not reviewed in detail to determine if a credible partial loss of power to the integrated control system could cause similar events; however, all other plants (including TMI-1) incorporate separate control circuits that automatically initiate auxiliary feedwater flow on low-water level in the steam generator. These circuits represent an improved design that mitigates a steam generator dryout scenario postulated for the reference plant.

Results and conclusions of analyses of the reference plant apply to other B&W PWR plants if they meet the following criterion with respect to control system design: Auxiliary feedwater flow is not automatically initiated on low-water level in the steam generator. (Plants in which AFW is automatically initiated on low-water level in the steam generator are less susceptible to steam generator dryout

and, therefore, represent an improvement over the reference design.)

#### Thermal-Hydraulic Differences

Variations in the designs exist at some plants, such as type and capacity of the feedwater valves or pumps. These variations are not significant when considering the overall size of the plant. Major systems are sized in roughly the same proportions so that the time of steam generator dryout at other B&W plants is expected to be similar to or bounded by the time to dryout predicted for the reference plant. The following criteria were used to assess the generic applicability of this event to other B&W plants:

- (1) The ratios of steam generator volume to main feedwater flow rate and steam generator volume to the auxiliary feedwater flow rate should be similar to these values for the reference plant.
- (2) The ratio of power to volume should be similar to this value for the reference plant.

Plants with thermal-hydraulic characteristics satisfying these criteria were judged to be similar to the reference plant.

#### Conclusions

- (1) All other B&W PWR plants provide control system designs to initiate auxiliary feedwater on steam generator low-water level to prevent steam generator dryout on loss of main feedwater. This design feature represents an improvement over the reference plant design.
- (2) Ratios of power to flow, power to feedwater flow rate, and steam generator volume to main feedwater flow at other B&W PWR plants are similar to values for the reference plant; thus the steam generator dryout analysis conducted for the reference plant is similar to or is a bounding analysis for other B&W PWR plants.
- (3) The overheating event scenario analyzed for the reference plant is not directly generically applicable but bounds overheating events at other B&W PWR plants.

### 4.4 CE PWR Plants

The review of the CE PWR reference plant identified several potentially significant control system failures that could contribute to (1) steam generator overfill events, (2) a reactor core overheating event, and (3) an overcooling event that could lead to a potential pressurized thermal shock event in a plant with a vulnerable pressure vessel.

All other control system failures that were evaluated were determined to be bounded by the FSAR analysis.

The failure mechanisms that contributed to these events are identified in Table 3.4.

The major contributors to these events were (1) single and multiple control system failures that initiated overfeeding transients or prevented atmospheric dump valves or turbine bypass valves from opening on demand and (2) incorrect operator actions to open the pressurizer PORVs when needed.

The sections that follow summarize the generic applicability of the major transients identified in the reference plant to other CE PWR plants.

### 4.4.1 Overfill Events Resulting From Operator Errors During a Steam Generator Overfeeding Event

#### Control System Differences

On all CE PWR plant designs, no automatic steam generator high-water-level signals trip the main feedwater pumps. If an overfeeding event occurs, a steam generator high-water-level signal will automatically trip the main steam turbine. A turbine trip signal will trip the reactor, shut the feedwater valves, and open the startup feedwater valves to 5-percent flow.

This trip system can limit the frequency of steam generator overfill events, but operator action is still required to trip the main feedwater pumps to prevent overfill. If the operator does not manually trip the feedwater pumps, a single failure in the feedwater control system can cause the steam generator to overfill.

The results and conclusions of analysis on the reference plant apply to other CE PWR plants if they meet the following criterion with respect to control system design: All main feedwater flow is not automatically isolated on a steam generator high-water-level signal. Plants with automatic overfill-control circuits would be more resistant to overfill transients than the reference plant would be.

#### Thermal-Hydraulic Differences

Variations in design exist at some plants. These variations include type and capacity of feedwater valves and pumps. These variations are not significant with regard to steam generator filling times when considering the relative size of the plants. Major systems are sized in roughly the same proportions so that the time to overfill at all other CE PWR plants is expected to be similar or bounded by the time to overfill predicted for the reference plant.

Several CE PWR plants incorporate designs that are different from the reference plant design. These design differences include (1) the use of charging pumps with a dis-

charge head higher than the reference plant design and (2) no pressurizer PORVs. These design differences would not change the conclusions for overfill events analyzed for the reference plant. Although other differences, such as operator training and procedures and design of the level indication system and alarms available to the operator, will alter operator response time to respond to an overfill event, the review did not identify any plants with characteristics that would cause more-severe overfill events.

The following criterion was used to assess the generic applicability of this event to other CE PWR plants: The ratio of steam generator volume to main feedwater flow rate and the ratio of steam generator volume to the auxiliary feedwater flow rate should be similar to or greater than these values for the reference plant.

Plants with thermal-hydraulic characteristics satisfying this criterion were determined to be similar to the reference plant.

#### Conclusions

- (1) The feedwater control system designs on all CE PWR plants are similar to feedwater control system design for the reference plant.
- (2) There are no automatic steam generator high-water-level feedwater-pump trip systems; manual operator action is required to trip the feed pumps or close isolation valves to prevent overfill.
- (3) The ratios of steam generator volume to main feedwater flow rate at all CE PWR plants are similar to such ratios at the reference plant; thus the overfill analysis conducted for the reference plant is considered applicable to other CE PWR plants.

### 4.4.2 Overheating Events and Possible Pressurized Thermal Shock Events Resulting From Operator Errors During Small-Break Loss-of-Coolant Accidents

Several failure scenarios were identified for specifically sized small-break loss-of-coolant accidents (SBLOCAs) that could lead to eventual core dryout and fuel damage if the operator does not take proper action to depressurize the reactor coolant system to (1) maintain adequate high-pressure injection flow or (2) avoid reaching  $R_{\text{T}}\text{NDT}$  (reference temperature nil ductility transition) limits.

#### Control System Differences

For the reference plant, manual operation of the atmospheric dump valves (ADVs) or the turbine bypass valves (TBVs) or both may be required to depressurize the

primary system during SBLOCAs to maintain adequate high-pressure injection flow. Operator use of the pressurizer PORVs or pressurizer auxiliary sprays could also be used to depressurize the primary system if the ADVs or the TBVs or both are not available or if the RPT NDT limits for the reactor vessel are exceeded. Failures that could keep the ADVs or the TBVs from opening on demand include loss of power or loss of instrument air to the valves. For the reference plant under LOCA conditions, a safety injection signal isolates service water flow to the air compressors that supply operation air to the ADVs and the TBVs. Loss of service water could result in a failure of the air system. This design is similar to the design of other CE PWR plants. Although an operator of the reference plant can manually transfer control of the ADV to the auxiliary shutdown panel and can provide air to the valves from the salt-water-cooled air compressor, emergency procedures for the reference plant do not instruct the operator to perform this task.

Results and conclusions of analysis of the reference plant apply to other CE PWR plants if they meet the following criteria with respect to administrative procedures or control system design:

- (1) Air supply to ADVs or to the TBVs is lost during SBLOCA conditions. (At the reference plant, automatic isolation of service water to instrument air compressors is initiated during LOCA conditions so that the ADVs or the TBVs are rendered inoperable. Plants that continue to supply instrument air to the ADVs under LOCA conditions are protected against this type of event.)
- (2) Administrative procedures do not clearly instruct the operators to provide operating air to the ADV or the TBVs from an alternate source in the event that service water flow is isolated to the main instrument air compressors (if administrative procedures exist, plants are less susceptible to overheating events of this type), and
- (3) An alternate compressed-air source to the ADVs or TBVs is available.

#### Thermal-Hydraulic Differences

Several CE PWR plants incorporate designs that are different from the reference plant design. These design differences include (1) the use of high-head safety injection pumps with higher heads than the reference plant has and (2) some CE PWR plants do not have pressurizer PORVs. The use of higher head injection pumps will significantly change the analyzed failure scenarios. Higher head pumps will be able to inject water into the reactor vessel at higher pressures, so that specifically sized SBLOCA events analyzed for the reference plant would be significantly less severe.

The following criterion was used to assess the generic applicability of this event on other CE PWR plants: The shutoff pressure of the high-head pumps should be similar to or less than the reference plant design safety injection.

Plants satisfying this criterion were determined to be similar to the reference plant. Plants with higher head safety injection pumps were determined to have less severe transients than analyzed.

#### Conclusions

- (1) Seven of the fifteen CE PWR plants have similar high-head pressure injection pump systems; thus failure scenarios analyzed on the reference plant are generically applicable.
- (2) Eight of the fifteen CE PWR plants have substantially higher high-head pressure injection pumps so that administrative procedures to depressurize the primary system are not as critical for these eight plants as for the reference plant.
- (3) Seven of the eight CE PWR plants that have high-head pressure injection pumps do not have pressurizer PORVs. For these plants, auxiliary pressurizer spray systems are used to control pressurizer pressure. This design difference does not significantly change the conclusions reached in item 2, above.

## 5 SUMMARY AND CONCLUSIONS

Before any safety issue can be resolved, the nature of the concern must be clearly described. Concerns described as general subject areas (such as common-cause failures, operator errors, sabotage, and undetected failures) can prove to be so broad that almost every conceivable safety issue could fall within the concern, and thus an issue would prove to be unmanageable. Therefore, to proceed with a resolution of the concern expressed as "safety implications of control systems," the NRC staff developed a set of limitations and assumptions to attempt to focus on the safety concern. The staff also decided to take advantage of other ongoing efforts. Thus, if some aspects that might be considered to have control system safety implications were better addressed by these other efforts, the scope of USI A-47 was modified, avoiding duplication of effort. As a result, a number of concerns (such as: (1) effects of seismic events on control systems, (2) dynamic effects on plant safety resulting from water entering the main steamlines, and (3) reduction in the frequency of integrated control-system-induced transients in B&W PWR plants) were left to be addressed outside the framework of the USI A-47 study. The limitations and assumptions identified in this report are crucial to understanding the scope of the issue and its resolution.

On the basis of the limitations and assumptions, a number of tasks were defined. These tasks were structured to: (1) make use of the operating experience of actual events, (2) take advantage of previous control system studies, (3) take advantage of the staff requirements identified in the TMI-2 Action Plan (NUREG-0660), (4) evaluate the safety significance of control system failures, and (5) evaluate the safety benefit and cost effectiveness of potential corrective measures.

Because the initiating events and the frequency of control system failures are for the most part plant specific, the risk estimates that are used to evaluate safety significance were difficult to extrapolate to other plants. The safety benefit derived for the reference plant and extrapolated to other plants is based both on qualitative insights and quantitative analysis. The generic applicability analysis is also based on qualitative analysis and deterministic arguments.

On the basis of the technical work completed by the staff and NRC contractors, the following conclusions have been reached:

(1) Control system failures are dependent on individual plant characteristics such as power supply configura-

tions and maintenance. The control system designs between the plants supplied by the same nuclear steam supply system (NSSS) vendor are functionally similar enough that the transients resulting from the failure of the same type of non-safety-related system on the different plants will produce similar transients (see Section 4, "Generic Applicability," for exceptions).

- (2) Control system failures have occurred that resulted in complex transients. Improvements made after the TMI-2 accident in the design of the auxiliary feedwater system and in operator information and training should greatly aid in the recovery actions in the future.
- (3) Plant transients resulting from control system failures can be adequately mitigated by the operators provided the failures do not compromise proper operation of the minimum number of protection system channels required to trip the reactor and initiate the safety systems if such initiation is required.
- (4) Control system failure scenarios have been identified that could potentially lead to reactor vessel/steam generator overfill events, core overheating events, and overpressure events.
- (5) Transients or accidents resulting from or aggravated by control system failures (except those noted in this report that can contribute to reactor vessel/steam generator overfill or core overheating events) are less severe and therefore are bounded by the transients and accidents identified in the FSAR analysis.
- (6) PWR plant designs having redundant commercial-grade (or better) overfill-protection systems that satisfy the single-failure criterion are considered to adequately preclude water entering the main steamlines.
- (7) BWR plant designs with commercial-grade (or better) overfill protection systems are considered to adequately preclude water entering the main steamlines.
- (8) PWR plant designs that provide automatic initiation of the auxiliary feedwater flow on steam generator low-water level are considered to adequately preclude core overheating.



## 6 REFERENCES

- Alter, J., and D. Okrent, "The Contribution of Control Systems in LWR Safety," University of California, Los Angeles, 1983.
- Babcock & Wilcox Owners Group, BAW 1564, "Integrated Control System Reliability Analysis," August 1979.
- Denton, H., NRC, Memorandum to R. Bernero, "Schedule for Resolving and Completing Generic Issue No. 94, 'Additional Low Temperature Overpressure Protection for Light Water Reactors'," July 23, 1985.
- Denton, H., Memorandum to V. Stello, "Staff Actions Resulting From the Investigation of the December 26, 1986 Incident at Rancho Seco (NUREG-1195)," April 25, 1986.
- Dircks, W., NRC, Memorandum to NRC Directors, "Staff Actions Resulting From the Investigation of the June 8, Davis-Besse Event (NUREG-1154)," August 5, 1985.
- Miraglia, F., NRC, Memorandum to NRR Directors, "Staff Actions Resulting From the Investigation of the December 26, 1986 Incident at Rancho Seco (NUREG-1195)," September 4, 1986.
- Stello, V., NRC, Memorandum to H. Denton, "Staff Actions Resulting From the Investigation of the December 26, 1986 Incident at Rancho Seco (NUREG-1195)," March 13, 1986.
- Tucker, H., BWO, Letter to D. Crutchfield, NRC, "B&W Owners Group Plant Reassessment," May 15, 1986.
- U.S. Nuclear Regulatory Commission, NUREG-0153, "Staff Discussions of Twelve Additional Technical Issues Raised by Responses to November 3, 1976 Memorandum From Director, NRR, to NRR Staff," December 1976.
- , NUREG-0460, "Anticipated Transients Without Scram for Light Water Reactors," Vols. 1 and 2, April 1978; Vol. 3, December 1978; Vol. 4, March 1980.
- , NUREG-0660, "NRC Action Plan Developed As a Result of the TMI-2 Accident," Vols. 1 and 2, May 1980.
- , NUREG-0667, "Transient Response of Babcock & Wilcox-Designed Reactors," May 1980.
- , NUREG-0737, "Clarification of TMI Action Plan Requirements," November 1980.
- , NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," LWR Edition, July 1981.
- , NUREG-0933, "A Prioritization of Generic Safety Issues," Main Report and Supplements 1-6, August 1987.
- , NUREG-1070, "NRC Policy on Future Reactor Designs," July 1985.
- , NUREG-1154, "Loss of Main and Auxiliary Feedwater Event at the Davis-Besse Plant on June 9, 1985," July 1985.
- , NUREG-1177, "Safety Evaluation Report Related to the Restart of Davis-Besse Nuclear Power Station, Unit 1, Following the Event of June 9, 1985," June 1986.
- , NUREG-1195, "Loss of Integrated Control System Power and Overcooling Transient at Rancho Seco on December 26, 1985," February 1986.
- , NUREG-1218 (Draft for Comment), "Regulatory Analysis for Proposed Resolution of USI A-47, Safety Implications of Control Systems," April 1988.
- , NUREG-1231, "Safety Evaluation Report Related to Babcock and Wilcox Owners Group Plant Reassessment Program," November 1987; Supplement No. 1, March 1988.
- , NUREG-1286, "Safety Evaluation Report Related to the Restart of Rancho Seco Nuclear Generating Station, Unit 1 Following the Event of December 26, 1985," October 1987; Supplement No. 1, March 1988.
- , NUREG/CR-3692 (ORNL/TM-9061), "Possible Modes of Steam Generator Overfill Resulting From Control System Malfunctions at the Oconee-1 Nuclear Plant," July 1984.
- , NUREG/CR-3958 (PNL-5767), "Effects of Control System Failures on Transients, Accidents and Core-Melt Frequencies at a Combustion Engineering Pressurized Water Reactor," March 1986.
- , NUREG/CR-3991 (ORNL/TM-9383), "Failure Modes and Effects Analysis (FMEA) of the ICS/NNI Electric Power Distribution Circuitry at the Oconee-1 Nuclear Plant," October 1985.



## References

- , NUREG/CR-4047 (ORNL/TM-9444), "An Assessment of the Safety Implications of Control Systems at the Oconee 1 Nuclear Power Plant, Final Report," March 1986.
- , NUREG/CR-4262 (EGG-2394), "Effects of Control System Failures on Transients and Accidents at a General Electric Boiling Water Reactor," Vols. 1 and 2, May 1985.
- , NUREG/CR-4265 (ORNL/TM-9640), "An Assessment of the Safety Implications of Control Systems at the Calvert Cliffs-1 Nuclear Plant," Vol. 1, Main Report, April 1986; Vol. 2, Appendices, July 1986.
- , NUREG/CR-4326 (EGG-2405), "Effects of Control System Failures on Transients and Accidents at a 3-Loop Westinghouse Pressurized Water Reactor," Vol. 1, August 1985; Vol. 2, October 1985.
- , NUREG/CR-4385 (PNL-5543), "Effects of Control System Failures on Transients, Accidents and Core-Melt Frequencies at a Westinghouse Pressurized Water Reactor," November 1985.
- , NUREG/CR-4386 (PNL-5544), "Effects of Control System Failures on Transients, Accidents, and Core-Melt Frequencies at a Babcock and Wilcox Pressurized Water Reactor," Pacific Northwest Laboratory, December 1985.
- , NUREG/CR-4387 (PNL-5545), "Effects of Control System Failures on Transients, Accidents, and Core-Melt Frequencies at a General Electric Boiling Water Reactor," December 1985.
- , NUREG/CR-4449 (ORNL/TM-9868), "A PWR Hybrid Computer Model for Assessing the Safety Implications of Control Systems," March 1986.
- , NUREG/CR-4758 (ORNL/TM-10236), "A RETRAN Model of the Calvert Cliffs-1 Pressurized Water Reactor for Assessing the Safety Implications of Control Systems," March 1987.
- , Office for Analysis and Evaluation of Operational Data, "AEOD Observations and Recommendations Concerning the Problem of Steam Generator Overfill and Combined Primary and Secondary Blow-down," December 17, 1980.
- , Office of Inspection and Enforcement, Bulletin 79-27, "Loss of Non-Class 1E Instrumentation and Control Power System Bus During Operation," November 30, 1979.
- , ORNL/NRC/LTR-86/19, Letter Report, "Generic Extensions to Plant Specific Findings of the Safety Implications of Control Systems (ORNL) Program."
- , SECY-82-465, "Pressurized Thermal Shock (PTS)," November 23, 1982.

## APPENDIX A

### OTHER RELATED STUDIES, PROGRAMS, AND ISSUES

A number of ongoing U.S. Nuclear Regulatory Commission (NRC) and industry programs are related to Unresolved Safety Issue (USI) A-47. These programs are discussed here and summarized in Table A.1.

#### (1) Generic Issues in NUREG-0933

As specifically identified in NUREG-0933, Generic Issues 70 and 94 dealing with overpressure protection may require modifications to existing control systems. The staff concluded that resolution of these issues should proceed via the more focused review specified for these generic issues.

#### (2) Seismic Qualification of Equipment in Operating Plants, USI A-46

Within the framework of ongoing NRC and industry programs, the seismic ruggedness and operability of control-grade and protection-grade design equipment during design-basis seismic events are being evaluated. Data from past experience during seismic events (including recent earthquakes in Chile and Mexico) are being evaluated to assess the seismic capability of electrical and mechanical equipment needed to safely shut down the plant. Equipment used in non-safety-related control systems that interact with safety-related equipment or that are used in achieving and maintaining hot shutdown are being evaluated to ensure that their operability (or lack thereof) does not compromise the plant's ability to achieve and maintain hot shutdown during or after a seismic event. All control system components and instruments are included in the USI A-46 scope by type if not explicitly reviewed. As part of the USI A-46 scope, the current review is evaluating two plant designs (i.e., Zion and Nine Mile Point Unit 1), focusing on equipment installation, its function, and its actual location. Once the methodology and review procedures are established, the review will extend to all other operating plants in the USI A-46 scope (which includes 70 operating plants).

#### (3) Reactor Vessel/Steam Generator Overfill

In separate evaluations, the staff is investigating the consequences of water entering the main steamlines resulting from overfeeding transients or steam generator tube rupture (SGTR) events. These evaluations include (a) analysis of the potential waterhammer conditions that could degrade steamline integrity, (b) assessment of the adequacy of existing emergency procedures for operator

actions needed to mitigate SGTR and prevent overfill, and (c) radiological offsite dose calculations from an SGTR event. These activities are being evaluated in the study of Generic Issue 135.

#### (4) Babcock & Wilcox (B&W) Design Reexamination

A comprehensive B&W Owners Group study (Tucker, May 15, 1986) was initiated to reassess all B&W pressurized-water-reactor (PWR) plant designs including, but not limited to, the integrated control system, support systems such as power supplies, and maintenance.

Of particular relevance to USI A-47 was the part of this reexamination that dealt with improving the reliability of the B&W PWR plants by (a) reducing the number of reactor trips caused by non-safety-related control and support systems or by operator or maintenance errors and (b) improving response to plant transients. The NRC staff monitored this comprehensive study. Recommended actions for design modifications, for maintenance, and for changes to operating procedures developed for the utilities by the owners group were coordinated with the staff through NRC's Division of Engineering and System Technology. The NRC staff assessment of the B&W Owners Group Plant Reassessment Program is documented in NUREG-1231 and Supplement No. 1 to that report, dated November 1987 and March 1988, respectively.

#### (5) Staff Actions Resulting From the Investigation of the December 26, 1985 Incident at Rancho Seco

Generic and plant-specific actions resulting from the investigation of the Rancho Seco incident (see NRC, NUREG-1195) were identified in part in a memorandum from V. Stello to H. Denton, dated March 13, 1986, and in a subsequent response memorandum, dated April 25, 1986. Several other memoranda have been issued subsequent to the April 25, 1986 response related to the identified issues. These memoranda are listed in the September 4, 1986 memorandum from F. Miraglia to the various directors of NRR. The activities discussed in these memoranda were pursued by the NRC staff and were requested to be evaluated by the B&W Owners Group (BWOOG). The major activities are summarized below:

- (a) Regarding completeness of actions taken with respect to BAW-1564 ("Failure Modes and Effects Analysis of the ICS") and the Oak Ridge National Laboratory (ORNL) review of it, the BWOOG has been asked to reevaluate BAW-1564

and to describe its plans to address the ORNL concerns. The staff evaluation is discussed in NUREG-1231, Supplement No. 1.

- (b) The staff initially asked the BWOG to reevaluate IE Bulletin 79-27 regarding the consequences of a loss of power to the instrumentation and control systems for all of the B&W-designed operating plants. Because of program constraints, the reevaluation of Bulletin 79-27 was removed from the BWOG scope and is now being conducted by the NRC staff. All B&W plants will be evaluated. The Rancho Seco plant evaluation has already been completed. This evaluation is presented in NUREG-1286, Supplement No. 1, March 1988. It is anticipated that the review of the other B&W plants will be completed by mid-1989.
- (c) With regard to atmospheric dump valves (ADVs) and turbine bypass valves (TBVs) opening on loss of integrated control system (ICS) power, the staff has met with the BWOG and determined that only Rancho Seco has the ADV problem and only Rancho Seco and Arkansas Nuclear One Unit 1 (ANO-1) have the TBV problem. Rancho Seco has already redesigned the ADV and TBV controls to eliminate the problem. The staff's evaluation is presented in NUREG-1286, Supplement No. 1. ANO-1 modified its TBV controls during the August 1986 refueling. The modified design prevents the TBV from automatically opening on a loss of power in the ICS.
- (d) The staff has conducted a survey of completeness of actions taken with respect to NUREG-0667 recommendations by the staff and by licensees of each B&W-designed operating reactor. The survey shows that 90 percent of the related staff requirements have been implemented. The Rancho Seco licensee and the BWOG have reviewed the recommendations as part of the Rancho Seco recovery and B&W-design reassessment programs. The staff's evaluation is provided in NUREG-1286 and NUREG-1231, Supplement No. 1.
- (e) In connection with the partial loss of the non-nuclear instrumentation (NNI) system at Rancho Seco in 1984, Rancho Seco staff and the BWOG have reviewed this event as part of the recovery and design reassessment programs. The staff's evaluation is provided in NUREG-1286 and in NUREG-1231, Supplement No. 1.

#### (6) Staff Actions Resulting From the June 6, 1985 Incident at Davis-Besse

Generic and plant-specific actions resulting from the investigation of the Davis-Besse incident (see NRC, NUREG-1154) have been identified in a memorandum from W. Dircks to the Directors of NRC, dated August 5, 1985. Short-term, plant-specific items have been addressed and the resolution is described in the "Safety Evaluation Report Related to Restart of Davis-Besse Nuclear Power Station" (see NRC, NUREG-1177). A number of potential generic issues were also identified. These issues include possible deficiencies in the design, construction, or operation of several or a class of nuclear power plants. The staff did not identify a need for any immediate staff action of a generic nature related to these issues. These issues have, however, been designated for review as part of Generic Issues 122 through 125. These issues are to be evaluated and resolved on a schedule consistent with their priority designation. Currently, the staff is completing the prioritization of these issues. Their status and priority level are provided in NUREG-0933. The staff is pursuing resolution of these issues on a separate schedule independent from the USI A-47 study.

#### (7) Systems Interactions (USI A-17)

Potentially undesirable interactions between plant systems, components, and structures were evaluated within the framework of the USI A-17 study. These evaluations include identification of interdependencies between safety-related protection systems and systems not related to safety, including non-safety-related control systems. The staff is pursuing resolution of this issue on a separate schedule independent from the USI A-47 study.

#### (8) Multiple Systems Response Program (MSRP)

A number of potential safety concerns were raised by the NRC staff and the Advisory Committee on Reactor Safeguards (ACRS) which were not covered by the existing USI programs (i.e., USI A-17, A-46, and A-47) or other safety issues (e.g., fire protection and environmental qualification). These concerns were identified because they were either: (a) outside the scope of the safety issue, (b) a spinoff from the existing issues, or (c) peripheral concerns for which additional review effort is thought necessary.

The MSRP was established to address these concerns and develop them as issues of sufficient detail that they may be evaluated, if needed, as new generic issues according to priority. This program is being pursued on a separate schedule independent from the USI A-47 study.

Table A.1 Summary of USI A-47 related studies, programs, and issues

Issue	Subject	Estimated completion schedule
GI-70	PORV and block valve reliability	Early 1989
GI-94	Low-temperature overpressure protection for light-water reactors	Early 1989
USI A-46	Seismic qualification of components	Mid-1991 (plant-specific implementation)
GI-135	Water entering main steamlines (overflow)	Late-1989
B&W plant reexamination	BWOG reevaluation to minimize challenges to protection systems and improve mitigation of complex transients	Completed in March 1988
Staff actions resulting from Rancho Seco Dec. 26, 1985 incident	Included as part of BWOG reevaluation	Completed in March 1988
Staff actions resulting from Davis-Besse June 6, 1985 incident	NUREG-1177 (short-term actions)	Completed in June 1986
	GI-122 (initiating feed and bleed)	Mid-1988
	GI-124 (AFW system reliability)	Mid-1988
	GI-125 (reevaluate design to automatically isolate feedwater from the steam generator)	Mid-1989
USI-A-17	Systems interactions	Mid-1989
Multiple Systems Response Program (MSRP)	Various potentially safety-significant subjects	To be determined on individual issues

## APPENDIX B

### SUMMARY OF THE PRINCIPAL DOCUMENTS USED FOR USI A-47 STUDY

The following are summaries of the principal documents underlying the resolution of Unresolved Safety Issue (USI) A-47.

- (1) Draft NUREG-1217, "Evaluation of Safety Implications of Control Systems in LWR Nuclear Power Plants, Technical Findings Related to Unresolved Safety Issue A-47."

This report presents the technical findings and summarizes the work performed on USI A-47 by the U.S. Nuclear Regulatory Commission (NRC) and its contractors: Pacific Northwest Laboratory (PNL), Idaho National Engineering Laboratory (INEL), and Oak Ridge National Laboratory (ORNL). Summaries and staff conclusions regarding other related work, such as generic applicability and operating experience survey, are also presented.

From the technical findings presented in this report, the staff formulated the resolution of USI A-47.

- (2) Draft NUREG-1218, "Regulatory Analysis for Proposed Resolution of USI A-47 Safety Implications of Control Systems."

This report presents a summary of the regulatory analysis conducted by the NRC staff to evaluate the value impact of alternatives for resolution of USI A-47. The resolution presented in this USI A-47 study is based on these analyses.

- (3) NUREG/CR-4262, "Effects of Control System Failures on Transients and Accidents at a General Electric Boiling Water Reactor" (Vols. 1 and 2). (See summary for NUREG/CR-4326.)

- (4) NUREG/CR-4326, "Effects of Control System Failures on Transients and Accidents at a 3-Loop Westinghouse Pressurized Water Reactor" (Vols. 1 and 2).

These two reports (numbers 3 and 4) summarize the work performed on USI A-47 by INEL. Summaries of failure modes and effects analysis, computer analysis, recorded plant occurrences, and probabilistic assessment of significant control system failure frequencies are provided. In addition,

the contractor presents its conclusions and recommendations.

From the technical findings presented in these two reports, the staff formulated the resolution of USI A-47 for General Electric and Westinghouse plants.

- (5) NUREG/CR-4047, "An Assessment of the Safety Implications of Control at the Oconee 1 Nuclear Plant." (See summary for NUREG/CR-4265.)

- (6) NUREG/CR-4265, "An Assessment of the Safety Implications of Control Systems at the Calvert Cliffs 1 Nuclear Power Plant" (Vols. 1 and 2).

These two reports (numbers 5 and 6) summarize the work performed on USI A-47 by ORNL. Summaries of failure modes and effects analysis, computer analysis, recorded plant occurrences, and probabilistic assessment of significant control system failure frequencies are provided. In addition, the contractor presents its conclusions and recommendations.

From the technical findings presented in these two reports, the staff formulated the resolution of USI A-47 for Babcock & Wilcox Company and Combustion Engineering plants.

- (7) NUREG/CR-4385, "Effects of Control System Failures on Transients, Accidents, and Core-Melt Frequencies at a Westinghouse Pressurized Water Reactor." (See summary for NUREG/CR-3958.)

- (8) NUREG/CR-4386, "Effects of Control System Failures on Transients, Accidents and Core-Melt Frequencies at a Babcock and Wilcox Pressurized Water Reactor." (See summary for NUREG/CR-3958.)

- (9) NUREG/CR-4387, "Effects of Control System Failures on Transients, Accidents, and Core-Melt Frequencies at a General Electric Boiling Water Reactor." (See summary for NUREG/CR-3958.)

- (10) NUREG/CR-3958, "Effects of Control System Failures on Transients, Accidents and Core-Melt Frequencies at a Combustion Engineering Pressurized Water Reactor."



These four reports (numbers 7-10) summarize the work performed on USI A-47 by PNL. Probabilistic risk analyses and estimates of core-melt frequencies and public risk associated with control system failures in Westinghouse, Babcock & Wilcox, General Electric, and Combustion Engineering reactors are presented. In addition, value/

impact analyses of possible modifications to prevent control system failures are presented. These analyses are based on the control system failures identified by INEL and ORNL.

From the technical findings presented in these four reports, the staff developed the regulatory analysis for USI A-47.

## APPENDIX C

### STAFF RESOLUTION OF PUBLIC COMMENTS

Drafts of NUREG-1217 and NUREG-1218 were issued in April 1988 for comment. Public comments were received from the organizations and individuals listed below. The comment period was extended to September 1988 so that the substantive comments that came in late could be included.

- Charles H. Cruse - Baltimore Gas & Electric Company
- W. J. Johnson - Westinghouse Electric Corporation
- Harry G. O'Brien - Tennessee Valley Authority
- J. L. Sullivan - GPU Nuclear Corporation
- H. B. Tucker - Duke Power Company

The comments that follow were extracted from the responses the staff received.

#### COMMENT 1

The events listed in Table 3.3 [of NUREG-1217] lack detail and are few in number. There are more events to draw conclusions from and, without details, it is difficult to judge the importance and probability of these events.

#### Resolution

Table 3.3 of NUREG-1217 only summarizes (1) the failure scenarios and the failure mechanisms that were identified as safety significant and (2) the failure probabilities of control systems failure sequences initiating or contributing to the events of concern. The contractor reports referenced in Sections 2.1 and 3 of NUREG-1217 provide additional detailed description of the type of events evaluated and the type of events that were identified as potentially safety significant. For additional clarity, Tables 3.1 through 3.4 were revised to refer directly to the contractor reports.

#### COMMENT 2

Appendix C [of NUREG-1218] implies that steam generator tube rupture [SGTR] is inevitable as a result of an overfill event. This is totally unsupported by analysis. The assumed thermal shrinkage which causes [SGTR] is not possible since there is no large volume of unheated feedwater when the plant is at power. Only a very large addi-

tion of unheated feedwater could provide the cooling necessary to cause significant OTSG [once-through steam generator] tube tensile loading. Tube stresses during MSLB [a main steamline break] have been evaluated as acceptable.

#### Resolution

Appendix C of NUREG-1218, with regard to SGTRs as they relate to overfill events, states that "the more-severe scenarios could potentially lead to a steamline break and a steam generator tube rupture." This statement implies that such an occurrence is possible; however, the statement does not imply certainty. The supporting analyses for the staff conclusions are described in detail in NRC contractor reports (NUREG/CR-3958, NUREG/CR-4385, and NUREG/CR-4386) for the three different pressurized-water reactor (PWR) designs of the major nuclear steam supply system (NSSS) vendors.

The conditional probability estimates for SGTR given a steamline break were taken from the results of unresolved safety issue (USI) A-3, A-4, and A-5 studies provided in NUREG-0844 and varied from 0.017 to 0.003 depending on the number of tubes ruptured.

In addition, a sensitivity study for reactor vessel/steam generator overfill scenarios, provided in Appendix B of NUREG-1218, also describes the dominant accident sequences used to determine public risk resulting from overfill events and evaluates the risk associated with three different conditional probability estimates for a main steamline break given an overfill event. These estimates go to at least two orders of magnitude lower than used in the initial analyses.

Since this information is already stated in NUREG-1218 (e.g., Section 3 and Appendix B), no additional modification or clarification is necessary.

#### COMMENT 3

The probability of main steamline break (MSLB) due to overfill is arbitrarily high and not supported by the evidence of damage for events that have occurred.

#### COMMENT 3a

The estimated frequency for main steamline break (MSLB), given [an] SG [steam generator] overfill, is too high. As referenced by NUREG-1217, a comprehensive

review of such events [NUREG/CR-3958] indicated that no such MSLBs had occurred despite several spillover events. We are also unaware of any such events occurring since the date of this study.

#### Resolution

Most overfills that were identified were initiated by failures in the main feedwater control and high-water-level trip circuits. If these events were not terminated by the operator, they would lead to water filling the steamlines, which could possibly result in damage or total steamline failure. A large uncertainty exists concerning this potential damage; therefore, the staff conservatively assumed a high probability of MSLB given a spillover of water into the steamlines. This probability was assumed to be either 0.95 or 0.50. Recognizing this conservatism, a sensitivity study (see Appendix B of NUREG-1217) also was performed to assess the public risk associated with what is considered to be more-realistic conditional probability estimates for MSLB (given a spillover). These best-estimate values derived from operating history data were estimated to be between a factor of 4 to a factor 7 times less than the initial estimates and were based on two events in Europe in which steamline damage resulted from water entering the steamline. The sensitivity studies also included an estimate 100 times less than the initial estimate. The staff's conclusions factor in the more-realistic best-estimate MSLB probabilities resulting from overfill events. Since this information is already described in Appendix B of NUREG-1217, no additional modification or clarification to the report is considered necessary.

#### COMMENT 4

The importance of the operator in responding to events is not recognized in the conclusions of [NUREG-1217].

#### Resolution

The scope of the USI A-47 study is described in Section 2 of NUREG-1217. Factors such as the adequacy of existing operating procedures and information displays were evaluated for the important transients, but operator errors of omission and commission were not systematically addressed.

For all significant event sequences, the importance of the operator response in the face of failed control systems was included in the final judgment of probability of the event—hence a factor in the resolution of this issue. The degree to which operator errors were addressed is described in Section 2.2(3) and also in the various contractor reports that are identified in Section 2.1 of NUREG-1217. The probability estimates for operator errors in mitigating the significant-events sequences also

are summarized in the footnotes of Tables 3.1 through 3.4 of NUREG-1217. Therefore, no additional modification or clarification to this report is considered necessary.

#### COMMENT 5

It is not clear if systems interaction was or was not included in this study. [See Table 2.3 of NUREG-1217.]

#### Resolution

The staff agrees that additional clarification is needed to explicitly state that systems interactions are addressed by others and are not included in the USI A-47 scope. Therefore Section 2.2(1) has been revised so that the last two sentences now read: "In addition, as part of the USI A-17 systems interaction program, spatial interactions between safety-related systems and non-safety-related systems were considered. Any identified interactions between safety-related systems and non-safety-related control systems were evaluated as part of that program and are not included in the scope of the USI A-47 review."

#### COMMENT 6

Appendix A item (4) of [NUREG-1217] is incorrect where it states "The purpose of this reexamination is to improve the reliability of the B&W [Babcock & Wilcox] PWR [pressurized-water reactor] plants by (a) reducing the number of reactor trips caused by non-safety-grade control and support systems...." The Safety Performance Improvement Program looked at all systems regardless of their safety-grade [safety-related] or non-safety-grade [non-safety-related] status.

#### Response

The staff agrees that the Babcock & Wilcox Owners Group Safety Performance Improvement Program scope included safety-related systems. The discussion in item (4) of Appendix A states that the reassessment review included, but was not limited to, the events identified. The scope of the reassessment program was extensive; however, the discussion in NUREG-1217 focused only on those systems that are applicable to the A-47 scope, i.e., non-safety-related systems.

Item (4) of Appendix A has been reworded to clarify this area.

#### COMMENT 7

It is not clear from NUREG-1218 whether the suggested redundant trip circuitry should apply to the actual trip circuits within the FWPT [feedwater pump trip], or only to the logic that applies the trip signal to the FWPT main trip solenoid valve.

**Resolution**

For most applications it is difficult to have coincidence logic such as a 2-out-of-3 for the entire system from the sensors to the actuators. However, if the output of the logic operates only a single solenoid actuator, there is a single point of failure that can defeat one of the main purposes of coincidence logic. To eliminate a single point of failure, it is necessary that there be redundant actuators. If there are redundant actuators, a logic of 2-out-of-3, 2-out-of-4, or 1-out-of-2 taken twice can be designed so that there is no single point of failure in the system.

**COMMENT 8**

The paragraph associated with Section 4.3(1) of NUREG-1218 is incorrect. The signal monitors are a deenergize-to-trip logic. The trip relay is an energize-to-trip [logic] but it is from a different power source from the rest of the control system. Therefore, the design of the system is such that loss of control system power will automatically trip the MFW [main feedwater] pumps.

**Resolution**

The intent of the referenced paragraph is to show that there are single failures for the existing 2-out-of-2 trip logic for the MFW pump trip on high-water level in the steam generator and that the existing 2-out-of-2 trip logic cannot be tested while the reactor is operating. A single failure could defeat the trip, but it would not be detected until after the reactor was shut down and the system was tested. Although the paragraph of concern is correct, it was modified to clarify what was meant by control power and by the control system and is compatible with the terminology used above.

**COMMENT 9**

Duke [Duke Power Co.] agrees with the conclusion reached in Section 4.3.1(c) of NUREG-1218, that additional trips from monthly testing would occur and that the cost/benefit ratio makes this alternative unattractive.

**Resolution**

It should be noted that the conclusions discussed in Section 4.3.1(c) apply only for providing full system testing capability on a monthly basis on the existing 2-out-of-2 steam generator high-water-level trip system. Periodic testing and verification of overflow protection systems with additional modification as indicated is however a viable alternative, as discussed in Section 4.3.2. Periodic verification and testing guidelines are provided in Appendix C, item (3)(b) of NUREG-1218. The staff also believes that periodic verification and testing of overflow protection sys-

tems can be provided without a significant increase in feedwater pump trips.

**COMMENT 10**

In regard to various solutions presented to create a 2-out-of-3 logic in the overflow protection circuits, it does not appear that using startup level indication as a third channel would offer adequate redundancy, because the startup level and operating level (downcomer level) are not completely related. The operating level is temperature compensated, the startup level is not. The operating level looks at level within the downcomer, and thus offers detection of level that would flood the aspiration ports; the startup level looks at water level in the heat transfer area of the OTSG [once-through steam generator], and is subject to resistive pressure drop errors and other variations at power. Therefore, during normal power operation, the startup level is subject to much greater inaccuracies than is the operating level.

**Resolution**

In NUREG-1218, Section 4.3(3), Case 1 is an evaluation for changing steam generator high-water-level trip by adding a level system to trip the MFW block valves independently of the 2-out-of-2 trip logic that trips the MFW pump. The basis for the cost estimate in NUREG-1218 is an assumption that an existing steam generator water level sensor could be used (e.g., startup range system) for this independent trip system. If the startup range transmitter cannot be used, the cost estimate is not applicable. However, there is a second value/impact evaluation (Case 2) based on the installation of additional equipment. This alternative also is considered viable on the basis of the value/impact evaluation, but its benefit is less. The selection of the best alternative should be based on the individual plant requirements.

Since this information is already stated in NUREG-1218 (and presented in the referenced NUREG/CR-4386 report), no additional modification or clarification is necessary.

**COMMENT 11**

The two overheating events described in Table 3.3 of NUREG-1217 are no longer applicable due to a modification presently being installed at Oconee. This modification produces an automatic MFW pump trip on a loss of either hand or auto power to the ICS [integrated control system]. This modification is the same as corrective action (iii) for alternative (4) in Section 4.3 of NUREG-1218. In addition, corrective actions (iv) and (v) have already been implemented at Oconee. Operators have been trained to cope with a loss of hand or auto power to the ICS, and alarms have been installed in the

control room to alert operators to the loss of hand or auto power to the ICS. Therefore, it is not necessary to provide automatic initiation of the EFW [emergency feedwater] system on steam generator low-water level. The automatic initiation circuitry for EFW at Oconee uses low MFW pump discharge pressure or low MFW pump control oil pressure signals to anticipate the loss of MFW. This design feature permits automatic initiation in a more timely manner to reduce the likelihood of steam generator dryout. Furthermore, low-level initiation of EFW has some potential negative impacts such as increased reactor trips, increased operator burden, additional challenges to safety systems and potential overcooling due to EFW overfill, which has not been adequately addressed.

Duke [Duke Power Co.] notes that the values used to estimate operator reliability in the two overheating events are conservative. In particular, the probability that the operators fail to initiate high-pressure injection following a loss of feedwater is estimated to be  $1.0E-02$  [0.01]. Work performed for the NRC by EG&G Idaho and published in NUREG/CR-4966 shows that this probability should actually be  $1.0E-03$  [0.001] or lower. Other operator actions which have been given too high a failure probability are reinstating MFW or initiating EFW during the overheating events. Given that more than 30 minutes are available to take either action, significantly lower failure probabilities would be appropriate. The use of a more realistic assessment of operator actions following these overheating events produces calculated core-melt frequencies one to two orders of magnitude lower than those given.

In summary, using a more realistic assessment of operator actions significantly lowers the calculated probability of overheating events leading to core melt. Furthermore, the two overheating events described in NUREG-1217 are no longer applicable due to actions already taken at Oconee. As a result, a value/impact analysis shows that none of the remaining corrective actions meet the stated criterion of \$1,000/man-rem.

#### COMMENT 11a

Steam generator dryout for B&W plants has been found not to be a concern based on the fact that restoring feedwater flow to the steam generator restores cooling even without a significant water level present. Emergency feedwater (EFW) actuation on low steam generator [water] level is provided for reasons other than avoiding dryout. Although dryout is not desirable, technical specification requirements to maintain it are not appropriate for B&W plants.

#### Resolution

The staff agrees that the modifications identified and implemented on the Oconee plants by Duke Power Company to provide an automatic MFW pump trip on a loss of either hand or auto power to the ICS may be found acceptable if designed to include all the branch circuits identified in Section 2, item 4, of NUREG/CR-3991. For additional clarity, Section 3 of Appendix C to NUREG-1218 has been modified to include all other acceptable corrective actions that could be taken to avoid steam generator dryout on a loss of power. The staff, however, still maintains that low-water-level initiation of EFW ensures adequate flow to the steam generator in the event of other failures, such as inadvertent MFW valve closure, and that the system can be designed to minimize inadvertent trips and challenges to the safety systems. On the basis of the location of the low MFW pump discharge pressure, it is not clear that in the event of an MFW valve closure, EFW would be automatically initiated. Justification for the adequacy of such a design should be submitted for staff review.

The staff agrees that there is considerable uncertainty in the values used to estimate operator reliability for these events. However, on the basis of operating history of B&W plants and the amount of confusion introduced by an ICS power failure (for example, as exemplified by the Rancho Seco power supply failures), the staff believes that the estimates used are justified. Although it also should be noted that the consequences of dryout of one steam generator have been adequately analyzed, dryout of both generators is a more severe event not adequately analyzed for all plants.

#### COMMENT 12

The draft NUREGs [NUREG-1217 and NUREG-1218] indicate that a 1-out-of-2 taken-twice trip logic is acceptable. This design would place the unit at a higher risk of inadvertent unit trip, since a single failure can cause actuation of the trip logic. This situation would result in unnecessary challenges to safety systems. This concern and the resultant impact are not considered by the investigation.

#### Resolution

A 1-out-of-2 taken-twice logic, if properly designed, would not inadvertently actuate the trip logic as a result of a single failure. For example, the General Electric Co. uses a 1-out-of-2 taken-twice logic in the reactor scram system. A boiling-water reactor (BWR) has four solenoids on each control rod assembly, two of which are deenergized to trip and two of which are energized to trip. There is no single failure that could cause an inadvertent actuation of the trip system. The selection of the logic should best meet the individual plant requirements.



## COMMENT 13

The overfilling scenario described in Table 3.3 of NUREG-1217 assumes a 0.95 probability of main steamline break (MSLB) given spillover into the steamlines. This arbitrary assumption results in a  $9.58E-06$ /yr calculated core-melt frequency and a 45.8 man-rem/yr calculated public risk, as stated in NUREG/CR-4386. However, Duke Power analysis of the Oconee main steamlines shows that, following spillover, the loads produced in the lines do not result in an MSLB. Since main steamline integrity is maintained, the conditional steam generator tube rupture, which is postulated in the dominant sequence, will also not occur. Therefore, the actual calculated core-melt frequency from the overfill scenario is that due solely to the remaining T2 transient (a loss of main feedwater due to turbine damage). NUREG/CR-4386 calculated this frequency to be  $6.88E-08$ /yr with a calculated public risk of 0.186 man-rem/yr. The resulting safety benefits (in man-rem) of the potential upgrades for the overcooling scenario are actually [more than] two orders of magnitude less than those stated in NUREG-1218. A value/impact analysis, using the actual public risk benefit with the estimated costs given in NUREG-1218, shows that none of the alternatives meet the stated criteria of \$1,000/man-rem.

This conclusion is in agreement with the statement in Appendix B of NUREG-1218... "If the probability of an MSLB (given overfill) was further reduced by as much as 2 orders of magnitude, the risk reduction would not be significant enough to warrant a design change." This is also in overall agreement with the NRC staff position that overcooling events at B&W plants are minor contributors to core damage, as stated in NUREG-1231.

## Resolution

The staff agrees that the initial estimate of the conditional probability of an MSLB, given an overfill event, is conservative. The staff maintains, however, that the claim of ensured main steamline integrity following an overfill event is unsubstantiated. A static load analysis is not convincing for the accident conditions being investigated. This single event can result in the introduction of high-temperature saturated water into the steamlines with the potential for being rapidly accelerated and potentially introduces forces on the steamlines large enough to break them. Experience suggests that there is a real chance of an MSLB given an overfill event. In two events in Europe, steamlines were damaged when water entered the steamline. These two events were used in the sensitivity analysis found in Appendix B of the regulatory analysis (NUREG-1218). As illustrated in the sensitivity analysis, the use of a best-estimate less-conservative value based on operating experience (of 0.13) for the conditional probability of an MSLB given an overfill event resulted in

a smaller, but still appreciable, reduction in public risk and a favorable cost-benefit analysis as a result of the proposed resolution.

The staff conclusions consider the more realistic estimate for the conditional probability of an MSLB given an overfill. Even with the less-conservative estimates, the proposed fix is still warranted. Since this information is already presented in Appendix B, no additional modification or clarification to the report is necessary.

## COMMENT 14

We agree that events may be postulated in which a failure of the feedwater control system and failure of the operator to take timely action can initiate an SG [steam generator] overfill event. However, we believe that the value/impact analysis does not justify the proposed alterations because the probability of the control room operator not taking corrective action in time to preclude an SG overfeed event is too conservative. The Oak Ridge National Laboratory (ORNL) analysis states the probability of operator error to be 0.1 failure per demand but does not describe the basis for this value. It appears that this value is based upon the human reliability analysis as provided in [NUREG/CR-1278]. However, our operators have demonstrated their proficiency in mitigating this type of event before SG overfilling occurs by both operating experience and training. A reactor trip plus a stuck feedwater valve scenario did occur at Calvert Cliffs [Nuclear Power Plant] in October 1983 and was successfully terminated by prompt operator action. Corrective action is specifically given in emergency operating procedures. The ORNL analysis was based upon the configuration of Calvert Cliffs at the time of data collection. Since that time, we have made several changes to upgrade both the control room and operating procedures to improve operator performance. Many of these changes were in response to TMI-related initiatives. Changes made include: (1) implementation of functional recovery emergency procedures; (2) upgrading abnormal operating procedures including SG overfill event; (3) requiring degreed shift technical advisors to complement the operating shift crews; (4) addition of a computer-based safety parameter display system to the control room; and (5) construction and use of a fully operational site-specific control room simulator. Human factors upgrades in progress will further aid operators to function more effectively during unusual operating conditions. None of these changes were considered in the original analysis. However, these changes affect the performance shaping factors relevant to the human reliability analysis and, as a result, increase the probability that the operator will terminate the event.

## Resolution

In the staff's reviews and simulations of credible overfill scenarios, several scenarios were identified in which

water could spill over into the steamline within 3 to 5 minutes of the initiating event. If this event were coupled with reactor scram that was not directly related to the overflow event, then such an event scenario could further distract the operator from the overflow problem. Operator actions to mitigate the overflow event under these conditions would be more complex and difficult to predict. The staff's criteria on establishing quantitative success probabilities for operator actions in such circumstances is discussed in Section 4.4 of NUREG/CR-4265. A review of operating history in the overflow event identified in Licensee Event Report (LER) 87-011-02, which occurred at San Onofre Nuclear Generating Station, Unit 3, indicates that a failure probability of 0.1 for an operator to terminate an overflow event is a reasonable estimate. Since a less-conservative but defensible estimate was not proposed, no modification to NUREG-1217 is warranted.

#### COMMENT 15

The estimated cost to implement the proposed automatic trip as calculated by the draft NUREGs [NUREG-1217 and NUREG-1218] is too low. We have estimated that the total cost would actually be closer to \$200,000....The cost estimated for design engineering and safety evaluation was increased because the modification may be determined to be an unresolved safety question. The change would increase the probability of occurrence of a design-basis event, loss of feedwater. Accordingly, the trip system will have to be designed such that we do not degrade the reliability of the feedwater system or increase the probability of unnecessary challenges to safety systems. Our estimate does not include the cost of installing new containment penetrations, cabling, or cabinet space; this can only be determined by a detailed plant-specific design analysis. If these changes are needed, the cost would increase dramatically. Our estimate also does not include indirect factors such as the opportunity costs or escalated costs. Also, the remaining plant life was assumed to be 30 years. Since the proposed automatic trip would not be fully operational for 3 years from the project initiation, the actual remaining plant licensed life for Calvert Cliffs [Nuclear Power Plant] would be less than 25 years.

#### Resolution

The staff agrees that the original cost estimate of \$100,000 may be low and that the total cost estimated by the utility for this alternative may be closer to \$200,000. It should be noted, however, that the sensitivity analysis in Appendix B of NUREG-1218 shows that design modifications costing \$248,000 would still be justified.

The staff revised the report to reflect the utility's cost estimates; no additional modifications were warranted. In addition, the staff does not propose any changes and believes that the assumption of a 30-year remaining lifetime

is a more prudent estimate than the suggested 25 years, particularly in light of potential life extension and/or license renewal activities.

#### COMMENT 16

The core-melt frequency stated in Table 5.1 of [NUREG-1218] ( $1 \times 10^{-7}$ ) does not agree with that stated in the text in Section 4.2(5)(a), page 4-8 ( $1.4 \times 10^{-7}$ ).

#### Resolution

Table 5.1 of NUREG-1218 summarizes the alternatives discussed in Section 4. For simplicity, the estimated core-melt frequency values shown in this table were rounded off to the most significant number and are within the error band of the calculations performed. No modification to the report is necessary as a result of this comment.

#### COMMENT 17

In NUREG-1218, Section 4.2(5), page 4-7, Case 1 is described as the inadvertent opening of all five condenser-steam dump valves. Most Westinghouse plants provide for condenser-steam dump isolation on a protection grade low-low  $T_{avg}$  signal which closes the steam dump valves regardless of the control-grade demand signal.

#### Resolution

The staff agrees. Section 4.2(5) was revised to reflect this comment.

#### COMMENT 18

Section [4.2(1) of NUREG-1218] states that steam generator overflow via the AFW [auxiliary feedwater] system was predicted to occur in about 3 minutes.

For overflow event #1, as described in NUREG-1217, any of the four proposed failure mechanisms result in the main feedwater (MFW) valve to inadvertently open resulting in overfeed of the steam generator. Upon reaching the steam generator hi-hi water-level setpoint, the MFW pumps and turbine are tripped and the AFW pumps are initiated on MFW pump trip. The time to overflow the steam generators via AFW for this scenario is expected to exceed the 3 minutes due to the effect of turbine trip and MFW pump trip.

For overflow event #2, as described in NUREG-1217, the initial failure mechanism (e.g., a failure in the controlling steam generator level channel) results in the MFW valve to inadvertently open resulting in overfeed of the steam generators. The second failure assumed is the loss of a second channel of the hi-hi steam generator level trip system which would result in the loss of MFW pump and

## Appendix C

turbine trip. However, the AFW pumps would not be actuated. The time to overfill the steam generator in this scenario due to MFW is approximately 3 minutes. However, this conclusion is in conflict with the statement in Section 4.2(1) which states the steam generator is overfilled via the AFW system in about 3 minutes.

### Resolution

The computer simulation of the first event showed that approximately 205 seconds into the transient there was significant flooding of the moisture separators and that moisture carryover was experienced from one of the three steam generators. This overfill transient assumed no operator action to manually terminate the AFW flow.

The second overfill event resulted from an MFW flow overfeeding transient with no automatic or operator-assisted manual termination of the MFW flow. For this event, AFW was not initiated. The computer simulation for this event showed a substantial reduction in steam quality 20 seconds into the event.

The RELAP5 computer model that was used to perform these simulations was subjected to code verifications and quality assurance checks as well as correlation checks between calculated results and actual plant measured results. These checks provide reasonable assurance that the model closely predicts plant behavior. Analyses of these two events are described in more detail in NUREG/CR-4326, Volume 1.

For additional clarity, Section 4.2 of NUREG-1218 was revised to preclude any perceived conflict by identifying the specific event of concern in the reference plant study.

### COMMENT 19

In NUREG-1217, Section 4.2.1(2), page 4-7, the use of the terminology "charging pumps" is confusing in this context. Generally, charging pumps refer to the Westinghouse high-head safety injection pumps and not the auxiliary feedwater or startup feedwater pumps.

### Resolution

The staff agrees. Section 4.2.1(2) has been revised to eliminate this confusion.

### COMMENT 20

The implication from the statement [in NUREG-1217, Section 4.2.1(1)(b), page 4-6] concerning the availability of plant administrative procedures for manually throttling auxiliary feedwater (AFW) flow following reactor trip or safety injection is that many Westinghouse NSSS

[nuclear steam supply system] plants do not have such procedures available.

We would like to emphasize that all Westinghouse NSSS plants that were members of the Westinghouse Owners Group (WOG) have available administrative procedures for controlling level in the steam generator following reactor trip or safety injection as described in the Emergency Response Guidelines (ERG), Procedure E-0, "Reactor Trip or Safety Injection." This guideline directs the operators to maintain total feed flow greater than a preset value until narrow range level is restored to the narrow range span in at least one steam generator. Subsequently, the operator is to control feed flow to maintain the narrow range level between 0 and 50 percent of spar.

Hence, any plant that has implemented the WOG ERGs has administrative procedures for controlling feedwater flow (both main and auxiliary) following reactor trip or safety injection.

### Resolution

The staff is not implying that many Westinghouse plants do not have procedures for instructing the operators to manually throttle AFW flow following reactor trips or safety injection events. Section 4.2.1(1)(b) states that if a Westinghouse plant does not have such procedures, or if the procedures (or training) are inadequate, then these plants are susceptible to AFW overfill transients similar to those described in the reference plant. It is prudent for all plants, not just members of the Westinghouse Owners Group, to ensure that their plant procedures and training are adequate to preclude overfill transients via the AFW system.

No modification or clarification is proposed as a result of this comment.

### COMMENT 21

**Need and Criteria for Plant-Specific Evaluations**—The analysis to support the USI A-47 conclusions seems to have examined control system failures that could have the most adverse impact on the primary- and secondary-side systems. Although the spatial effects of specific hazards such as fire, flooding, harsh environments, earthquakes, etc., were not specifically addressed, this approach may give a reasonable "coverage" of these effects. Evaluations were made of the generic applicability of the analyses of the representative plants. This approach has a great deal of merit for both a generic assessment and for plant-specific assessments.

However, it is not clear that this approach gives sufficient coverage of this very broad area. I think that *plant-specific* evaluations are needed to factor in (a) the various hazards

and their spatial effects on the control systems...and (b) plant-specific control and support systems. I think that the industry needs to develop *criteria* and practical *methodology* for use in plant-specific evaluations. The evaluations for operating plants can be based on risk reduction and value/impact for operating plants; however, the evaluations for future plants and perhaps construction plants [plants under construction] need to also factor in the traditional design-basis event (DBE) type of safety limits and safety analyses.

#### COMMENT 21a

The environmental qualification requirements in 10 CFR 50.49 require that non-safety-related electrical equipment must be environmentally qualified if its failure under harsh environments can prevent safety-related equipment from accomplishing its safety function. USI A-47 needs to be expanded to cover unintended operation of control systems caused by environmental conditions caused by pipe breaks and other events that could produce a harsh environment. For example, NRC Information Notices 79-22, 86-106, etc., should be factored into the evaluation. USI A-47 also should be expanded to cover flooding from moderate energy line breaks, flow diversions, etc., that are outside of the scope of 10 CFR 50.49.

#### COMMENT 21b

NRC Generic Letter 87-02 implies that USI A-46 may *not* cover unintended (spurious) operations of nonseismic (non-safety-grade [related]) control systems in earthquakes (see pages 4 and 12, etc.). The seismic experience data base does not seem to cover unintended (spurious) operations during an earthquake. If my understanding is correct, the discussions in Section 2.2(2) and Appendix A(2) of NUREG-1217 may need some expansion.

Sections III.G and III.L of 10 CFR 50, Appendix R, require that spurious actuations be addressed for fires. However, NRC Generic Letter 86-10 does not appear to require that more than *one* spurious actuation be assumed. This does not appear to be adequate coverage since *multiple* unintended operations have occurred in several actual fires.

#### COMMENT 21c

**Treatment of Specific Events and Spatial Effects—**Section 2.2(2) and Appendix A of NUREG-1217 and Section 2.1(2) of NUREG-1218—The draft NUREGs indicate that “external” events such as earthquakes, floods, fires, and sabotage have not been considered. It appears that the evaluations did *not* consider the *spatial* aspects of potential hazards (e.g., fires, floods, etc.) or the locations

of the control systems. However, a limited number of multiple unintended (spurious) operations were assumed. These assumptions may be fairly representative and give good “coverage” of the failures that might be caused by these types of events. I think further work is needed to develop an *integrated treatment* of these types of events as well as the failures within the current scope of USI A-47. This integrated treatment should include (1) the various hazardous events, such as pipe breaks, “internal” flooding, “internal” fires, other events that produce harsh environments, earthquakes, etc., and (2) consideration of the spatial aspects of the hazards and their effects on the control systems located within the zone of their influence. Different assumptions may be appropriate for different hazards.

#### Resolution

In its technical evaluation of USI A-47, the staff considered individual and selected multiple system failures that result from nonmechanistic failure modes. This approach evaluates, to some extent, the effects of system failures that could occur as a result of external events such as fires, flooding, and earthquakes. This was a limited study focusing only on non-safety-related control system failures. This study assumed that at least one channel of safety-related mitigating systems would be available if needed. The limitations of the USI A-47 evaluation were established on the basis that these events were addressed in other programs: USI A-17, USI A-46, Fire Protection (10 CFR 50 Appendix R) review program, Environmental Qualifications program. However, some potential safety concerns were identified by the staff and the Advisory Committee for Reactor Safeguards (ACRS) that were either (1) not in the scope of the safety issue or other programs, (2) a spinoff from the existing issues, or (3) peripheral concerns for which additional review effort is thought to be needed. As a result, a program has been established to address these concerns and to develop them as issues of sufficient detail so that they may be evaluated, if needed, as new issues according to priority. This program is entitled the Multiple Systems Response Program and is progressing on a separate schedule independent from USI A-47.

#### COMMENT 22

**Overfill Events—**One of the more rapid and significant overfill events for a PWR seems to be a reactor trip followed by a failure of the control systems to rapidly run-back the MFW. This type of event seems to only be addressed in two cases in Section 3 of NUREG-1217: (1) overfill event #1 in Table 3.4 and (2) overheat event #1 in Table 3.3. I think that this type [of] overfill event needs to be treated in more detail for all of the representative plants.



### Resolution

All of the representative plants studied during the USI A-47 evaluation were evaluated for this type of transient. It should be noted that NUREG-1217 only summarizes the results of several contractor reports. Specific details of the analyses performed can be found in the referenced contractor reports.

Section 4 of NUREG-1217 discusses the generic applicability of such events, and Appendix C of NUREG-1218 proposes recommended actions for each type of nuclear steam supply system (NSSS) plant in order to mitigate the consequences of such events. Therefore, no additional action is considered necessary as a result of this comment.

### COMMENT 23

**B&W Overfill Protection Systems**—Section 4.3 of NUREG-1217 and Section (3) of Appendix C of NUREG-1218—Our 205 fuel element B&W plant, Bellefonte, does not have a measurement of steam generator water level. This resulted in the need for a much more complex overfill protection system that used neutron flux, MFW flow, steam generator differential pressure, etc., to develop trip signals. The NUREGs [NUREG-1217 and NUREG-1218] should reflect this different protection system used on a few B&W construction plants.

### Resolution

The staff agrees. Overfill protection for Bellefonte Nuclear Plant and Washington Nuclear Plant, Unit 1, is provided by high steam generator differential pressure (i.e., level) when the reactor power is below 31 percent and by excessive feedwater flow when the reactor power is above 25 percent. Reactor power dependence is removed from the level trip after a reactor trip has been initiated. This system is designed as part of the engineered safety features actuation system and is designed to conform with the prescribed criteria for these systems. This design also may be considered an equivalent alternative, depending on the outcome of the staff's review.

As a result of this comment, Section 4.3.1 of NUREG-1217 and Section (3) of Appendix C of NUREG-1218 have been revised to permit other designs that are equivalent or better.

### COMMENT 24

**Atmospheric and Condenser Dump Valve Controller Logic**—Section 4.2(6) of NUREG-1218—TVA modified the atmospheric and condenser dump valve controller logic in the ICS for our B&W plant so that a single failure

in the logic could only open a few dump valves. This was done to prevent a relatively likely initiating event single failure from causing the fuel safety limits for a frequent event (ANS Condition II event) to be exceeded. Although this is not directly related to frequency of core melt, I think it is an improvement worth considering for other PWRs—particularly for future plants and perhaps for [plants under construction].

### Resolution

Existing NRC criteria require that accidents and transients be analyzed assuming a worst-case single failure. Acceptance criteria also are specified for each category of events. The acceptance criteria for increase in steam flow transients are specified in NUREG-0800, Section 15.1.1. Each licensee is responsible for providing an appropriate plant design that will meet the applicable acceptance criteria for all accidents and transients.

### COMMENT 25

**Steam Generator Tube Rupture Events**—Section 3 of NUREG-1217, and Sections 3.2.4 and 4.2(9) of NUREG-1218...address the affects of control system failures on SGTR [steam generator tube rupture] events for Westinghouse plants (see SGTR event #1 and #2 in Table 3.2 [NUREG-1217]). It appears to me that these types of failures should present similar concerns for the B&W and CE plants. If valid, these failures and events should be addressed in [NUREG-1217 and NUREG-1218].

### Resolution

SGTR events were addressed in the contractor reports for both the B&W and CE plants. The evaluations are provided in NUREG/CR-4047 and NUREG/CR-4265, respectively, and are referenced in NUREG-1217.

### COMMENT 26

**Initiating Event Failures vs. Consequential Failures**—The USI A-47 evaluation considers some control system failures that are the consequences of DBEs [design-basis events]; however, most of the emphasis is placed on initiating event control system failures. I think additional attention needs to be given to consequential control system failures. For example, the unintended opening of the secondary side PORVs [power-operated relief valves] upstream of the main steam isolation valves (MSIVs) can create safety problems of (a) a loss of containment isolation in a LOCA [loss-of-coolant accident] (assuming a small pre-existing steam generator tube leak), (b) excessive cooldown rates and loss of pressurized steam generators for a heat sink in a steamline break, (c) loss of



capability to terminate the radiation release in a steam generator tube rupture, etc.

### Resolution

The USI A-47 study addressed DBEs being made more severe than previously analyzed as a result of non-safety-related control system failures. These failures could occur as a result of the event or independently. A review of the contractor reports referenced in NUREG-1217 shows that a significant effort was made in this area. In all but a few cases, it was shown that the existing safety-related systems adequately mitigated DBEs even when compounded by multiple non-safety-related system failures. Single and selected multiple non-safety-related control failures were evaluated under different normal operating conditions and accident conditions. These failures included consequential failures as well as random failures of non-safety-related control systems in order to assess worst-case transient conditions.

### COMMENT 27

**General Impressions**—Based on a brief review, I think that the evaluation and the proposed resolutions for USI A-47 are generally reasonable for operating plants. I think some further effort may be needed on an integrated approach for unintended (spurious) operations of non-safety-related equipment. Plant-specific evaluations may be appropriate. A somewhat more conservative approach may be appropriate for future plants and perhaps for [plants under construction].

### COMMENT 27a

**TVA Initiatives Related to USI A-47**—TVA has undertaken several initiatives for design improvements related to the USI A-47 area. The majority of these were made for our later Babcock & Wilcox (B&W) and Combustion Engineering (CE) pressurized-water reactors (PWRs)—Bellefonte and Yellow Creek.

TVA was instrumental in identifying the potential problem with control system failures that could cause a steam generator overfill transient in 1972 before it became an NRC concern. We noted that Westinghouse (W) had provided a safety-grade [safety-related] cutoff of main feedwater (MFW) on high steam generator [water] level for core overcooling protection (which also provided steam generator overfill protection), and that B&W and CE did not have any provisions for automatic MFW isolation. We also noted that B&W had transferred [its] integrated control system (ICS) design from [its] fossil to [its] nuclear plants; however, [B&W] had not transferred the separate overfill "protection" type system provided in [its] fossil plants. At TVA's direction, B&W and CE added provi-

sions to isolate MFW to prevent overfill to the engineered safety features actuation systems (ESFAS) for our Bellefonte and Yellow Creek plants.

In other areas, TVA directed B&W in the early 1970s to add a safety-grade [safety-related] system for Bellefonte to initiate and control auxiliary feedwater (AFW). This was expanded after TMI-2 to provide better control. In the mid-1970s, TVA upgraded the primary- and secondary-side power-operated relief valves (PORVs) to be safety grade for both the opening and closing modes for our B&W and CE plants. (Our CE plants did not have PORVs on the primary side.) These valves serve the safety functions of cooldown, depressurization, isolation, and prevention of unintended operations. TVA has also provided safety-grade pressurizer sprays to serve the safety function of depressurization (in conjunction with the PORVs). In the early 1970s, TVA also provided safety-grade control air systems to power the PORVs, AFW control valves, etc., for our W, B&W, and CE plants.

### Resolution

It is commendable that TVA has undertaken several initiatives for design improvements related to USI A-47. Procedural, administrative, and design modifications that improve plant safety are encouraged.

As a result of operating experience and transients that have occurred at several Babcock & Wilcox (B&W) plants, an industry-sponsored program was developed by the owners of the B&W plants. The stated goal of this program (i.e., Babcock & Wilcox Owners Group Safety and Performance Improvement Program) was to increase the level of plant safety by reducing plant trips and by reducing or eliminating complex transients. This effort complements the proposed actions under USI A-47.

A large number of recommendations were developed and are currently being implemented by the individual plants, including Bellefonte. The staff believes that this industry effort makes plants safer.

### COMMENT 28

**Commercial Grade vs. Safety-Grade [Safety-Related] Overfill Protection Systems**—Items (6) and (7) of Section 5 of NUREG-1217, and items (6) and (7) and Appendix C of NUREG-1218—The conclusions for USI A-47 indicate that commercial-grade overfill protection systems that meet certain design requirements are considered to be adequate. This is reasonable for backfits for operating plants; however, I think future plants and perhaps construction plants need to provide safety-grade overfill protection systems.

**Resolution**

The staff's recommendations are presented in NUREG-1218, Appendix C. These recommendations reflect minimum acceptability. It should be noted that the more-recent plant designs have chosen to incorporate safety-related overfill protection systems. These designs are fully endorsed by the staff. It is, however, the responsibility of each licensee to justify the adequacy of its design. The staff believes that it is appropriate for licensees of new plants to provide such safety-related systems and encourages them to do so.

**COMMENT 29**

**Traditional DBE Safety Limits vs. Risk Basis**—The proposed resolutions of USI A-47 are generally based on risk reduction and value/impact analyses. This is appropriate for potential backfits for operating plants. However, for future plants and perhaps for [plants under construction], I think that traditional DBE [design-basis event] type of safety limits and safety analyses needs to also be considered. For newer plants, the control system failures need to be factored into the traditional conservative safety analyses to some degree. Examples include: Item (1) Overfill Events—If an overfill event can cause the failure of steamlines or relief valves on a PWR, then the traditional safety limits associated with steamline breaks need to be considered as well as the risk basis concerns of a steamline break causing steam generator tube ruptures and core melt. See also the safety concerns in item (3) of Appendix A of NUREG-1217. Item (2) SGTR Events—The effects of control system failures need to be evaluated in terms of the traditional SGTR [steam generator tube rupture] dose limits—even though [such failures do] not lead to a core melt considered in the risk basis. See also the safety concerns in item (3) of Appendix A of NUREG-1217.

**Resolution**

The technical evaluation to address USI A-47 included consideration of DBEs and specifically addressed accidents or transients being more severe than previously analyzed. This methodology inherently included assessment of traditional safety limits and safety analyses. It should be noted that Section 7.7 of the Standard Review Plan (SRP) (NUREG-0800) already describes acceptance criteria for non-safety-related control systems, including the consequences of their failures. The SRP is applicable to current license applications as well as to future plants. With the exception of incorporating guidelines for overfill protection, no additional revisions to the SRP are anticipated as a result of the USI A-47 effort.

Regarding SGTR events, in its study of Generic Issue 135, the staff is investigating the consequences of water entering the main steamlines refer to item 3 (p. A-1) of Appendix A to NUREG-1217.

**COMMENT 30**

**Development of Methods of Treating Multiple Failures in Control Systems**—The assumptions for unintended (spurious) failures has been a controversial topic and a source of confusion for many years. The assumptions for non-safety-grade [non-safety-related] equipment are much more uncertain than are the assumptions for safety-grade [safety-related] equipment.

I think that the industry needs to *develop* a practical methodology for designers to use to evaluate and provide protection from a limited number of multiple unintended operations of non-safety-related equipment. As discussed..., this needs to be an *integrated* approach for the various types of hazards. The spurious operations need to be addressed for non-safety-grade components that are (a) in the zone of influence of the event and (b) not qualified (or designed to function) in the environment. The methodology should build on (a) the approaches being developed for the resolution of USI A-47 and USI A-17 and (b) the approaches being developed for various individual hazards.

The methods development needs to include an evaluation of the (a) need, (b) merits, and (c) practicality of addressing a *limited* number of *multiple* unintended operations. This involves an evaluation of whether or not the increased complexity of the analysis of, and protection from, a limited number of multiple unintended operations would give a worthwhile and cost-effective increase in safety over the assumption of one spurious action. There is a need to develop *practical methods* of *limiting* the number of multiple unintended operations to those that are more likely and that are also more significant.

The previous treatments for unintended (spurious) operations that have been either proposed or used by industry have involved a full range of assumptions. They are generally limited to equipment in the zone of influence that is not designed to work in the environment produced by the event. These include:

- (1) No unintended (spurious) operations.
- (2) One unintended operation.
- (3) A *limited* number of *multiple* unintended operations.
- (4) Multiple unintended operation of *all* nonqualified equipment in zone of influence.

I *do not* think it is reasonable to assume either (a) no unintended operations or (b) multiple unintended operations

of *all* nonqualified equipment in the zone of influence. The *most likely* results of DBEs [design-basis events] with hazards, such as fires, harsh environment, flooding, vibration from an earthquake, etc., are a *limited* number of *multiple* unintended operations. It is difficult to defend the assumption of *one* unintended operation from likelihood and past experience. However, the assumption of *one* unintended operation "covers" a good interim position until (a) a more detailed evaluation of the issue, (b) positions, and (c) practical methods of addressing multiple unintended operations can be developed.

Although only *one* spurious action is assumed, it could occur at any location in the zone of influence; thus, *all* spurious actions would need to be evaluated *individually*. In general, the likelihood of multiple unintended operations decreases as the number is increased. (There are a few exceptions such as containment isolation and other actions of the ESFAS [engineered safety features actuation system], the solid-state control systems, etc.) Also, the assumption of one failure may be commensurate with the importance to safety. If the equipment is not safety related, its function is not directly related to the mitigation of the DBEs. If it is assumed that it does not work, a class of failure modes is already analyzed. If one spurious failure is assumed, an additional class of events is eliminated. The failures not analyzed would be multiple failures of non-safety[-related] equipment that somehow combine to affect multiple trains of safety[-related] equipment, or in combination with a random failure, affect the remaining specific train. The effort involved in eliminating this threat may not be commensurate with the risk.

#### Resolution

The staff generally agrees with the suggestion that industry should develop improved analysis of the effects of non-safety-related system failures and interactions and believes that the effects of multiple failures on the ability of operators to diagnose the need for intervention and correctly intervene should be studied in more detail. The staff also believes that a significant number of plant upsets are the result of multiple failures and that a systematic means for dealing with them is not available to all plants. Some effort in this area is currently being addressed via the use of plant simulators and plant-specific probabilistic risk assessment analysis.

In the USI A-47 study, multiple control system failures were considered. The selection of the multiple failures

was the result of a careful consideration of the most likely failure combinations and the most safety-significant combinations. The selections were based on engineering evaluation and were derived from a large number of transient simulations.

#### COMMENT 31

The proposed resolution includes requirements for including certain items in the plant technical specifications. It is not apparent that this position has been evaluated using the NRC Interim Policy Statement on Technical Specification Improvements.

We believe that the NRC Interim Policy Statement, as written, does not support including steam generator overfill protection in the technical specifications. We are aware of the NRC staff position in [the NRC] letter dated May 9, 1988, to Mr. Wilgus, chairman of the B&W Owners Group. We disagree that the existing criteria support including "certain *active* design features...and operating restrictions...needed to *preclude unanalyzed accidents*." Furthermore, it cannot be generically concluded that steam generator overfill protection is necessary to preclude an unanalyzed accident on the basis of a review of a single plant. Therefore, the need for new technical specifications must be made on a case-by-case basis. As a matter of interest, the event has been evaluated for TMI-1 and does not result in an unanalyzed event without taking credit for overfill protection. This conclusion has been reviewed by the NRC staff and found acceptable.

#### Resolution

The NRC staff does not agree. The staff maintains that the position to periodically verify the operability of the overfill protection system is consistent with the NRC Interim Policy Statement on Technical Specification Improvements. For most plants, this position satisfies criterion 2 of the NRC Interim Policy Statement, which delineates constraints on design and operation of nuclear power plants that are derived from the plant safety analysis report, and does belong in the technical specifications. Also, for some plants, this position also satisfies criterion 3 of the same policy statement because the high-water-level trip system is used to mitigate a main feedwater overfill transient, which is a design-basis event.

Therefore, the resolution has not been modified as a result of this comment.

MODEL SERMODEL SAFETY EVALUATION TO BE USED AS GUIDANCE  
BY THE OFFICE OF NUCLEAR REACTOR REGULATION  
RELATED TO LICENSE AMENDMENT REQUESTS FOR  
TECHNICAL SPECIFICATION CHANGES FOR  
REACTOR VESSEL (BWR) OR STEAM GENERATOR (PWR) OVERFILL PROTECTION1.0 INTRODUCTION

By Generic Letter 89-XX<sup>(1)</sup>, the NRC recommended that a system be provided to mitigate main feedwater overflow events for all boiling and pressurized water reactors (BWRs & PWRs) that currently do not have such protection. This action was part of the technical resolution of Unresolved Safety Issue (USI) A-47, "Safety Implications of Control Systems in LWR Nuclear Power Plants." Furthermore, it was requested that all LWR plants have Technical Specifications that address the operability of the overflow protection systems that are provided in response to the Generic Letter on USI A-47.

2.0 EVALUATION

Overflow protection for each LWR consists of protection channels that initiate the termination of main feedwater flow to the reactor vessel for a BWR or to the steam generators for a PWR, on sensing a high water level condition. The overflow protection mitigates the consequences of main feedwater control system failures as an event which could lead to overflow conditions, as well as limiting the operating water level to within the bounds of the assumptions used in the safety analysis. Both functions fall within the scope of the criteria for determining the content of Technical Specifications as established by the Commission's Interim Policy Statement on Technical Specifications<sup>(2)</sup>.

The action set forth by Generic Letter 89-XX on Technical Specifications for overflow protection is that license amendment requests be submitted that encompass requirements for Limiting Conditions for Operation, Setpoints, and Surveillance Requirements which are commensurate with the safety actions required by the existing Technical Specifications.

By letter dated \_\_\_\_\_, (the Licensee) responded to generic letter 89-XX. [PM should provide a description of the specific plant's response, i.e., describe the system to be installed with the appropriate Technical Specification changes.]

Per generic letter 89-XX, an acceptable overflow protection system design is one which (a) is separate from the feedwater control system so that it is not powered from the same source, (b) is not located in the same cabinet as the feedwater control system, and (c) the cables are not routed so that a fire is likely to affect both the feedwater control system and the overflow protection system simultaneously. Common-mode failures, however, that could disable overflow protection and the feedwater control system, but would still cause a feedwater pump trip, are considered acceptable failure modes.

[The PM should provide specifics of how the design meets the review criteria. The PM must conclude that the licensee's design is acceptable or not acceptable as appropriate. If the design is unacceptable, the amendment would be rejected.]



The plant's existing Technical Specifications for systems that initiate safety actions define requirements which the NRC has previously reviewed and found to be in conformance with the applicable regulatory requirements for Technical Specifications; namely those set forth in 10 CFR 50.36 in regard to Limiting Conditions for Operation, Limiting Safety System Settings (Setpoints), and Surveillance Requirements. The licensee has proposed technical specifications for the overfill protection system which are equivalent to similar existing technical specifications for [PM provide specifics]. The proposed technical specifications for the overfill protection system insure operability of the system at appropriate times, are consistent with existing requirements for systems providing a commensurate level of safety and are therefore acceptable.

### 3.0 ENVIRONMENTAL CONSIDERATION

This amendment involves a change to a requirement with respect to the installation or use of a facility component located within the restricted area as defined in 10 CFR 20 and changes to the surveillance requirements. The staff has determined that the amendment involves no significant increase in the amounts, and no significant change in the types, of any effluents that may be released offsite and that there is no significant increase in individual or cumulative occupational radiation exposure. The Commission has previously issued a proposed finding that this amendment involves no significant hazards consideration and there has been no public comment on such finding. Accordingly, this amendment meets the eligibility criteria for categorical

exclusion set forth in 10 CFR 51.22(c)(9). Pursuant to 10 CFR 51.22(b), no environmental impact statement or environmental assessment need be prepared in connection with the issuance of this amendment.

#### 4.0 CONCLUSION

The Commission made a proposed determination that the amendment involves no significant hazards consideration which was published in the Federal Register ( FR ) on \_\_\_\_\_. The Commission consulted with the state of \_\_\_\_\_. No public comments were received, and the state of \_\_\_\_\_ did not have any comments.

We have concluded, based on the considerations discussed above, that: (1) there is reasonable assurance that the health and safety of the public will not be endangered by operation in the proposed manner, and (2) such activities will be conducted in compliance with the Commission's regulations, and the issuance of this amendment will not be inimical to the common defence and security or to the health and safety of the public.

#### 5.0 REFERENCES

- (1) U. S. Nuclear Regulatory Commission, Generic Letter 89-XX, "Request for Action Related to Resolution of Unresolved Safety Issue A-47, 'Safety Implication of Control Systems in Light Water Nuclear Power Plants,' Pursuant to 10 CFR 50.54(f)," dated \_\_\_\_\_, 1989.

- (2) \_\_\_\_\_, "Interim Policy Statement on Technical Specification Improvements for Nuclear Power Reactors," 52 FR 3788, February 6, 1987.

PRINCIPAL CONTRIBUTOR:

Dated:

Document Name:  
A-47 GENERIC SER

Requestor's ID:  
BEVAN

Author's Name:  
ASzukewicz

Document Comments:  
Enclosure 4 for Final Resolution Package

ENCLOSURE 5

PROPOSED STANDARD TECHNICAL SPECIFICATIONS FOR VERIFICATION TESTING  
OF OVERFILL PROTECTION SYSTEMS FOR B & W AND CE PLANTS



*No change  
THIS PAGE*INSTRUMENTATION3/4.3.2 ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATIONLIMITING CONDITION FOR OPERATION

3.3.2 The Engineered Safety Feature Actuation System (ESFAS) instrumentation channels shown in Table 3.3-3 shall be OPERABLE with their trip setpoints set consistent with the values shown in the Trip Setpoint column of Table 3.3-4 and with RESPONSE TIMES as shown in Table 3.3-5.

APPLICABILITY: As shown in Table 3.3-3.

ACTION:

- a. With an ESFAS instrumentation channel trip setpoint less conservative than the value shown in the Allowable Values column of Table 3.3-4, declare the channel inoperable and apply the applicable ACTION requirement of Table 3.3-3 until the channel is restored to OPERABLE status with the trip setpoint adjusted consistent with the Trip Setpoint Value.
- b. With an ESFAS instrumentation channel inoperable, take the action shown in Table 3.3-3.

SURVEILLANCE REQUIREMENTS

4.3.2.1 Each ESFAS instrumentation channel and bypass shall be demonstrated OPERABLE by the performance of the CHANNEL CHECK, CHANNEL CALIBRATION and CHANNEL FUNCTIONAL TEST operations for the MODES and at the frequencies shown in Table 4.3-2.

4.3.2.2 The ENGINEERED SAFETY FEATURES RESPONSE TIME of each ESFAS function shall be demonstrated to be within the limit at least once per 18 months. Each test shall include at least one channel per function such that all channels are tested at least once every N times 18 months where N is the total number of redundant channels in a specific ESFAS function as shown in the "Total No. of Channels" Column of Table 3.3-3.

TABLE 3.3-3 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEMS INSTRUMENTATION

<u>FUNCTIONAL UNIT</u>	<u>TOTAL NO. OF CHANNELS</u>	<u>CHANNELS TO TRIP</u>	<u>MINIMUM CHANNELS OPERABLE</u>	<u>APPLICABLE MODES</u>	<u>ACTION</u>
8. AUXILIARY FEEDWATER					
a. Manual Initiation	2	1	2	1, 2, 3	16
b. Steam Generator Pressure-Low	4/steam generator	2/steam generator	3/steam generator	1, 2, 3**	10#
c. Steam Generator Level-Low	4/steam generator	2/steam generator	3/steam generator	1, 2, 3	10#
d. Reactor Coolant Pumps Tripped	4	2	3	1, 2, 3**	10#
e. Containment Pressure-High	4	2	3	1, 2, 3	10#
f. Automatic Actuation Logic	2	1	2	1, 2, 3	15
g. Trip of Main Feedwater Pumps	3/pump	2/pump	2/pump	1, 2**	9
9. ENGINEERED SAFETY FEATURE ACTUATION SYSTEM BYPASSES					
a. Reactor Coolant System Pressure	1/channel	1/channel	1/operating channel	1, 2, 3	17
b. Steam Generator Pressure	1/channel	1/channel	1/operating channel	1, 2, 3	17
c. Containment Pressure	1/channel	1/channel	1/operating channel	1, 2, 3, 4	17
10. MAIN FEEDWATER ISOLATION					
a. Steam Generator level-High					
b. Automatic Actuation					

*Repeat as stated*

B&W-ST5

3/4 3-13

SEP 24 1980

B&W-ST5

TABLE 3.3-4 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEMS INSTRUMENTATION TRIP SETPOINTS

<u>FUNCTIONAL UNIT</u>	<u>TRIP SETPOINT</u>	<u>ALLOWABLE VALUES</u>
8. AUXILIARY FEEDWATER		
a. Manual Initiation	Not Applicable	Not Applicable
b. Steam Generator Pressure-Low	< ( ) psig	< ( ) psig
c. Steam Generator Level-Low	< ( ) feet	< ( ) feet
d. Reactor Coolant Pumps-Tripped	Loss of 2 or 4 Pumps	Loss of 2 or 4 Pumps
e. Containment Pressure-High	< (5) psig	< (5) psig
f. Automatic Actuation Logic	Not Applicable	Not Applicable
g. Trip of Main Feedwater Pumps	Not Applicable	Not Applicable
9. ENGINEERED SAFETY FEATURE ACTUATION SYSTEM BYPASSES		
a. Reactor Coolant System Pressure	(1600)	( )
b. Steam Generator Pressure	(725)	( )
c. Containment Pressure	Not Applicable	Not Applicable
10. <i>MAIN FEEDWATER ISOLATION</i>		
d. <i>Steam Generator Level-High</i>	<i>≤ ( ) feet</i>	<i>≤ ( ) feet</i>

3/4 3-18

TABLE 3.3-5 (Continued)

<u>INITIATING SIGNAL AND FUNCTION</u>	<u>RESPONSE TIME IN SECONDS</u>
8. <u>4.16 kv Emergency Bus Undervoltage (Loss of Voltage)</u> <u>Loss of Power</u>	$\leq ( )^*$
9. <u>4.16 kv Emergency Bus Undervoltage (Degraded Voltage)</u> <u>Loss of Power</u>	$\leq ( )^*$
10. <u>Steam Generator Pressure-Low</u> <u>Auxiliary Feedwater System</u> <u>Main Steam Isolation</u>	$\leq ( )^*/( )^{**}$ $\leq ( )^*/( )^{**}$
11. <u>Steam Generator Level-Low</u> <u>Auxiliary Feedwater System</u>	$\leq ( )^*/( )^{**}$
12. <u>Reactor Coolant Pumps-Tripped</u> <u>Auxiliary Feedwater System</u>	$\leq ( )^*/( )^{**}$
13. <u>Trip of Main Feedwater Pumps</u> <u>Auxiliary Feedwater System</u>	$\leq ( )^*/\leq ( )^{**}$

TABLE NOTATION

\*Diesel generator starting and sequence loading delays included. Response time limit includes movement of valves and attainment of pump or blower discharge pressure.

\*\*Diesel generator starting and sequence loading delays not included. Offsite power available. Response time limit includes movement of valves and attainment of pump or blower discharge pressure.

*4. Main Feedwater Isolation*

$\leq ( )$

TABLE 4.3-2 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEMS INSTRUMENTATION SURVEILLANCE REQUIREMENTS

FUNCTIONAL UNIT	CHANNEL CHECK	CHANNEL CALIBRATION	CHANNEL FUNCTIONAL TEST	MODES FOR WHICH SURVEILLANCE IS REQUIRED
b. 4.16 kv Emergency Bus Undervoltage (Degraded Voltage)	S	R	M	1, 2, 3, 4
<b>8. AUXILIARY FEEDWATER</b>				
a. Manual Initiation	N.A.	N.A.	M(1)	1, 2, 3
b. Steam Generator Pressure-Low	S	R	M	1, 2, 3
c. Steam Generator Level-Low	S	R	M	1, 2, 3
d. Reactor Coolant Pumps-Tripped	S	R	M	1, 2, 3
e. Containment Pressure-High	S	R	M(3)	1, 2, 3
f. Automatic Actuation Logic	N.A.	N.A.	M(2)	1, 2, 3
g. Trip of Main Feedwater Pumps	N.A.	N.A.	R	1, 2
<b>9. ENGINEERED SAFETY FEATURE ACTUATION SYSTEM BYPASSES</b>				
a. Reactor Coolant System Pressure	N.A.	R(4)	S/U(5)	1, 2, 3
b. Steam Generator Pressure	N.A.	R(4)	S/U(5)	1, 2, 3
c. Containment Pressure	N.A.	R(4)	N.A.	1, 2, 3, 4

B&W-ST5

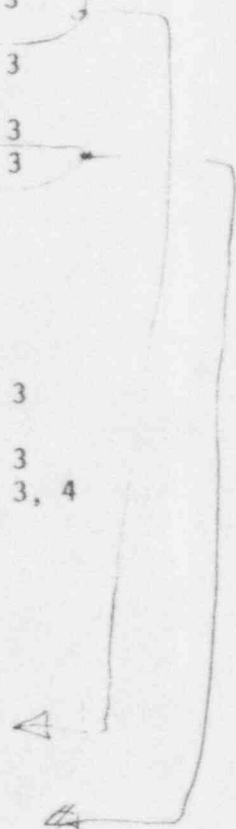
3/4 3-23

MAIN FEEDWATER ISOLATING

a. steam generator level high

b. automatic actuation logic

Repeat as stated





INSTRUMENTATION3/4.3.2 ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATIONLIMITING CONDITION FOR OPERATION

3.3.2 The Engineered Safety Feature Actuation System (ESFAS) instrumentation channels and bypasses shown in Table 3.3-3 shall be OPERABLE with their trip setpoints set consistent with the values shown in the Trip Setpoint column of Table 3.3-4 and with RESPONSE TIMES as shown in Table 3.3-5.

APPLICABILITY: As shown in Table 3.3-3.

ACTION:

- a. With an ESFAS instrumentation channel trip setpoint less conservative than the value shown in the Allowable Values column of Table 3.3-4, declare the channel inoperable and apply the applicable ACTION requirement of Table 3.3-3 until the channel is restored to OPERABLE status with the trip setpoint adjusted consistent with the Trip Setpoint value.
- b. With an ESFAS instrumentation channel inoperable, take the ACTION shown in Table 3.3-3.

SURVEILLANCE REQUIREMENTS

4.3.2.1 Each ESFAS instrumentation channel shall be demonstrated OPERABLE by the performance of the CHANNEL CHECK, CHANNEL CALIBRATION and CHANNEL FUNCTIONAL TEST operations for the MODES and at the frequencies shown in Table 4.3-2.

4.3.2.2 The logic for the bypasses shall be demonstrated OPERABLE during the at power CHANNEL FUNCTIONAL TEST of channels affected by bypass operation. The total bypass function shall be demonstrated OPERABLE at least once per 18 months during CHANNEL CALIBRATION testing of each channel affected by bypass operation.

4.3.2.3 The ENGINEERED SAFETY FEATURES RESPONSE TIME of each ESFAS function shall be demonstrated to be within the limit at least once per 18 months. Each test shall include at least one channel per function such that all channels are tested at least once every  $N$  times 18 months where  $N$  is the total number of redundant channels in a specific ESFAS function as shown in the "Total No. of Channels" Column of Table 3.3-3.

TABLE 3.3-3 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION

<u>FUNCTIONAL UNIT</u>	<u>TOTAL NO. OF CHANNELS</u>	<u>CHANNELS TO TRIP</u>	<u>MINIMUM CHANNELS OPERABLE</u>	<u>APPLICABLE MODES</u>	<u>ACTION</u>
9. LOSS OF POWER (LOV)					
a. 4.16 kv Emergency Bus Undervoltage (Loss of Voltage)	4/Bus	2/Bus	3/Bus	1, 2, 3	12
b. 4.16 kv Emergency Bus Undervoltage (Degraded Voltage)	4/Bus	2/Bus	3/Bus	1, 2, 3	12
10. EMERGENCY FEEDWATER (EFAS)					
a. Manual (Trip Buttons)	2 sets of 2 per S/G	1 set of 2 per S/G	2 sets of 2 per S/G	1, 2, 3	16
b. Automatic Actuation Logic	4/SG	2/SG	3/SG	1, 2, 3	14*, 15*
c. SG Level and Pressure (A/B) - Low and WP (A/B) - High	4/SG	2/SG	3/SG	1, 2, 3	13*
d. SG Level (A/B) - Low and No S/G Pressure - Low Trip (A/B)	4/SG	2/SG	3/SG	1, 2, 3	13*
e. Safety Injection	See 1 above for all Safety Injection Initiating Functions and Requirements				

11. MAIN FEEDWATER INSTRUMENTATION

a. SG Level - High

b. Automatic Actuation Logic

*Repeat as stated*

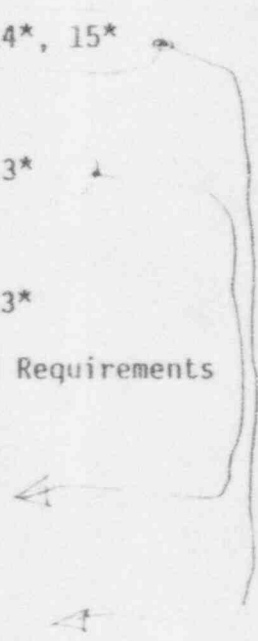


TABLE 3.3-4 (Continued)

## ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION TRIP VALUES

FUNCTIONAL UNIT	TRIP VALUE	ALLOWABLE VALUES
8. CONTAINMENT COOLING (CCAS)		
a. Manual (Trip Buttons)	Not Applicable	Not Applicable
b. Containment Pressure - High	$\leq (18.4)$ psia	$\leq (19.02)$ psia
c. Pressurizer Pressure - Low	$\geq (1740)$ psia	$\geq (1686.7)$ psia
d. Automatic Actuation Logic	Not Applicable	Not Applicable
9. LOSS OF POWER		
a. 4.16 kv Emergency Bus Undervoltage (Loss of Voltage)	(3120) volts	(3120) volts
b. 4.16 kv Emergency Bus Undervoltage (Degraded Voltage)	(423) $\pm$ (2.0) volts with an (8.0 $\pm$ 0.5) second time delay	(423) $\pm$ (4.0) volts with an (8.0 $\pm$ 0.8) second time delay
10. EMERGENCY FEEDWATER (EFAS)		
a. Manual (Trip Buttons)	Not Applicable	Not Applicable
b. Steam Generator (A&B) Level-Low	$> (46.5)\%$	$> (45.61)\%$
c. Steam Generator $\Delta P$ -High (SG-A $>$ SG-B)	$< (39)$ psi	$< (48.35)$ psi
d. Steam Generator $\Delta P$ -High (SG-B $>$ SG-A)	$< (39)$ psi	$< (48.35)$ psi
e. Steam Generator (A&B) Pressure - Low	$> (728)$ psia	$> (706.6)$ psia
f. Safety Injection	See I above for all Safety Injection Initiating Functions and Requirements	
g. Automatic Actuation Logic	Not Applicable	Not Applicable

11. MAIN REACTOR ISOLATION

a. Steam Generator Level-High

 $\leq ( )\%$  $\leq ( )\%$

TABLE 3.3-5 (Continued)

ENGINEERED SAFETY FEATURES RESPONSE TIMES

<u>INITIATING SIGNAL AND FUNCTION</u>	<u>RESPONSE TIME IN SECONDS</u>
10. <u>Steam Generator Level-Low</u>	
a. Emergency Feedwater	$\leq$ _____*/_____**
11. <u>Steam Generator <math>\Delta P</math>-High-Coincident With Steam Generator Level Low</u>	
a. Emergency Feedwater	$\leq$ _____*/_____**
12. <u>Steam Generator Level - High</u>	
a. <u>Main Feedwater Isolation</u>	$\leq$ _____

NOTE: Response time for Motor-Driven Auxiliary Feedwater Pumps on all S.I. signal starts  $\leq$  (60.0)

TABLE NOTATION

\* Diesel generator starting and sequence loading delays included. Response time limit includes movement of valves and attainment of pump or blower discharge pressure.

\*\* Diesel generator starting and sequence loading delays not included. Offsite power available. Response time limit includes movement of valves and attainment of pump or blower discharge pressure.

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION SURVEILLANCE REQUIREMENTS

FUNCTIONAL UNIT	CHANNEL CHECK	CHANNEL CALIBRATION	CHANNEL FUNCTIONAL TEST	MODES FOR WHICH SURVEILLANCE IS REQUIRED
10. EMERGENCY FEEDWATER (EFAS)				
a. Manual (Trip Buttons)	N.A.	N.A.	R	N.A.
b. SG Level and Pressure (A/B)-Low and ΔP (A/B) - High	S	R	M	1, 2, 3
c. SG Level (A/B) - Low and No Pressure - Low Trip (A/B)	S	R	M	1, 2, 3
d. Automatic Actuation Logic	N.A.	N.A.	M(1)	1, 2, 3
e. S.I.	(See 1 above (S.I. Surveillance Requirements))			

3/4 3-26-78

11. Manual Feedwater Isolation  
 a. SG level - High  
 b. Automatic Actuation Logic

Repeat as stated



TABLE NOTATION

- (1) Each train or logic channel shall be tested at least every 62 days on a STAGGERED TEST BASIS.
- (2) The CHANNEL FUNCTIONAL TEST shall include exercising the transmitter by applying either a vacuum or pressure to the appropriate side of the transmitter.



INSTRUMENTATION3/4.3.2 ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATIONLIMITING CONDITION FOR OPERATION

3.3.2 The Engineered Safety Feature Actuation System (ESFAS) instrumentation channels shown in Table 3.3-3 shall be OPERABLE with their trip setpoints set consistent with the values shown in the Trip Setpoint column of Table 3.3-4 and with RESPONSE TIMES as shown in Table 3.3-5.

APPLICABILITY: As shown in Table 3.3-3.

ACTION:

- a. With an ESFAS instrumentation channel trip setpoint less conservative than the value shown in the Allowable Values column of Table 3.3-4, declare the channel inoperable and apply the applicable ACTION requirement of Table 3.3-3 until the channel is restored to OPERABLE status with the trip setpoint adjusted consistent with the Trip Setpoint Value.
- b. With an ESFAS instrumentation channel inoperable, take the action shown in Table 3.3-3.

SURVEILLANCE REQUIREMENTS

4.3.2.1 Each ESFAS instrumentation channel and bypass shall be demonstrated OPERABLE by the performance of the CHANNEL CHECK, CHANNEL CALIBRATION and CHANNEL FUNCTIONAL TEST operations for the MODES and at the frequencies shown in Table 4.3-2.

4.3.2.2 The ENGINEERED SAFETY FEATURES RESPONSE TIME of each ESFAS function shall be demonstrated to be within the limit at least once per 18 months. Each test shall include at least one channel per function such that all channels are tested at least once every N times 18 months where N is the total number of redundant channels in a specific ESFAS function as shown in the "Total No. of Channels" Column of Table 3.3-3.

TABLE 3.3-3 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEMS INSTRUMENTATION

<u>FUNCTIONAL UNIT</u>	<u>TOTAL NO. OF CHANNELS</u>	<u>CHANNELS TO TRIP</u>	<u>MINIMUM CHANNELS OPERABLE</u>	<u>APPLICABLE MODES</u>	<u>ACTION</u>
<b>8. AUXILIARY FEEDWATER</b>					
a. Manual Initiation	2	1	2	1, 2, 3	16
b. Steam Generator Pressure-Low	4/steam generator	2/steam generator	3/steam generator	1, 2, 3**	10#
c. Steam Generator Level-Low	4/steam generator	2/steam generator	3/steam generator	1, 2, 3	10#
d. Reactor Coolant Pumps Tripped	4	2	3	1, 2, 3**	10#
e. Containment Pressure-High	4	2	3	1, 2, 3	10#
f. Automatic Actuation Logic	2	1	2	1, 2, 3	15
g. Trip of Main Feedwater Pumps	3/pump	2/pump	2/pump	1, 2**	3
<b>9. ENGINEERED SAFETY FEATURE ACTUATION SYSTEM BYPASSES</b>					
a. Reactor Coolant System Pressure	1/channel	1/channel	1/operating channel	1, 2, 3	17
b. Steam Generator Pressure	1/channel	1/channel	1/operating channel	1, 2, 3	17
c. Containment Pressure	1/channel	1/channel	1/operating channel	1, 2, 3, 4	17
<b>10. MAIN FEEDWATER ISOLATION</b>					
a. Steam Generator level-High	1	1	1	1	1

*Repeat as stated*

B&W-ST5

3/4 3-13

SEP 21 1980

TABLE 3.3-4 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEMS INSTRUMENTATION TRIP SETPOINTS

FUNCTIONAL UNIT

TRIP SETPOINT

ALLOWABLE VALUES

8. AUXILIARY FEEDWATER

- |                                  |                      |                      |
|----------------------------------|----------------------|----------------------|
| a. Manual Initiation             | Not Applicable       | Not Applicable       |
| b. Steam Generator Pressure-Low  | < ( ) psig           | < ( ) psig           |
| c. Steam Generator Level-Low     | < ( ) feet           | < ( ) feet           |
| d. Reactor Coolant Pumps-Tripped | Loss of 2 or 4 Pumps | Loss of 2 or 4 Pumps |
| e. Containment Pressure-High     | < (5) psig           | < (5) psig           |
| f. Automatic Actuation Logic     | Not Applicable       | Not Applicable       |
| g. Trip of Main Feedwater Pumps  | Not Applicable       | Not Applicable       |

9. ENGINEERED SAFETY FEATURE ACTUATION SYSTEM BYPASSES

- |                                    |                |                |
|------------------------------------|----------------|----------------|
| a. Reactor Coolant System Pressure | (1600)         | ( )            |
| b. Steam Generator Pressure        | (725)          | ( )            |
| c. Containment Pressure            | Not Applicable | Not Applicable |

10. MAIN FEEDWATER ISOLATION

- |                               |            |            |
|-------------------------------|------------|------------|
| 1. Steam Generator Level-High | ≤ ( ) feet | ≤ ( ) feet |
|-------------------------------|------------|------------|

B&W-ST5

3/4 3-18

TABLE 3.3-5 (Continued)

<u>INITIATING SIGNAL AND FUNCTION</u>	<u>RESPONSE TIME IN SECONDS</u>
8. <u>4.16 kv Emergency Bus Undervoltage (Loss of Voltage)</u> Loss of Power	$\leq ( )^*$
9. <u>4.16 kv Emergency Bus Undervoltage (Degraded Voltage)</u> Loss of Power	$\leq ( )^*$
10. <u>Steam Generator Pressure-Low</u> Auxiliary Feedwater System Main Steam Isolation	$\leq ( )^*/( )^{**}$ $\leq ( )^*/( )^{**}$
11. <u>Steam Generator Level-Low</u> Auxiliary Feedwater System	$\leq ( )^*/( )^{**}$
12. <u>Reactor Coolant Pumps-Tripped</u> Auxiliary Feedwater System	$\leq ( )^*/( )^{**}$
13. <u>Trip of Main Feedwater Pumps</u> Auxiliary Feedwater System	$\leq ( )^*/\leq ( )^{**}$

TABLE NOTATION

\*Diesel generator starting and sequence loading delays included. Response time limit includes movement of valves and attainment of pump or blower discharge pressure.

\*\*Diesel generator starting and sequence loading delays not included. Offsite power available. Response time limit includes movement of valves and attainment of pump or blower discharge pressure.

14. *Main Feedwater Isolation*

$\leq ( )$

TABLE 4.3-2 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEMS INSTRUMENTATION SURVEILLANCE REQUIREMENTS

FUNCTIONAL UNIT	CHANNEL CHECK	CHANNEL CALIBRATION	CHANNEL FUNCTIONAL TEST	MODES FOR WHICH SURVEILLANCE IS REQUIRED
b. 4.16 kv Emergency Bus Undervoltage (Degraded Voltage)	S	R	M	1, 2, 3, 4
<b>8. AUXILIARY FEEDWATER</b>				
a. Manual Initiation	N.A.	N.A.	M(1)	1, 2, 3
b. Steam Generator Pressure-Low	S	R	M	1, 2, 3
c. Steam Generator Level-Low	S	R	M	1, 2, 3
d. Reactor Coolant Pumps-Tripped	S	R	M	1, 2, 3
e. Containment Pressure-High	S	R	M(3)	1, 2, 3
f. Automatic Actuation Logic	N.A.	N.A.	M(2)	1, 2, 3
g. Trip of Main Feedwater Pumps	N.A.	N.A.	R	1, 2
<b>9. ENGINEERED SAFETY FEATURE ACTUATION SYSTEM BYPASSES</b>				
a. Reactor Coolant System Pressure	N.A.	R(4)	S/U(5)	1, 2, 3
b. Steam Generator Pressure	N.A.	R(4)	S/U(5)	1, 2, 3
c. Containment Pressure	N.A.	R(4)	N.A.	1, 2, 3, 4

B&W-ST5

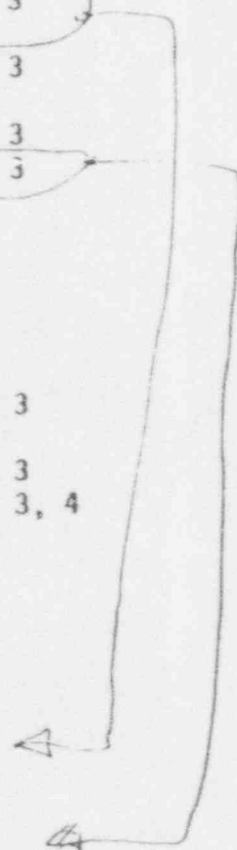
3/4 3-23

10 MAIN FEEDWATER ISOLATION

a. Steam Generator Level-High

b. Automatic Actuation Logic

Repeat as stated





INSTRUMENTATION3/4.3.2 ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATIONLIMITING CONDITION FOR OPERATION

3.3.2 The Engineered Safety Feature Actuation System (ESFAS) instrumentation channels and bypasses shown in Table 3.3-3 shall be OPERABLE with their trip setpoints set consistent with the values shown in the Trip Setpoint column of Table 3.3-4 and with RESPONSE TIMES as shown in Table 3.3-5.

APPLICABILITY: As shown in Table 3.3-3.

ACTION:

- a. With an ESFAS instrumentation channel trip setpoint less conservative than the value shown in the Allowable Values column of Table 3.3-4, declare the channel inoperable and apply the applicable ACTION requirement of Table 3.3-3 until the channel is restored to OPERABLE status with the trip setpoint adjusted consistent with the Trip Setpoint value.
- b. With an ESFAS instrumentation channel inoperable, take the ACTION shown in Table 3.3-3.

SURVEILLANCE REQUIREMENTS

4.3.2.1 Each ESFAS instrumentation channel shall be demonstrated OPERABLE by the performance of the CHANNEL CHECK, CHANNEL CALIBRATION and CHANNEL FUNCTIONAL TEST operations for the MODES and at the frequencies shown in Table 4.3-2.

4.3.2.2 The logic for the bypasses shall be demonstrated OPERABLE during the at power CHANNEL FUNCTIONAL TEST of channels affected by bypass operation. The total bypass function shall be demonstrated OPERABLE at least once per 18 months during CHANNEL CALIBRATION testing of each channel affected by bypass operation.

4.3.2.3 The ENGINEERED SAFETY FEATURES RESPONSE TIME of each ESFAS function shall be demonstrated to be within the limit at least once per 18 months. Each test shall include at least one channel per function such that all channels are tested at least once every  $N$  times 18 months where  $N$  is the total number of redundant channels in a specific ESFAS function as shown in the "Total No. of Channels" Column of Table 3.3-3.

TABLE 3.3-3 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION

<u>FUNCTIONAL UNIT</u>	<u>TOTAL NO. OF CHANNELS</u>	<u>CHANNELS TO TRIP</u>	<u>MINIMUM CHANNELS OPERABLE</u>	<u>APPLICABLE MODES</u>	<u>ACTION</u>
9. LOSS OF POWER (LOV)					
a. 4.16 kv Emergency Bus Undervoltage (Loss of Voltage)	4/Bus	2/Bus	3/Bus	1, 2, 3	12
b. 4.16 kv Emergency Bus Undervoltage (Degraded Voltage)	4/Bus	2/Bus	3/Bus	1, 2, 3	12
10. EMERGENCY FEEDWATER (EFAS)					
a. Manual (Trip Buttons)	2 sets of 2 per S/G	1 set of 2 per S/G	2 sets of 2 per S/G	1, 2, 3	16
b. Automatic Actuation Logic	4/SG	2/SG	3/SG	1, 2, 3	14*, 15*
c. SG Level and Pressure (A/B) - Low and WP (A/B) - High	4/SG	2/SG	3/SG	1, 2, 3	13*
d. SG Level (A/B) - Low and No S/G Pressure - Low Trip (A/B)	4/SG	2/SG	3/SG	1, 2, 3	13*
e. Safety Injection	See 1 above for all Safety Injection Initiating Functions and Requirements				

11. MAIN FEEDWATER INSTRUMENTATION

- a. SG Level - High
- b. Automatic Actuation Logic

*Repeat as stated*

CE-ST5

3/4 3-17

JUL 09 1982

TABLE 3.3-4 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION TRIP VALUES

<u>FUNCTIONAL UNIT</u>	<u>TRIP VALUE</u>	<u>ALLOWABLE VALUES</u>
8. CONTAINMENT COOLING (CCAS)		
a. Manual (Trip Buttons)	Not Applicable	Not Applicable
b. Containment Pressure - High	$\leq (18.4)$ psia	$\leq (19.02)$ psia
c. Pressurizer Pressure - Low	$\geq (1740)$ psia	$\geq (1686.7)$ psia
d. Automatic Actuation Logic	Not Applicable	Not Applicable
9. LOSS OF POWER		
a. 4.16 kv Emergency Bus Undervoltage (Loss of Voltage)	(3120) volts	(3120) volts
b. 4.16 kv Emergency Bus Undervoltage (Degraded Voltage)	(423) $\pm$ (2.0) volts with an (8.0 $\pm$ 0.5) second time delay	(423) $\pm$ (4.0) volts with an (8.0 $\pm$ 0.8) second time delay
10. EMERGENCY FEEDWATER (EFAS)		
a. Manual (Trip Buttons)	Not Applicable	Not Applicable
b. Steam Generator (A&B) Level-Low	$\geq (46.5)\%$	$\geq (45.61)\%$
c. Steam Generator $\Delta P$ -High (SG-A > SG-B)	$\leq (39)$ psi	$\leq (48.35)$ psi
d. Steam Generator $\Delta P$ -High (SG-B > SG-A)	$\leq (39)$ psi	$\leq (48.35)$ psi
e. Steam Generator (A&B) Pressure - Low	$\geq (728)$ psia	$\geq (706.6)$ psia
f. Safety Injection	See I above for all Safety Injection Initiating Functions and Requirements	
g. Automatic Actuation Logic	Not Applicable	Not Applicable

11. MAIN FEEDWATER ISOLATION

a. Steam Generator Level-High

 $\leq ( ) \%$  $\leq ( ) \%$ 

CE-STS

2/4 3-22

DES 2 - 1901

TABLE 3.3-5 (Continued)

ENGINEERED SAFETY FEATURES RESPONSE TIMES

<u>INITIATING SIGNAL AND FUNCTION</u>	<u>RESPONSE TIME IN SECONDS</u>
10. <u>Steam Generator Level-Low</u>	
a. Emergency Feedwater	$\leq$ _____*/_____**
11. <u>Steam Generator <math>\Delta</math>P-High-Coincident With Steam Generator Level Low</u>	
a. Emergency Feedwater	$\leq$ _____*/_____**
12. <u>Steam Generator Level-High</u>	
a. Main Feedwater Isolation	$\leq$ _____

NOTE: Response time for Motor-Driven  
Auxiliary Feedwater Pumps on all  
S.I. signal starts  $\leq$  (60.0)

TABLE NOTATION

\* Diesel generator starting and sequence loading delays included. Response time limit includes movement of valves and attainment of pump or blower discharge pressure.

\*\* Diesel generator starting and sequence loading delays not included. Offsite power available. Response time limit includes movement of valves and attainment of pump or blower discharge pressure.

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION SURVEILLANCE REQUIREMENTS

<u>FUNCTIONAL UNIT</u>	<u>CHANNEL CHECK</u>	<u>CHANNEL CALIBRATION</u>	<u>CHANNEL FUNCTIONAL TEST</u>	<u>MODES FOR WHICH SURVEILLANCE IS REQUIRED</u>
10. EMERGENCY FEEDWATER (EFAS)				
a. Manual (Trip Buttons)	N.A.	N.A.	R	N.A.
b. SG Level and Pressure (A/B)-Low and ΔP (A/B) - High	S	R	M	1, 2, 3
c. SG Level (A/B) - Low and No Pressure - Low Trip (A/B)	S	R	M	1, 2, 3
d. Automatic Actuation Logic	N.A.	N.A.	M(1)	1, 2, 3
e. S.I.	(See 1 above (S.I. Surveillance Requirements))			

3/4 3-26-78

11. MAIN FEEDWATER ISOLATION  
 a. SG level - High  
 b. Automatic Actuation Logic

repeat as stated

TABLE NOTATION

- (1) Each train or logic channel shall be tested at least every 62 days on a STAGGERED TEST BASIS.
- (2) The CHANNEL FUNCTIONAL TEST shall include exercising the transmitter by applying either a vacuum or pressure to the appropriate side of the transmitter.