NRC FORM 426A (2-79) NCRM 3201

U.S. NUCLEAR REGULATORY COMMISSION

PUBLICATIONS RELEASE FOR UNCLASSIFIED NRC CONTRACTOR AND CONSULTANT REPORTS

(Please Type or Print)

1. REPORT NUMBER *(If any)*: BNL-NUREG-36799

2. DISTRIBUTION CATEGORY NO. *(If any)*:

Obtain in advance Division of Technical Information and Document Control

Insert appropriate from the NRC Distribution Category List (see NUREG-0550)

3. TITLE AND SUBTITLE *(State in full as shown on document)*

Systems Interaction Study of a Westinghouse PWR

4. AUTHORS *(If more than three, name first author followed by "and others")*

R. Youngblood and others

5. NAME OF CONTRACTOR: Brookhaven National Laboratory

MAILING ADDRESS *(Number and street, city, state and zip code)*: Upton, NY 11973

TELEPHONE No.: 666-2815

6. DATE MANUSCRIPT COMPLETED: July 8, 1985

7. NRC PROGRAM SPONSOR/TECHNICAL MONITOR: E. Chelliah

TELEPHONE No.: 492-8338

8. CONTRACT DATA

a. CONTRACT OR FIN NUMBER *(Do not list DOE contract number)*: 3725

b. IF CONTRACTOR IS AUTHORIZED TO PRINT, PLEASE PROVIDE THE FOLLOWING INFORMATION

Number of Copies Printed	Estimated Composition Cost	Estimated Printing Cost

9. TYPE OF DOCUMENT *(Check appropriate box)*

- [ ] a. TECHNICAL REPORT
  - (1) FORMAL
  - (2) INTERIM
- [X] b. CONFERENCE PAPER
  - (1) TITLE OF CONFERENCE PAPER: Nuclear Power Plant Aging, Availability Factor & Reliability Analysis
  - (2) DATE(S) OF CONFERENCE: July 8-12, 1985
  - (3) LOCATION OF CONFERENCE: San Diego, CA
- [ ] c. OTHER *(Indicate type of item, e.g., thesis, speech, journal article, guide, etc.)*

10. SPECIAL DISTRIBUTION *(Send all copies to the Distribution Services Branch, Division of Technical Information and Document Control.) (Specify special instructions such as "Make available only as specifically approved by program office," or "Send to attached addressees." Submit addressed mailing labels for special distribution. Continue instructions on reverse or separate sheet if necessary.)*

11. PATENT CLEARANCE *(If applicable)*

Forward completed, signed NRC Form 426A together with the related documents for review, TO: Appropriate Patent Counsel

- [ ] a. PATENT CLEARANCE NOT REQUIRED
- [X] b. PATENT CLEARANCE GRANTED
- [ ] c. PATENT CLEARANCE DENIED

d. PATENT COUNSEL'S SIGNATURE | DATE

12. SUBMITTED BY

a. NAME OF AUTHORIZED CONTRACTOR OFFICIAL OR NRC MONITOR *(Type or print)*

b. OFFICIAL'S ORGANIZATIONAL UNIT: Department of Nuclear Energy

c. SIGNATURE *(Authorized contractor official or NRC Monitor)* | DATE: 7/11/85

BNL-NUREG-36799

Systems Interaction Study of a Westinghouse PWR*

R. Youngblood, N. Hanan, R. Fitzpatrick, D. Xue,
G. Bozoki, A. Fresco, I. A. Papazoglou
Department of Nuclear Energy
Brookhaven National Laboratory
Upton, New York 11973

Abstract

This paper presents methods and findings of a systems interaction study of Indian Point 3. The study was carried out in support of the resolution of Unresolved Safety Issue A-17 on Systems Interactions. Fault tree methods were employed. Among the study's findings is a single active failure in the low pressure injection function; this discovery led to a plant modification.

THE PURPOSE of this paper is to report methods and findings of a systems interaction study[1] conducted at Brookhaven National Laboratory in support of the resolution in Unresolved Safety Issue (USI) A-17. In addition to providing support to the staff in resolving USI A-17[2], the project discovered[3] an important new class of failure modes which led the utility to implement a hardware modification.[4] Below, the scope of the project is indicated, key features of the method are highlighted, principal findings are discussed, and comments are offered on the usefulness of this type of study.

SCOPE

Several years ago, NRC solicited recommendations on how best to study systems interactions. Brookhaven National Laboratory (BNL) recommended[5] a staged application of fault trees and interacting failure modes and effects analyses (FT/IFMEA). Lawrence Livermore National Laboratory (LLNL) recommended an alternative ("digraph") method of generating cut sets.[6] Subsequently, each laboratory was contracted by NRC to apply its recommended method to a specified problem, for purposes of comparing the two approaches. To simplify NRC's methodology comparison, BNL and LLNL were directed to cover essentially the same ground, i.e., analyze a prescribed set of accident sequences. In addition, to preclude duplication of ongoing efforts to resolve other safety issues, certain topics were declared out of scope, notably "Human Factors" and control systems.

In this study, a systems interaction corresponds to a reduction of the ostensible redundancy of the system(s) performing a safety function. This includes, but is not limited to, violations of the single failure criterion. Three types of systems interaction have been addressed in this study: functional, spatial, and induced-human. Functional interactions are cases in which a functional failure leads, through hardware dependences, to effective reduction in redundancy; an example is hardware shared between trains. Spatial interactions propagate from one component to another spatially, rather than functionally; an example is a pipe rupture near an instrument rack, causing it to fail. "Induced-human" refers to cases in which an operator who is correctly following procedures is induced by an instrument failure to take actions which are counterproductive or nonproductive to safety.

METHOD

The method employs technique which are standard tools of PRA, namely, fault trees and event trees. However, emphasis is placed on obtaining results from the model before details of individual components are developed and after support system faults are reflected in the model. A given frontline system is modeled to a level of detail corresponding to segments, or supercomponents consisting of elements in series; local faults whose sole effect is to fail a given supercomponent are coalesced into a single event amounting to "local fault of the

*Work performed under the auspices of the U.S. Nuclear Regulatory Commission.
Views expressed are not necessarily those of the Nuclear Regulatory Commission.

supercomponent," while all support faults are treated explicitly. The resulting fault tree is not detailed in its treatment of local faults, but is logically complete in the sense that all possible system failures are implicit in some combination of the coalesced event groups which are the building blocks of the model. Leading cut sets of the resulting fault trees can easily be obtained; as a result of the disciplined approach outlined above, the computational problem is far less severe than it is when detailed lists of individual failure modes are explicitly incorporated into the logic. The cut sets of the resulting fault trees explicitly display combinations of support system faults and front-line system faults in a format which lends itself to review and understanding. It is emphasized that low-probability events are not omitted from the model; all credible events are implicitly modeled, but are subsumed into one or another of the supercomponent local fault events.

Emphasis has also been given to proper conditioning of the failure events on the character of the initiating event. A fault tree for transient initiators was developed, based on FMEA of support system faults. Certain conditions were explicitly displayed on the fault trees: presence of an SI signal, whether or not the LOCA was "small," bus undervoltage signal, etc. NOT logic was used to distinguish failure modes appropriate to different conditions.

Studies of spatial interactions and induced-human interactions are based on the functional model. Cut sets of the functional model can be examined to see whether spatial or induced-human coupling can "shorten" them by causing two or more events to become effectively a single event. Information regarding locations of components can be incorporated directly into the model, as can information from reactor operator task analyses which would show what instrument conditions might cause an operator to propagate a fault.

As outlined above, the model was constructed to yield the minimum number of cut sets which would still properly reflect the logic of the system and span the appropriate range of failure modes. These cut sets were then culled by the following criteria. In the BNL study, to qualify as a "finding," a cut set was required:

a) to have been previously undiscovered, i.e., not part of IPPSS;
b) to exceed 10^{-8} events/yr in frequency, quantified with IPPSS data;
c) to correspond to a systems interaction;
d) to represent either a functional, spatial, or induced-human coupling.

It was found that most cut sets emerging from the model were either already well known, were extremely unlikely, or represented a severe conservatism. These were relegated to an appendix in the report[1], while the remaining handful were discussed further. Here, an example will be given to illustrate the culling process. In the following subsection, "findings" and candidates for further analysis will be presented.

Cut set number 12 in the results for the RCP * U core damage sequence (RCP seal LOCA * failure of high pressure injection) is "TR-LOOP * SWN17-A." TR-LOOP is loss of offsite power, and represents the initiating event in this case, and SWN17-A is insufficient flow through nuclear service water segment number 17. This segment supplies nuclear service water to all three diesels, and, as one would expect, appears in a relatively large number of cut sets in a number of sequences. This particular cut set emerges from the model for this sequence because the support systems required to cool the RCP seals lose power, and the HPI system needed to mitigate the postulated resulting seal LOCA also loses power. This is correct as far as it goes, but it does not go far enough. Before considering time available for recovery, consider the event SWN17-A. This segment can itself cause insufficient flow by rupturing, by being plugged, or by having a manual valve plugged or closed. In short, either a passive failure or a human error is necessary to cause this event. "Induced-human" causes for this were sought and not found, there being no indication which could induce an operator acting by procedures to deprive the diesels of cooling. Human error is arguably possible (always) but both labs were directed by NRC to confine modeling the human to the induced-human area; although some aspects of plant design forced the study to acknowledge the role of the operators, BNL did not quantify classical procedural errors as part of the study. Even if a screening probability is assigned to this error, it must then be considered that:

a) offsite power must be lost for a very long time unless extremely high leak rates are postulated;
b) the diesels must be irretrievably damaged in the first place, in spite of no other failures having occurred to distract the operators' attention from the status of the diesels;
c) power can be made available from the gas turbines.

To summarize, then, this cut set and a number of similar ones were considered by BNL in the culling process, and included in an appendix. The comments by LLNL[3] and others[2] that BNL did not "find" this interaction should be modified to indicate that while BNL explicitly lists this cut set among the results of its model, only LLNL has chosen to assign a high frequency of core damage to this sequence.

Table 1 - Examples of How Each Top Event Can Be Caused from Within the Indicated Zones

Top Event	Zone	Example of Component Combination Residing in Zone, and Capable of Causing Top Event.
D (LPI failure)	F3	RHR pump 31 and cabling for RHR pump 32.
	F4A	Cabling for RHR pumps 31 and 32.
	F7A	Cabling for RHR pumps 31 and 32.
	F9A	Cabling for RHR pumps 31 and 32.
	F11A	Cabling for RHR pumps 31 and 32.
	F12A	Cabling for RHR pumps 31 and 32.
	F14	Cabling for RHR pumps 31 and 32.
	F15	Cabling for RHR pumps 31 and 32.
	F13	Battery 32.
	F17	MCC 36A & MCC36B (power for LPI valves).
U_2 (HPI given small LOCA)	F9	HPI pumps 31, 32, 33.
	F11	Cabling for HPI pumps 31, 32, 33.
	F14	
	F15	
	F17A	
U_1 (HPI given medium LOCA)	All zones applicable to U_2.	
	F60A	Cabling for HPI pumps 31 and 33.
L (AFWS Failure)	F11	Cabling for AFWS pumps 31, 32, 33.
	F14	Cabling for AFWS pumps 31, 32, 33.
	F15	Cabling for AFWS pumps 31, 32, 33.
	F23	Location of AFWS pumps 31, 32, 33.
T*L	F11	Cable spreading room: cabling for SW & CCW pumps and AFW pump.
	F14	Switchgear room: transient (e.g., Loss of CCW or SW) and cabling of AFW pumps.
	F15	Control room (transient and loss of pump control)
$S_2(P)$	F11	Cable spreading room: cables for CCW pumps and charging pumps.
	F14	Switchgear room: cables for CCW pumps and charging pumps.
	F15	Control room (control of CCW pumps and charging pumps).
	F17A	CCW heat exchangers and cabling for charging pumps.
$S_2(P)*U_2$	F11	See table above for zones yielding $S_2(P)$ and zones yielding U_2
	F14	
	F15	
	F17A	
$S_2(P)*L$	F11	See table above for zones yielding $S_2(P)$ and zones yielding L.)
	F14	
	F15	

FINDINGS

SPATIAL INTERACTIONS - Table 1 illustrates candidate spatial interactions. Each table entry notes a critical combination of components located within a fire zone[7]; these combinations are therefore candidates for physical analysis to see whether any credible event could degrade all components in the combination. Physical analysis of this sort is beyond the scope of the project.

FUNCTIONAL INTERACTIONS - It was found that loss of dc at power panel 32 has pervasive effects in several accident sequences. Most notably, loss of battery 32 prevents automatic actuation of low pressure injection (LPI) following a large or medium LOCA. The situation is illustrated in Figure 1. The two LPI pumps (denoted RHR 31 and 32 in the figure) derive power from 480-V ac buses 3A and 6A. In the event of a LOCA, the safeguards actuation signal causes MCC37 to be shed from bus 6A, leaving dc power panel 32 dependent on the battery. If the battery is unavailable, there is no control dc to operate the breaker of RHR pump 32. Dc power panel 32 also controls fast transfer of 6.9-kV bus 3; without battery 32, then, 480-V bus 3A loses offsite power and RHR Pump 31 loses power as a result. Before the recent plant modification, no automatic action restored power to 480-V Bus 3A because tie breaker 2AT3A was configured to close only on closure of the DG31 breaker, which does not occur in the present scenario because 480-V bus 2A never loses voltage. Therefore, given unavailability of battery 32, a safeguards signal leaves RHR 32 without control dc and leaves RHR 31 without ac power. The recent modification changes the logic of breaker 2AT3A so that in this scenario it will automatically close, powering 3A from 2A and allowing RHR 31 to function.

CONCLUSIONS

After developing a plant model and obtaining its preliminary cut sets, BNL applied stringent criteria to these cut sets to assess their significance. As would be expected for a plant which had undergone a major PRA, a licensing process, and several years of operation, the probabilistic weight of the cut sets surviving these criteria for the handful of sequences analyzed is not great (somewhat less than 10^{-5} per year). On the other hand, a study of this type will not normally be carried out for plants which have already undergone full-scope PRAs. It is much more natural to perform a study of this type as part of a PRA. Therefore, the highly constrained set of "findings" emerging from BNL's rather stringent criteria is too pessimistic a yardstick for assessing the probable benefits of a study of a plant lacking a PRA.

Even following the PRA, this study found an important new class of system failure modes which led the utility to implement an immediate hardware modification. This finding resulted from a systematic development of support system failure modes which was logically complete, but sufficiently disciplined in its level of detail that an explicit determination of leading fully linked cut sets was feasible. It is noteworthy that the finding emerged from a systematic computerized application of logic techniques, and was not anticipated by any of the analysts.

The conclusion is that a PRA which explicitly develops all support system faults and generates fully-linked cut sets is an important contribution to understanding a plant and helping to assure that there are no previously unsuspected interactions.

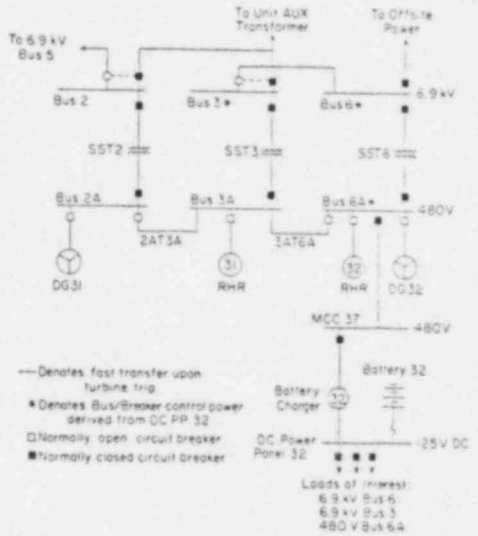

Figure 1 Indian Point 3 Electrical Power System Normal Configuration.

REFERENCES

1. Youngblood, R., N. Hanan, R. Fitzpatrick, D. Xue, G. Bozoki, A. Fresco, I. A. Papazoglou, S. Mitra, G. MacDonald, and T. Mazour, "Fault Tree Application to the Study of Systems Interactions at Indian Point 3, (NUREG/CR-4207, April 1985).

2. "RRAB Inputs to the USI A-17 Program, NRC memorandum from A. Thadani, Reliability and Risk Assessment Branch, to K. Kniel, Generic Issues Branch (March 20, 1985).

3. "Daily Highlight - Loss of RHR at the Indian Point Nuclear Generating Plant, Unit No. 3 (IP-3)," NRC memorandum from P. J. Polk to H. Denton, Docket No. 50-286 (July 1984).

4. "Final Modification to Engineered Safeguards Features to Mitigate Potential Consequences of Battery No. 32 Failures," Attachment to letter from J. P. Bayne (NY Pa) to S. Varga (NRC), Docket No. 50-286 (October 31, 1984).

5. Buslik, A., I. A. Papazoglou, and R. A. Bari, "Review and Evaluation of Systems Interactions Methods" (NUREG/CR-1901, 1981).

6. Alesso, H. P., I. J. Sacks, and C. F. Smith, "Initial Guidance on Digraph-Matrix Analysis for Systems Interaction Studies (NUREG/CR-2915, 1983).

7. Review of the Indian Point Station Fire Protection System, Consolidated Edison Company of New York and Power Authority of the State of New York (December 1976).

8. Indian Point Probabilistic Safety Study, Power Authority of the State of New York, Consolidated Edison Company, New York, Inc. (1982).

9. Alesso, H. P., et al., "Digraph Matrix Analysis of System Interaction at Indian Point-3," (NUREG/CR-4179 Draft, Vol. 1, August 1984).