UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, D. C. 20555
February 20, 1980

The Honorable Morris K. Udall, Chairman
Committee on Interior and Insular Affairs
House of Representatives
Washington, D. C. 20515

Dear Congressman Udall:

In a letter dated July 27, 1979, you expressed the hope that the study of Licensee Event Reports by the Advisory Committee on Reactor Safeguards would address the consistency of actual component failure experience (e.g. valve failure rates) with that projected in WASH-1400. You also asked the ACRS to determine the probabilities of occurrence that, prior to the events, would have been predicted for the sequences of events that occurred at Davis-Besse on September 24, 1977 and at Rancho Seco on March 20, 1978 on the basis of WASH-1400 failure rates and methodology. In a letter dated August 15, 1979, the ACRS advised you that it would undertake to provide a detailed response to your requests and that it hoped to be able to complete this effort in approximately six months.

Of course, the calculation of the probability of an event sequence, in retrospect, is ill-defined, since it depends entirely upon the ensemble of event sequences in which the one under discussion is embedded. This letter includes what are thought to be reasonable judgments on this point, and the results depend upon these judgments.

With the aid of the NRC Staff, the ACRS invited a large number of institutions in the U.S. and abroad, including the Electric Power Research Institute and the U.S. reactor vendors, to provide data and analyses responsive to your request. Several groups, including the NRC Staff itself, have submitted component failure rate data developed since the compilation was made for the Reactor Safety Study, WASH-1400. The NRC Staff have summarized the new data in Table 1, which also provides the failure rates used in WASH-1400 for the same components and systems. Some of the information in Table 1 is plotted in Figure 1 and illustrates graphically the considerable spread in data obtained and the relative position of WASH-1400. Also of some interest is the considerable variation observed from plant to plant which is illustrated in Figure 2. Only plants which reported any failures are shown in Figure 2; hence, some plants had much higher failure rates than WASH-1400 on certain components while other plants had no failures during the reporting period studied. Although to some degree the observed variation may reflect actual differences from plant to plant, a certain portion of the variation may be due to differences in the reporting requirements specified in the individual plant Technical Specifications and to differences in the responses of reporting personnel.

Turbine-driven pumps generally exhibit a higher failure rate (a factor of 10 to 100) than used in WASH-1400. The NRC Staff is now giving extra attention to this specific item. Furthermore, a large variation in diesel reliability was observed among the various plants.

The NRC Staff believe that the uncertainties in failure rate data are larger than were projected in WASH-1400, and that the general trend is toward somewhat higher failure rates. Their preliminary assessment is that this might produce an increase in their best estimate of core melt probability by about a factor of three.

None of the groups who were invited have provided probabilistic analyses, using WASH-1400 failure rates and methodology, of the Rancho Seco and Davis-Besse transients of March 20, 1978 and September 24, 1977 respectively. The ACRS, therefore, asked three ACRS Fellows to devote effort commensurate with the time available to provide such analyses; the results of their study are included as Attachment A to this letter.

The ACRS believes that the results they obtained are reasonable. It is clear that the manner of treatment of human error can have a very large effect on the results obtained. Also, for the Rancho Seco transient, the numerical results are very sensitive to the context in which failure of control system power is calculated.

The ACRS Fellows also estimated a probability per reactor year of occurrence of the major sequences which were present in the Three Mile Island 2 accident of March 28, 1979. Of some interest in this regard is an observation by representatives of Electricite de France that by applying WASH-1400 methodology they would calculate an overall probability of the order of $3x10^{-7}$ for TMI-2, but when the events were connected by strategic operator errors, they found a probability as high as $6x10^{-3}$.

The ACRS anticipates that, had several institutions provided independent estimates of the probability of the two transients, a considerable variation in their answers would have been likely.

Although the NRC Staff did not analyze the probability of the Rancho Seco transient using WASH-1400 failure rate data and methodology, they did provide the ACRS with two related memoranda, which are enclosed as Attachments B and C for your possible interest.

The ACRS trusts that this letter is responsive to your request.

Sincerely,

Milton S. Plesset

Milton S. Plesset
Chairman

Attachments:

A. ACRS Fellows Report, "Analysis of Feedwater Transient Sequences in B&W Nuclear Steam Supply Systems," February 7, 1980

B. Nuclear Regulatory Commission Staff Report, "Evaluation of Davis-Besse and Rancho Seco Feedwater Transients on 9/24/77 and 3/20/78 Using WASH-1400 Data"

C. Memorandum from F. Rowsome to R. Fraley, "ACRS Query on Material Relevant to Udall Letter: Davis-Besse and Rancho Seco Transients," February 12, 1980

TABLE 1
SUMMARY OF CURRENT FAILURE RATE DATA SURVEY

		(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)
COMPONENT	FAIL MODE	BIBLIS	GENERAL ATOMIC	LER EVALUATION PROGRAM	NCSR	NPRDS	WASH-1400	WESTINGHOUSE	VOLTA	PICKARD, LOWE AND GARRICK	BECHTEL
AUX FEED PUMPS	FAIL TO START		+1E-2(3)					2.0E-5			1.7E-5
	FAIL TO RUN		1E-4(3/10)					1.2E-5			
ECCS PUMPS	FAIL TO START	+8.1E-3	+1E-3(3/10)	+2.7E-3	+2E-5	3.9E-5	+1E-3(3)		+1E-3	+1E-3(3)	
	FAIL TO RUN			(2.3-12)E-6	3.5E-4		3E-5(10)		(6-200)E-6	3E-5(10)	
	FAIL TO START & RUN							1.5E-5A			
MANUAL VALVES	'FAIL TO OPERATE		+1E-3(3)		6.3E-6					1E-4(3)	
	FAIL TO REMAIN OPEN (PLUG)						+1E-4(3)				
MOV'S	FAIL TO OPEN		{+1E-3(3)}	+2E-3				{2.5E-6A }	+(1-50)E-4	+1E-3(3)	
	FAIL TO CLOSE			+8E-4					+(1-5)E-3	+1E-3(3)	
	SPURIOUS OPERATION								(3-100)E-7	3.5E-6(10)	
	ALL MODES				4.5E-5		+1E-3(3)	5E-6			
SOLENOID VALVES	FAIL TO OPEN				+5E-4					+1E-3(3)	
	FAIL TO CLOSE				+5E-4					+1E-3(3)	
	SPURIOUS OPERATION									3.5E-6(3)	
	FAIL TO OPERATE				9E-6		+1E-3(3)	3.5E-7	(2-6)E-6		
AIR-FLUID VALVES	FAIL TO OPEN	+1.5E-3							+(2-500)E-5	+1.2E-5(2)	
	FAIL TO CLOSE	+1.3E-2							+(2-50)E-5	+1.2E-5(2)	
	SPURIOUS OPERATION									5.5E-6(2)	
	ALL MODES				2E-5(3)		+3E-4(3)				
VACUUM VALVES	FAIL TO OPEN				2.2E-6		+3E-5(3)		+7E-3	3E-5(3)	
RELIEF VALVES	FAIL TO OPEN		+1E-4(10)H	+(4-7)E-3	1.4E-6		+1E-5(3)	5E-6	+5E-4	+1.3E-3(10)	8.4E-6
	FAIL TO CLOSE		+3E-2(3)H	+(3-6)E-3	1.2E-6					+1.0E-2(10)	
	10% LIGHT				8E-6						
	10% HEAVY				3E-6						
	PREMATURE OPERATION		1E-5(3)H	3E-6			1E-5(3)			3.5E-6(3)	
PILOT RELIEF VLVS	FAIL TO OPERATE				4.5E-6						
	FAIL TO RESEAT							+1E-2			
BELLOWS REL VLV	FAIL TO OPERATE				7E-6						
SAFETY VALVE	FAIL TO OPEN	2.1E-7								+1E-5(3)	
	FAIL TO CLOSE									+1E-4(3)	
	SPURIOUS OPERATION									3.5E-6(3)	
CHECK VALVES	REVERSE LEAKAGE		3E-6(3/10)	5E-7						2.9E-6(1,2)	
	FAIL TO OPEN			+5E-5	1.4E-5		+1E-4(3)		+5E-3	+1E-4(3)	6E-7
	FAIL TO CLOSE			+2E-4	8.4E-6						1E-6
	SPURIOUS OPERATION								1E-5		
	FAIL TO OPERATE		+1E-4(3)		3.2E-5			+1.2E-5			
PIPES >3"	RUPTURE				1.6E-10/S					1E-10(30)/S	
	ALL MODES		3E-10(100/30)/S		2.4E-9/S	1.5E-5	1E-10(30)/S				1E-10
PIPES <3"	RUPTURE				1.6E-10/S					1E-9(30)	
	ALL MODES		3E-10(100/30)/S		2.4E-9/S	7.7E-6	1E-9(30)/S		8E-7		1E-9
SCRAM RODS	FAIL TO SCRAM					1.9E-7	+1E-4(3)		+(1-25)E-6	+1E-4(3)	
ELECT. CLUTCH	FAIL TO OPERATE				1.8E-5		+3E-4(3)				
	PREMATURE DISENGAGEMENT						1E-6(10)				
MECH. CLUTCH	FAIL TO OPERATE				6E-6		+3E-4(3)				
	PREMATURE DISENGAGEMENT										
GASKETS	LEAKAGE				4.2E-6						
CONTROL ROD DRIVE FUNCTION						3.8E-6					

Sheet 1 of 2

COMPONENT	FAIL MODE	(1) BIBLIS	(2) GENERAL ATOMIC	(3) LER EVALUATION PROGRAM	(4) NCSR	(5) NPRDS	(6) WASH-1400	(7) WESTINGHOUSE	(8) VOLTA	(9) PICKARD, LOWE AND GARRICK	(10) BECHTEL
BATTERY	ALL MODES				7E-6	3.5E-7				1.6E-6(9.8)	
	NO OUTPUT									1.6E-8(9.8)	
BATTERY SYSTEM	FAILURE ON DEMAND								+2E-6		
	FAILURE						3E-6(3)				
	ALL MODES		6E-6(3/3)/P		7E-6						
BATTERY CHARGER	ALL MODES					2.2E-6				1.5E-6(29.9)B	
DIESEL GENERATOR	FAIL TO START	+4.2E-3	+3E-2(2/10)	+2.2E-2	+3E-2		+3E-2(3)	3E-5	+(5-50)E-3	+3E-2(3)	+9.2E-3D
	FAIL TO RUN		3E-4(3)				3E-3(10)	3.3E-4	7E-4	3E-3(10)	1.3E-5D
	OVERALL FAILURE				1.3E-3						
CIRCUIT BREAKERS	FAIL TO OPEN				5.8E-7				+(1-100)E-4	+2.3E-4(8.9)	
	FAIL TO CLOSE				1.2E-6				+5E-6	+1.0E-6(10)	
	SPURIOUS OPERATION		1E-6(3)		1.2E-7		1E-6(3)		5E-6	4.3E-8(10)	
	FAIL TO OPERATE		+1E-3(3)		2.3E-6	7.5E-7	+1E-3(3)	+3E-6		+4E-4(8.9)	
RELAYS	FAIL TO OPERATE				9.1E-7	3.3E-7		2.7E-6	(2-5)E-6	+3.5E-6(4)	
	FAIL TO ENERGIZE				3.4E-7		+1E-4(3)				
	SPURIOUS OPERATION								(3-10)E-7	5.7E-8(35)	
MAN. SWITCHES	FAIL TO OPEN						{+1E-5(3)}			+1.5E-8(71.1	
	FAIL TO CLOSE									+5.0E-9(67.1	
	SPURIOUS OPERATION									6.6E-8(1.4)	
	FAIL TO OPERATE				3E-7						
TORQUE SWITCHES	FAIL TO OPERATE						+1E-4(3)				
PRESSURE SWITCH	FAIL TO OPERATE				3.5E-5		+1E-4(3)			2E-7(3.3)	
	PREMATURE OPERATION									9.4E-8(36.5	
LIMIT SWITCHES	FAIL TO OPEN									+2.1E-6(1.9)	
	FAIL TO CLOSE									+6.2E-7(1.9)	
	SPURIOUS OPERATION									4.2E-6(1.9)	
	FAILURE TO OPERATE				2.5E-6		+3E-4(3)		+2E-5		
LIQ. LEV. SENSOR	FAIL TO OPERATE				3.5E-5			<4E-6	(5-10)E-6	4.4E-6(2.7)	
	PREMATURE OPERATION										
PRESS. SENSOR	FAIL TO OPERATE				3.4E-5			<6E-7	(5-28)E-6	1.7E-7(5.7)	
	OUT OF LIMITS		1E-5(10)								
TEMP. SENSOR	FAILURE				7.5E-5				(5-10)E-6	1.5E-6(5.8)	
	OUT OF LIMITS		3E-5(3)								

NOTES.

1. LETTER SUFFIXES ON FAILURE RATES DENOTE THE FOLLOWING:
   A - UPPER 95% CONFIDENCE BOUND
   B - RATE FOR STATIC BATTERY CHARGER
   P - PER PLANT HOUR
   S - PER SECTION OF PIPE
   D - FOR SIZE CLASS 1750-2000 KW DIESEL-GENERATORS
   H - FAILURE DATA FOR HELIUM

2. THE NUMBER OR NUMBERS IN PARENTHESES FOLLOWING FAILURE RATES DENOTE THE RANGE FACTORS. FOR EXAMPLE (XX/YY) MEANS ONE SHOULD MULTIPLY THE MEDIAN VALUE BY XX TO OBTAIN THE UPPER 95% CONFIDENCE BOUND AND DIVIDE THE MEDIAN BY YY TO OBTAIN THE LOWER 5% CONFIDENCE BOUND. A SINGLE NUMBER IN PARENTHESES INDICATES THE RANGE FACTOR IS FOR BOTH THE UPPER AND LOWER BOUND.

3. A "+" preceeding a failure rate denotes failure-per-dems

All other failure rates are failure-per-hour.

Sheet 2 of 2

DEFINITION OF TERMS

Biblis -	Biblis Nuclear Plant in Federal Republic of Germany
NCSR -	Provided by the National Center of Systems Reliability - United Kingdom
Volta -	Provided by Dr. Guiseppe Volta - Ispra
LER -	Provided by Licensee Event Report Data Evaluation
GA -	Provided by General Atomic Company
Pickard-	Provided by Pickard, Lowe, and Garrick
MOVs -	Motor Operated Valves
RVs -	Relief Valves
DGs -	Diesel Generators
CBs -	Circuit Breakers

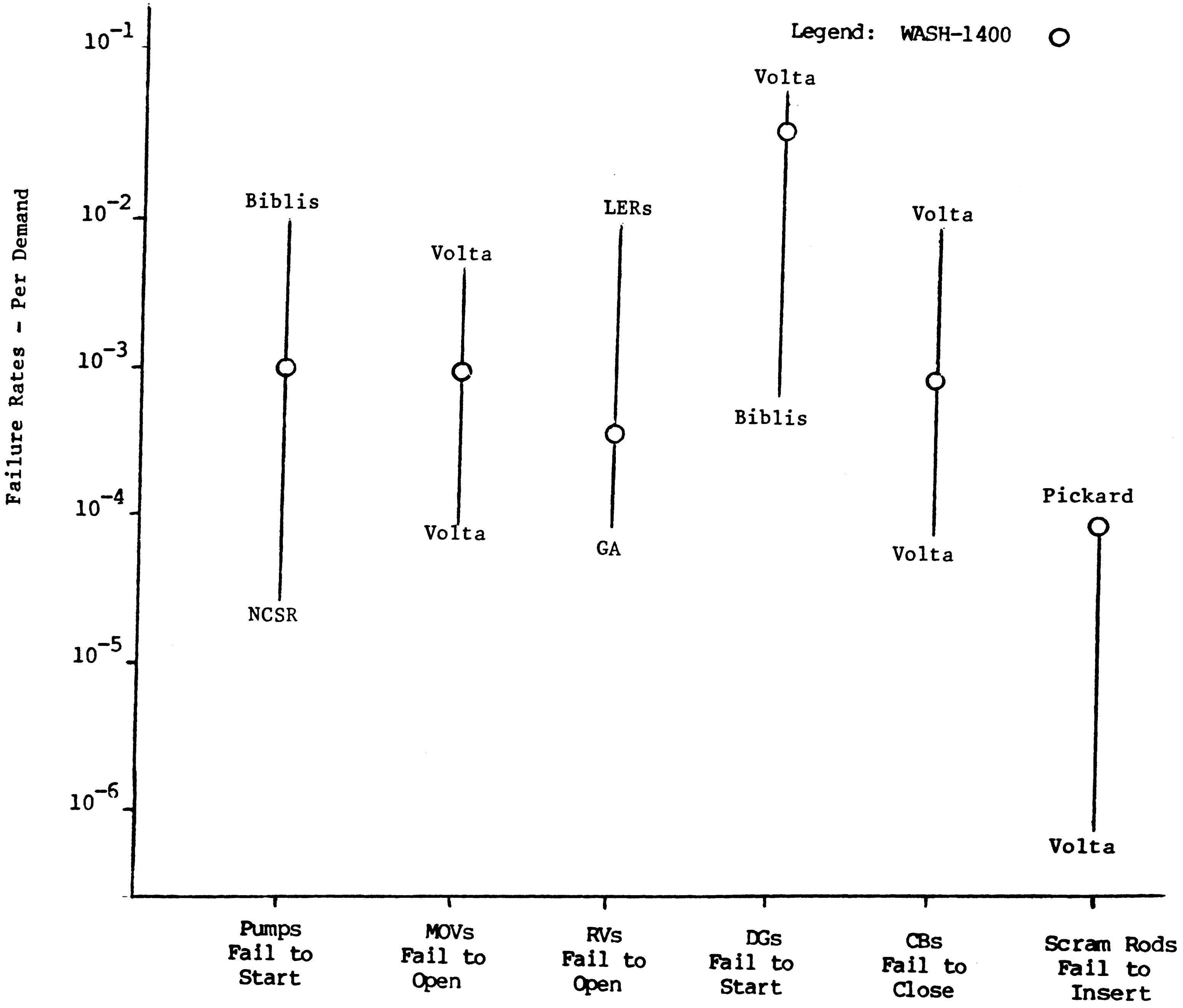

Figure 1. Data Point Estimate Extremes

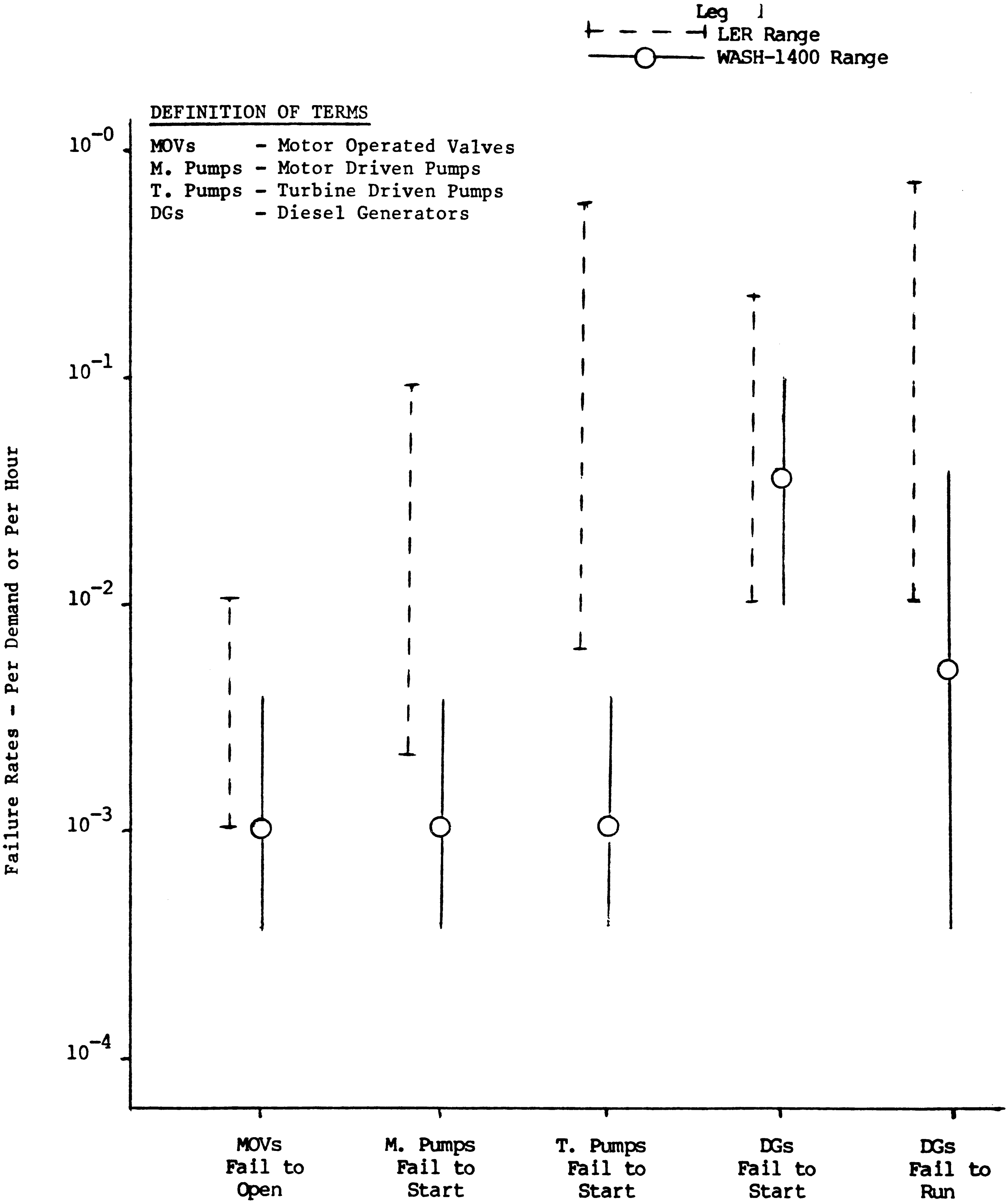

Figure 2. Plant to Plant Variation

ACRS Fellows Report, "Analysis of Feedwater Transient Sequences in B&W Nuclear Steam Supply Systems," February 7, 1980

Attachment A

UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, D. C. 20555

February 7, 1980

David Okrent, Chairman, Subcommittee on Reliability and Probabilistic Assessment

ANALYSIS OF FEEDWATER TRANSIENT SEQUENCES IN B&W NUCLEAR STEAM SUPPLY SYSTEMS

To aid in the Subcommittee's work in formulating a response to Congressman Udall's letter of July 29, 1979, please find attached a draft of our analysis of the Three Mile Island, Rancho Seco, and Davis Besse events. Using the WASH-1400 event trees and data directly gives meaningless results because several important features of the sequences are omitted. Using an event tree which we constructed for B&W feedwater transients, and using WASH-1400 methodology and data, we obtain the following:

Rancho Seco	1.2×10^{-4}/B&W reactor year
Davis Besse	1.2×10^{-3}/B&W reactor year
Three Mile Island	1.5×10^{-4}/B&W reactor year

A major uncertainty is the characterization of operator behavior. It appears that with appropriate use of WASH-1400 methodology and data, events of this type would be anticipated.

The study will be distributed to all Subcommittee Members and appropriate consultants.

If you have any questions, please do not hesitate to call us.

Edward S. Abbott
Edward Abbott, ACRS Senior Fellow

John H. Bickel
John Bickel, ACRS Fellow

William Kastenberg
William Kastenberg, ACRS Senior Fellow

ANALYSIS OF FEEDWATER TRANSIENT SEQUENCES IN B&W NUCLEAR STEAM SUPPLY SYSTEMS

E. Abbott, J. Bickel & W. E. Kastenberg
ACRS Fellows

I. INTRODUCTION

This study uses event tree analysis, and existing WASH-1400 methodology and data to determine various sequence probabilities for three different events which have occurred in plants with a B&W Nuclear Steam Supply System. The events evaluated are the March 29, 1979 Accident at Three Mile Island (TMI), the March 30, 1978 Loss of Instrument Power Transient at Rancho Seco (RS) and the September 24, 1977 Depressurization Transient at Davis Besse (DB). The sequence of events at RS and DB are given in Appendix A. The events are generically classified as loss of main feedwater. The TMI and DB events are similar in that the sequence of events (i.e., the separate plant and operator actions) are comparable up to the point of the operator manually blocking the power operated relief valve (PORV). The RS event is similar only in that the initiating event resulted in a loss of main feedwater. The plant and operator actions, however, are different from TMI and DB.

In the first part of this memo, a heuristic analysis of feedwater transients in B&W plants prior to TMI is given. This is followed by an analysis using the data, event trees and sequences contained in WASH-1400 for the S2 small break LOCA (break diameter $\leq 2"$) and for the T-transient.* It must be recognized, however, that WASH-1400 utilzes event sequences characteristic of the Westinghouse Nuclear Steam Supply System and its associated protective and engineered safeguard systems. In the last part of the study, we develop a feedwater transient

* A glossary of abbreviations is given in Table I (page 3).

event tree sequence unique to B&W plants valid prior to April 1979. This tree is applicable to B&W plants where the PORV is designed to lift prior to RPS trip during a feedwater transient.

TABLE I

GLOSSARY OF TERMS

AFWS - Auxiliary Feedwater System

CHRS - Containment Heat Removal System

CSIS - Containment Spray Injection System

CSRS - Containment Spray Recirculation System

CVCS - Chemical Volume Control System

ECI - Emergency Coolant Injection

ECR - Emergency Coolant Recirculation

EP - Electric Power

DB - Davis Besse

ICS - Integrated Control System

HPIS - High Pressue Injection System

LOCA - Loss of Coolant Accident

NNI-Y - non-nuclear instrumentation power bus Y. (power supply for instruments not associated with the determining of the fission rate in the core)

PCS - Power Conversion System

PORV - Power (or pilot) operated relief valve

Psi - Pounds per square inch

P_X - probability of failure for system X. (e.g., P_k = probability the RPS system fails to insert the reactor's control rods)

PWR - Pressurized Water Reactors

RCS - Reactor Coolant System

RHRS - Residual Heat Removal System

RPS - Reactor Protective System

RS - Rancho Seco

S2 - small break LOCA event tree of WASH-1400 for a PWR

SFRCS - Steam Feedwater Rupture Control System

SHA - Sodium Hydroxide Addition

SR - Safety Relief

SSR - Secondary Steam Relief

T - Transient Event Tree of WASH-1400 for a PWR

TE - Transient Event

TMI - Three Mile Island

VO - Valve Opens

VR - Valve Recloses

WASH-1400 - The Reactor Safety Study NUREG-75/014.

II. HEURISTIC ANALYSIS OF B&W FEEDWATER TRANSIENTS

As stated above, the sequence of events at Davis Besse (DB) and Rancho Seco (RS) are given in Appendix A. The Three Mile Island (TMI) accident is similar to the DB transient up to the last event where the stuck open PORV is isolated at DB but not at TMI. As discussed later in this development, the time frames are however, somewhat different.

Examination of the sequences given in Appendix A yields the following heuristic analysis:

1. The events for TMI and DB are determined by: a) the frequency of feedwater transients in PWRs ∼ 3 per reactor year, b) the fact that in B&W plants prior to April 1979, a feedwater transient causes the PORV to open independent of AFWS operation, and c) failure of the PORV to close (3 x 10^{-2} per demand). Hence this family of transients would be initiated on the order of 9 x 10^{-2} per reactor year.

2. The eventual outcome of this sequence depends upon a) whether or not the PORV is gagged at the time of transient initiation (50% of the time it is), b) operator action in not interrupting the HPIS, and c) isolating the PORV if it fails to close.

3. For DB the PORV was not gagged, the operator interrupted the HPIS and did isolate the PORV. In order to estimate the frequency of the outcome, the probability of these three events must be obtained. A telephone survey of B&W plants by the authors revealed that the PORV is gagged 50% of the

time. The operator action is more difficult to obtain. WASH-1400 (Appendix III) states that the probability of operator failure under stress is:

0.9 - 5 minutes after a large LOCA

0.1 - 30 minutes after a large LOCA

0.01 - several hours later

The average error rate, in a high stress situation is given as 0.2 to 0.3.

In addition, if P is the probability of operator error, and the number of people present is n, then P^n is given as the probability of a collective error. In practice, the final decision rests with the shift supervisor so that n can vary between 1 and 3 depending on his influence. (See Appendix B)

One problem (among others) in using this data is that it is not clear that the operator made an error in defeating the HPIS. That is, the procedure followed called for interruption of HPIS with high level indicated in the pressurizer. In that case, it may have been the procedure that was in error, and the operators failed to recognize it.

Using a probability of 0.5 for the chance of a gagged PORV, $(0.3)^3 = 0.027$ for defeating the HPIS after several minutes, and using $1-(0.1)^3 = .999$ for successfully blocking the PORV at 20 minutes yields a frequency for DB

$$DB = (9\text{x}10^{-2})(0.5)(0.027)(0.999) = 1.2\text{x}10^{-3}$$

4. At TMI, the PORV was not gagged, the operator interrupted the HPIS and the PORV was not isolated. Since the decay heat load was greater at TMI than DB, the failure to block the PORV occurred sooner. The operator

should have recognized that the PORV had stuck open by the time the quench tank rupture disk blew (about 15 minutes into the transient). This yields an estimate of the error probability of $(.5)^3$. Hence at TMI

$$TMI = (9x10^{-2})\ (0.5)(0.027)(.125) = 1.5x10^{-4}$$

5. For Rancho Seco (RS), the initiating event (loss of non-nuclear instrumentation) was estimated to be $8.6x10^{-3}$ per reactor year*. Since this loss initiated the feedwater transient, this value is used, rather than the 3 per reactor year used for DB and TMI.

   Since the PORV was gagged (0.5), the operators throttled the HPIS (0.027) and the code safety valves opened and closed as required (1.0), the frequency of this event is estimated as

   $$RS = (8.6x10^{-3})(0.5)(0.027) = 1.2x10^{-4}$$

   In the next section, an attempt is made to map these events on the WASH-1400 event trees.

*/ Because of the difficulty in estimating the specific failure of the non-nuclear instrumentation (NNI-Y) power supply in the absence of a detailed fault tree analysis, the failure rate for low power, solid state devices was used. It should be noted that the final result is very sensitive to this failure rate and should be viewed as representing the family of NNI failures.

III. WASH-1400 EVENT TREES

In this section, we have attempted to trace the Davis-Besse (DB), Rancho-Seco (RS) and Three Mile Island (TMI) events on the WASH-1400 Transient (T) and Small Break LOCA (S2) event trees shown in Figures 1 and 2. Mapping the sequences occurring at DB and RS on the WASH-1400 T tree without any modification yields sequence TM, which does not result in core melt, and was subsequently omitted from the dominant risk sequences in WASH-1400. Mapping TMI on the T tree yields: (a) sequence TMLQU if no credit is given for the return of the Auxiliary Feedwater System (AFWS) or TMU if credit is given for AFWS. Both paths do not give credit for actuation of the High Pressure Injection System (HPIS). With HPIS actuation, the corresponding paths are TM and TMLQ (See Figure 1). Several problems arise when trying to evaluate these events in terms of this event tree. For the DB and RS events, sequence TM does not differentiate between the failure of the PORV to close at DB and the initially gagged PORV at RS. Second, the sequence is for <u>all</u> transient initiated events and hence does not identify the initial loss of non-nuclear instrumentation (power bus NNI-Y) induced by human action which resulted in the feedwater transient and in the loss of indicators during the transient at RS. Lastly, for DB and TMI, the tree fails to include the fact that the PORV will lift regardless of the availability of the auxillary feedwater supply in B&W plants, and, therefore, neglects the possibility that the PORV fails to close.

For the DB and RS events, the frequency of sequence TM for <u>all</u> feedwater transients would be given by:

$$P_{TM} = P_T \ (1-P_K) \ P_M \ (1-P_Q) \ (1-P_U) \ (1-P_W).$$

Based on WASH 1400 data, P_T = 3 feedwater transients per reactor year, P_M = 1 (failure to recover the main feedwater system within minutes) and assuming $(1-P_i)$ = 1 we obtain

P_{TM} = 3 per reactor year.

For TMI, the appropriate sequence (taking into account the return of the AFWS) is TMU with

$$P_{TMU} = P_T \ (1-P_K) \ P_M \ (1-P_Q) \ P_U$$

Hence P_{TMU} = 3 x P_U per reactor year where P_U is the unavailability of the HPIS. Since HPIS was available, but the operators interrupted its operation, P_U is chosen as $(0.3)^3$ which is in the range of WASH-1400 numbers for operator error. Hence for this sequence

$P_{TMU} = 8.1 \times 10^{-2}$ per reactor year.

Again, this tree neglects failure of the PORV to close.

In WASH-1400, it is suggested that transients, for which the PORV fails to close, should be treated as a small break LOCA, and the event tree S2 be used (Figure 2). Since the LOCA is terminated at both DB and RS, (the PORV is finally blocked at DB and the code safety valve reseats at RS), these events become sequence S_2 with a frequency of 3 per year.

Mapping the TMI event on the small break LOCA tree yields sequence S_2D. The initiating frequency S2 is given by

S2 = 3 feedwater transients/year x 10^{-2} failure to close/demand *

= 3 x 10^{-2} S2 events/yr.

Using a HPIS unavailability of $(0.3)^3$ due to operator error, TMI becomes

$P_{TMI} = 8.1 \times 10^{-4}$/year

Failure to block the PORV is not included in the tree and the PORV failure to close on demand number comes from Appendix V, page V-38 of WASH-1400.

* WASH-1400 states this number has an error factor of 10.

For the particular feedwater transient at Rancho Seco, the probability of loss of non-nuclear instrumentation (which led to loss of feedwater) and the probability that the loss was attributable to human error should be obtained.

Data from WASH-1400 on loss of non-nuclear instrumentation is about 8.6 x 10^{-3}/reactor year. Hence the Rancho Seco initiating event may be on the order of 8.6 x 10^{-3}/reactor year.

IV. APPLICATION OF A B&W EVENT TREE TO TMI, DB AND RS

A unique event tree was developed for feedwater transients in B&W plants which is different from those used in WASH-1400. The differences between the WASH-1400 - PWR and the B&W PWR were described in Section III.

The sequence of events at TMI is well known and not presented here. The events follow along sequence #5 on the attached event tree and are self-explanatory (Figure 3). The sequence of events for Davis Besse follows sequence #6 on the event tree. The sequence of events for Rancho Seco follows sequence #14 on the event tree.

The probabilities and failure rate data shown below were obtained from WASH-1400 except for those marked with * and **. The uncertainty in P_Q, and P_Q were also obtained from B&W data. The uncertainty in the other probabilities are difficult to obtain because they depend on human errors, operating procedures, etc., and have not been ascertained. Hence, the final results could have large error bounds.

The probabilities for the significant events in the event tree are:

P_T - 3 per reactor year (WASH-1400, Appendix V, pg. V-34)

* $P_P = .5$

** $P_{Q'} = 3 \times 10_{-2}$ ($\pm 1 \times 10^{-2}$)

$P_Q = 3 \times 10^{-2}$ ($\pm 1 \times 10^{-2}$)

$P_{U'} = (.3)^3$ (WASH-1400, Appendix III, page III-60)

$P_{Q''} = (.5)^3$ " " " " " " (for TMI)

$P_{Q''} = (.1)^3$ " " " " " " (for DB)

For TMI the probability is as follows:

$$P_{TMI} = P_T \times P_U \times (P_Q) \times (P_{U'}) \times (P_{Q''})$$
$$= 3 \times .5 \times 3 \times 10^{-2} \times (.3)^3 (.5)^3$$
$$= 1.5 \times 10^{-4}/\text{year}$$

For DB the probability is as follows:

$$P_{DB} = P_T \times P_P \times P_Q \times (P_{U'}) \times (1 - P_{Q''})$$
$$= 3 \times .5 \times (3 \times 10^{-2}) \times (0.3) \times (1-(.1)^3)$$
$$= 1.2 \times 10^{-3}/\text{year}$$

For the Rancho Seco event, the probability of the loss of an instrument bus leading to a feedwater transient must be used for P_T. Using WASH-1400 data, the failure rate of low power solid state devices is:

1×10^{-6}/hr or 8.6×10^{-3} per year.

* The P_P value was obtained from a telephone survey of B&W plants and their estimate of the frequency of defeating the PORV by blocking or gagging.

** Obtained from B&W

The probability of the RS family of events is then estimated as

$$\begin{aligned} P_{RS} &= P_{NNI} \times P_P \times P_U, \\ &= 8.6 \times 10^{-3} \times .5 \times (.3)^3 \\ &= 1.2 \times 10^{-4} \text{ per reactor year.} \end{aligned}$$

These results are summarized as follows:.

TABLE II.

	WASH-1400		B&W
	T	S_2	Feedwater Transient
TMI	8.1×10^{-2}	8.1×10^{-4}	1.5×10^{-4}
DB	3	*	1.2×10^{-3}
RS	8.6×10^{-3}	*	1.2×10^{-4}

It is important to recognize that the largest uncertainty is in characterization of operator action. WASH-1400 states that if P is the probability of operator error, then P^n is the probability of error if the number of personnel in the control room is n. Because of the supervisory nature of the shift supervisor, the probability may be between P and P^n. This report uses .3 for HPIS unavailability as an average for the initial one-half hour for all three sequences. Failure to block the PORV is given a probability at .5 at fifteen minutes and .1 at thirty minutes. This report does not evaluate in detail the resultant error in the calculations because of a lack of data on operator action. The values chosen are considered to be within the ranges of WASH-1400, and consistent with the methodology.

*Does not apply.

V. CONCLUSIONS

After mapping the TMI, DB and RS events on the WASH-1400 Transient and Small Break LOCA trees, constructing an event tree for B&W Feedwater Transients, and employing the WASH-1400 data, the following is concluded:

1. As shown in Table II, the values obtained from a B&W transient tree differ from those obtained from the T and S_2 event trees in WASH-1400 because the latter trees do not include the necessary features as discussed above.

   As noted in Section II, the WASH-1400 event trees cannot be used since the PORV lifts during a feedwater transient. This clearly shows that the strict use of these event trees to other PWRs yield erroneous results. This should be obvious because the trees in WASH-1400 are unique to the Surry Plant which is a Westinghouse PWR.

   The values obtained above could have been obtained prior to the event sequences discussed because the data, knowledge of the transients and methodology were known. The only requirement to complete a similar study would have been development of a unique event tree for B&W plants.

2. The consequences of these sequences of events depend upon the exposure history of the core. At DB, the plant was operating at low power with fresh fuel. At TMI, the plant was operating at full power well into the fuel cycle. The time allowed to block the PORV and for re-initiating HPSI before the core is uncovered was different in each case. These time differences are reflected in the characterization of operator action.

3. The NRC will construct event and fault trees for individual plants under the Integrated Reliability Evaluation Program (IREP). The individual licensees, however, could easily perform similar studies using available failure rate data and developing a unique event tree for their respective plants. This would immediately focus upon needed areas of improvement in operations and provide an independent check to IREP.

APPENDIX A

Sequence of Events

The sequence of events for Davis Besse is:

T - A spurious initiation of Steam Feedwater Rupture Control System (SFRCS) isolates the steam generators and starts the auxiliary feedwater pumps.

P - The pressure rise in the primary system causes the Power Operated Relief Valve (PORV) to open.

K - The control room operator manually trips the reactor because the pressurizer level is outside (high) of the operating range.

L - Both auxiliary feedwater pumps start but only one feeds a generator due to binding in the throttle linkage in the other pump's turbine control system.

P;Q- Code safety valves do not lift as the PORV is relieving reactor coolant pressure.

Q - The PORV "simmers" due to a missing relay in the closing circuit and after nine cycles it sticks open.

U - Safety Features Actuation System (SFAS) initiation on low RCS pressure starts the HPI pumps.

U'- The operator cycles the HPI pumps to maintain pressurizer level.

Q"- The operators recognize that the PORV is stuck open and shut the block valve.

The sequence of events for Rancho Seco is:

T - The loss of one of the two non-nuclear instrumentation fuses (NNI-Y) causes the Integrated Control System (ICS) to sense a loss of BTU output and isolates the feedwater system.

P - The primary system pressure rise would have caused the PORV to open but it was gagged shut.

K - The reactor trips on high RCS pressure.

L - The operator manually initiates main feedwater after realizing the NNI-Y failure has blocked the initiation of the auxiliary feedwater system (the auxiliary feedwater pumps initiates automatically on SFAS actuation later on in the transient.)

P - The increased RCS pressure causes one of the two code safety valves to open at a pressure less than maximum setpoint of 2500 psi. The subsequent decrease in RCS pressure causes a SFAS initiation (HPI and AFWS start).

Q'- The power safety valves reseat.

U'- NNI-Y is restored. The operators recognize an excessive cooldown ($> 100^{o}$ F/hr) has resulted. They throttle HPI and auxiliary feed flow to reduce rate of cooldown.

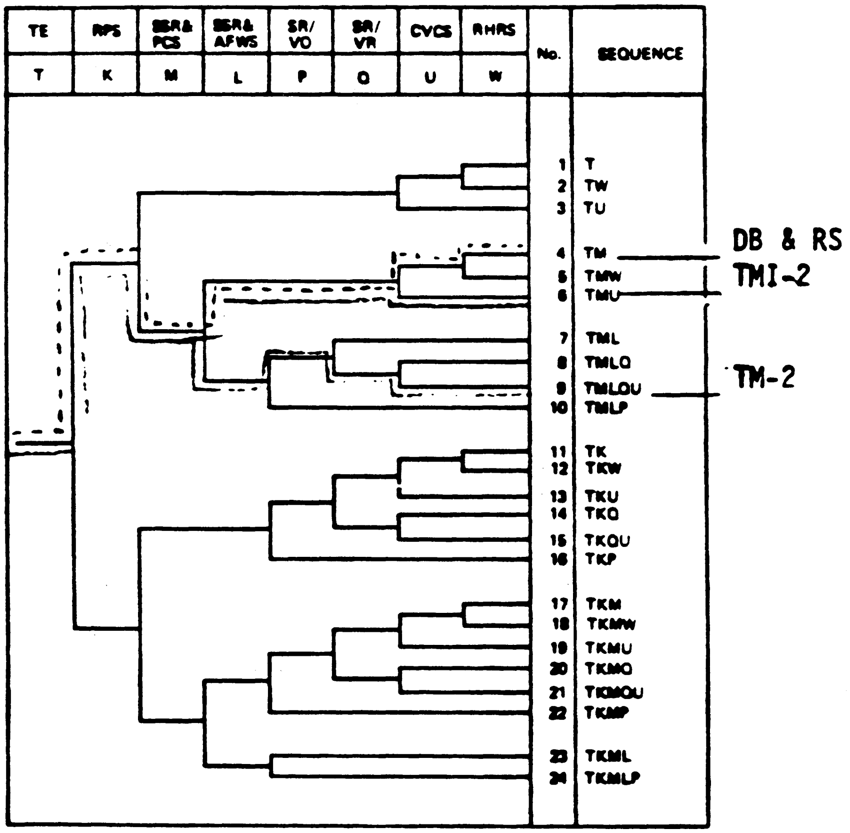

FIGURE I 4-14 PWR Transient Event Tree

FIGURE 1

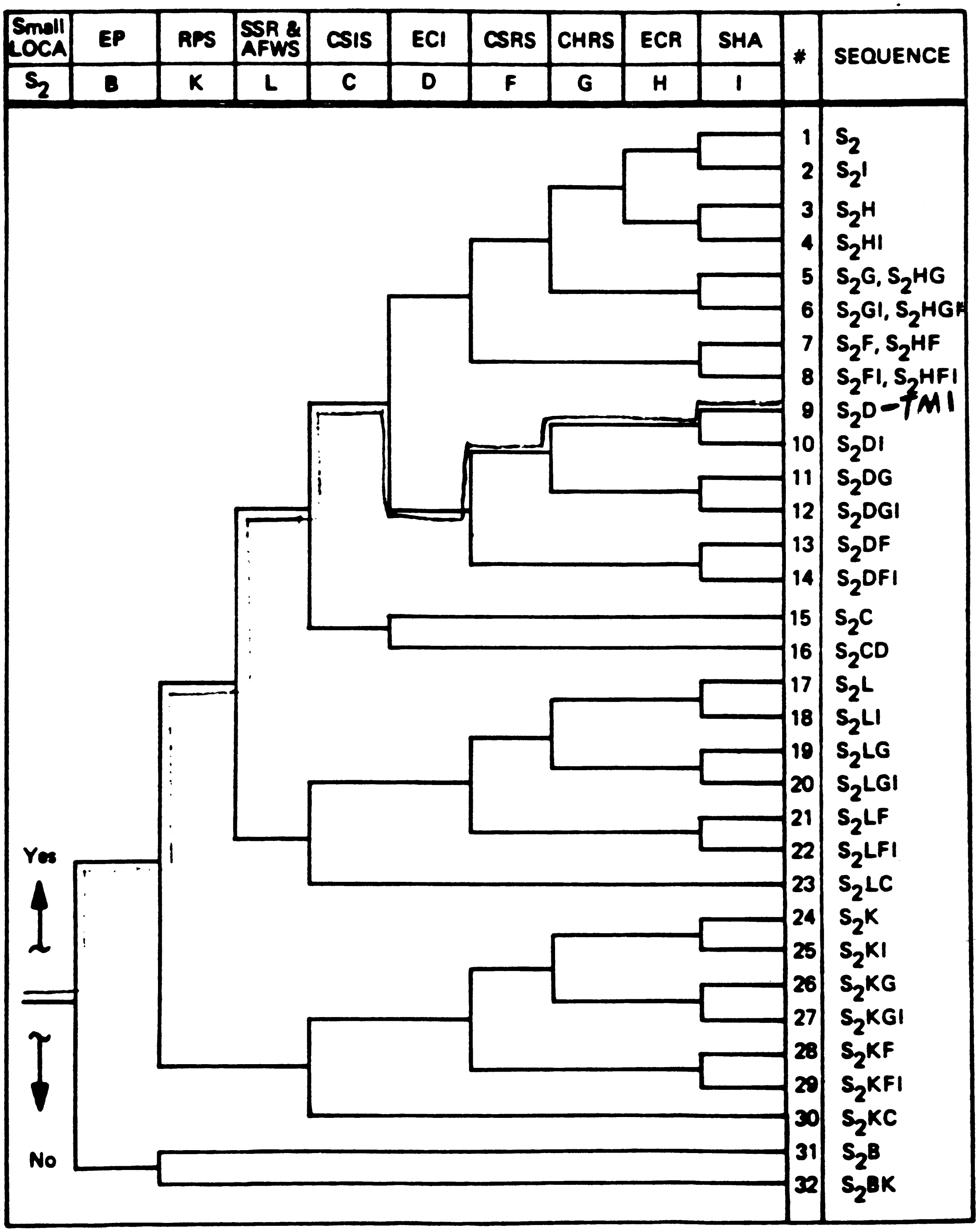

FIGURE I 4-4 PWR Small LOCA (S2, 1/2-2 inch diameter) in RCS

FIGURE 2

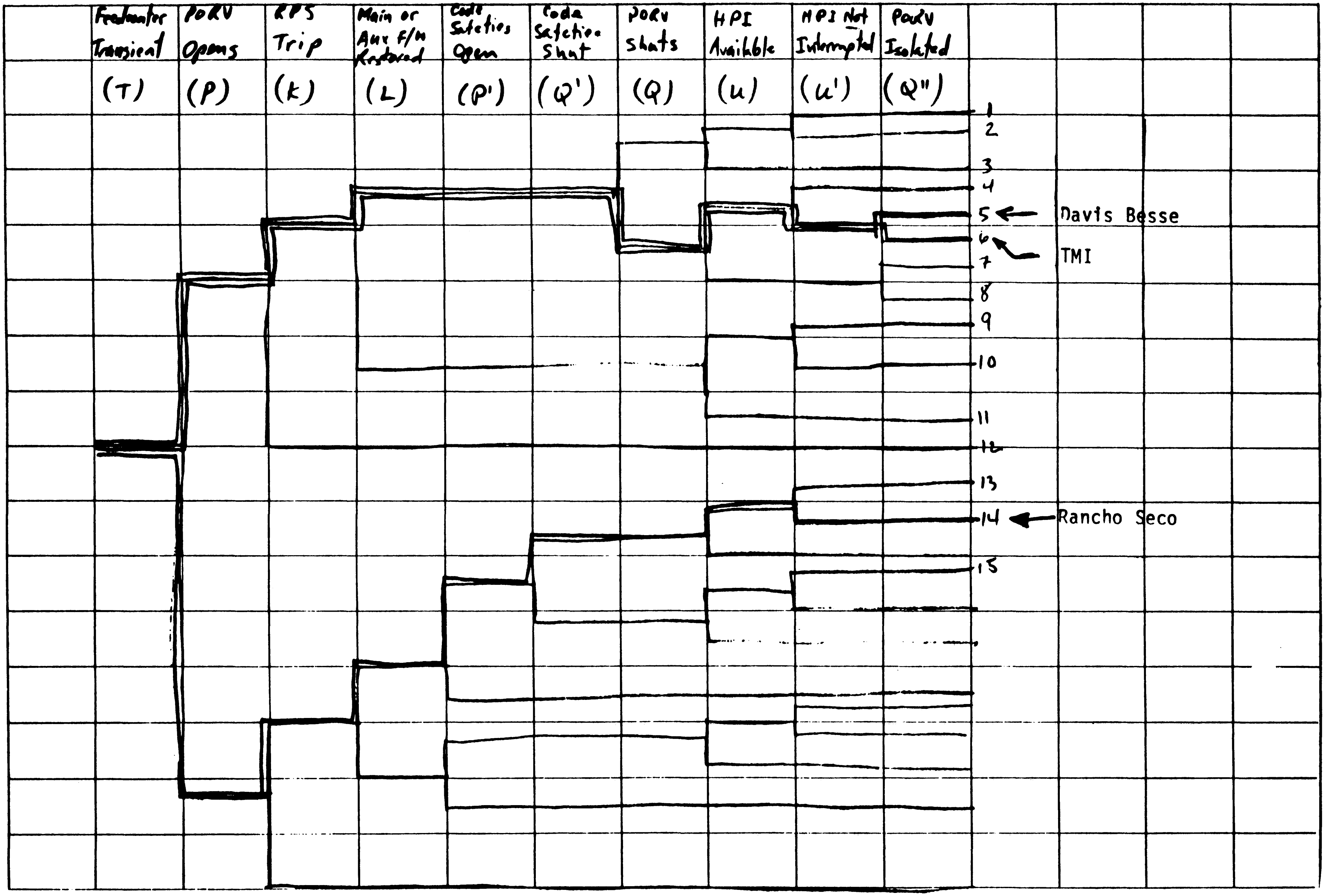

FIGURE 3. B&W FEEDWATER TRANSIENT EVENT TREE.

APPENDIX B
OPERATOR ERROR

The rationale for characterization of operator error in WASH-1400 can be demonstrated as follows. Let p_f be the probability of operator failure and let p_s be the probability of operator success. Then

$$p_s + p_f = 1 \qquad (1)$$

as it should. Suppose there are n operators in the control room. Let P_f be the probability the n operators make a "collective" error. In WASH-1400, P_f is given by

$$P_f = (p_f)^n \qquad (2)$$

Since probability must be conserved, the probability that the n operators make a "collective" success, denoted P_s is

$$P_s = P_f = 1-(p_f)^n \qquad (3)$$

To understand the implications of such an approach consider the following:

let $p_f = 0.1$ (individual failure), n=3.

It follows that:

$p_s = 1-0.1 \quad = 0.900$ (individual success)

$P_f = (0.1)^3 \quad = 0.001$ (collective failure)

$P_s = 1-(0.1)^3 \quad = 0.999$ (collective success)

The possible operator actions are:

$$p_f\ p_f\ p_f = (0.1)^3 = .001$$

$$p_f\ p_f\ p_s = (0.1)^2\ (0.9) = .009$$

$$p_f\ p_s\ p_f = (0.1)(0.9)(0.1) = .009$$

$$p_f\ p_s\ p_s = (0.1)(0.9)^2 = .081$$

$$p_s\ p_f\ p_f = (0.8)(0.1)^2 = .009$$

$$p_s\ p_s\ p_f = (0.9)^2\ (0.1) = .081$$

$$p_s\ p_f\ p_s = (0.9)(0.1)(0.9) = .081$$

$$p_s\ p_s\ p_s = (0.9)^3 = .729$$

$$\overline{}\quad 1.000$$

Hence, WASH-1400 can be interpreted as follows:

a) For a "collective" failure, all n operators must be in error.

b) For a "collective" success, at least <u>one</u> operator must take correct action.

With this interpretation, $P_s \neq p_s^n$ i.e. all operators are correct.

As stated in the report, the shift supervisor should have the final word ... however, to be consistent with the WASH-1400 approach

$$P_f = p_f^n \text{ and } P_s = 1-(p_f)^n$$

is used, with the interpretation given above.

Nuclear Regulatory Commission Staff
Report, "Evaluation of Davis-Besse and
Rancho Seco Feedwater Transients on
9/24/77 and 3/20/78 Using WASH-1400 Data"

Attachment B

A. INTRODUCTION

In this report we have evaluated the Loss of Main Feedwater transients which occurred at Davis-Besse-1 on 9/24/77 and at Rancho Seco on 3/20/78 and compared them with the accident at Three Mile Island-2 on 3/29/79. A summary is provided of the Davis-Besse and Rancho Seco events. The behavior of important safety systems is compared. An event tree for Loss of Main Feedwater transients is provided, and each transient sequence is identified in the context of the event tree, WASH-1400 data.

Certain caveats should be made. First, WASH-1400 was performed for the Westinghouse-designed Surry plant, not a B&W reactor. We have not done the kind of major in-depth analysis here that was done for WASH-1400. Such an analysis would require considerable effort and funds. Second, it should be recognized that there are significant uncertainties in the WASH-1400 data. Third, the evaluation refers to pre-TMI system behavior and transients.

B. DISCUSSION OF DAVIS-BESSE TRANSIENT

1. Event Summary - Davis-Besse

On September 24, 1977 a series of events occurred at the Davis-Besse Unit 1 which resulted in depressurization of the primary system from a normal operating pressure of 2150 psi to 900 psi in approximately eight minutes, and the release of approximately 11,000 gallons of water in the form of steam within the containment through the pressurizer quench tank rupture disc.

On the afternoon of Saturday, September 24, 1977 the main turbine was shut down to repair a leak in a pressure sensing connection on a steam line from the turbine governing valves to the turbine inlet. The reactor was being neld critical at approximately 9% thermal power.

At 2134 hours, a spurious half trip occurred in the Steam Feedwater Rupture Control System (SFRCS). This caused the startup feedwater valve on the No. 2 steam generator (which is the normal feed path at this power level) to close. Closure of this valve resulted in a low No. 2 steam generator level, which then resulted in a normal full trip of the SFRCS for this condition and initiation of the SFRCS. SFRCS initiation closes both main steam isolation valves and initiates feedwater flow to both steam generators from their individual steam-driven auxiliary feedpumps.

The half trip and resulting full trip of the SFRCS caused a reduction in heat removal from the primary system and a corresponding temperature/ pressure rise in the primary system. The pressure rise in the primary system caused the pressurizer power relief valve to lift. This valve then rapidly oscillated closed-to-open approximately nine times and remained in the full open position. The chattering of the relief valve was caused by the physical absence of a relay in the valve control logic circuitry. The relay normally provides for a deadband between "open" and "close" setpoints. An empty relay socket was found in the logic cabinet after the event.

The temperature rise in the primary system caused an increase in the pressurizer level, and the operator manually tripped the reactor on high pressurizer level approximately two minutes after the half trip on the SFRCS occurred.

The pressurizer power relief valve, in the full open position, rapidly reduced the primary system pressure, and a Safety Features Actuation

System (SFAS) trip occurred at the 1600 psi setpoint of the primary system. The power relief valve discharge goes to the pressurizer quench tank, which became overloaded and overpressurized, and approximately 4 1/2 minutes after reactor trip the rupture disc in this tank relieved due to overpressure, venting the steam into the containment. Approximately 20 minutes after reactor trip, the operators diagnosed the reason for the primary system depressurization as being the power relief valve, and from the control room closed the motorized block valve ahead of the power relief valve, terminating the loss of primary coolant into the containment.

Subsequent operator action using makeup pumps and high pressure injection pumps stabilized the primary system pressure and pressurizer level and a controlled shutdown to cold shutdown conditions followed.

The major physical damage from the incident was to the reflective metal insulation on the lower part of the No. 2 steam generator, which received the jet of steam coming from the pressurizer quench tank. A ventilating duct in the area of the quench tank was dimpled and required straightening. Twenty-three panels of reflective metal insulation required replacement. Entry into the containment was made at 0550 Sunday, September 25, 1977 for cleanup operations.

Another event occurred in the course of this incident that did not contribute materially to the above events, but did result in the No. 2 steam generator going dry. This was the failure of the No. 2 auxiliary feedpump to come up to full speed (3600 rpm) following the SFRCS trip. This feedpump came up to approximately 2600 rpm and stayed at this level with no flow to the steam generator until approximately 12 minutes after reactor trip, when the operators placed its control in manual and brought it up to full speed (commencing feedwater flow to the steam generator).

2. Key Systems Behavior - Davis-Besse

An important fact to bear in mind while discussing the Davis-Besse transient of 9/24/77 is that only one full-power day of operation had been accumulated at the time of the event (see Table 1). This means that considerably less decay heat was being generated in the core than was the case at TMI-2. In addition, the Davis-Besse reactor was only at 9% power when the main feedwater was lost. A high pressure reactor trip did not occur (it did at TMI in 9 seconds), confirming the slower, milder nature of the Davis-Besse transient.

Operator reaction to the transient was effective. Although the pressurizer level increased off-scale in the first ten minutes, the operators apparently realized the pressurizer level increase was misleading and caused by steam formation in the primary system. However, the operators did turn off the HPI pumps (just as at TMI) after only three minutes of operation.

The pressurizer relief valve stuck open early in the transient. The operators diagnosed this problem and closed the block valve after 21 minutes into the transient. At TMI a similar problem took 138 minutes to diagnose. The ability to diagnose and take remedial action in 21 minutes helped to terminate the Davis-Besse transient with a minimum of damage.

3. Event Tree Evaluation - Davis-Besse

The events at Davis-Besse on 9/24/77 can be depicted in an event tree (Figure 1). The Davis-Besse transient is #2 on the event tree. This may be compared with sequence #3 which is the TMI-2 sequence. The event tree is for a category of transients which begin with a loss of all main feedwater (TM). In the case of Davis-Besse, this was apparently initiated by a faulty input buffer in the logic control of the Steam Feedwater Rupture Control System.

WASH-1400 estimated three of these feedwater transients to occur per year at each reactor. In the 12 months prior to the TMI-2 accident, the average number of feedwater transients at B&W reactors was three per year (see Table 2), confirming the WASH-1400 value. It should be noted that a larger number of feedwater transients occur in the first few years of operation, and a smaller number after that. Perhaps 2 to 3 times this number might be appropriate for early operation. Plants which have operated longer than a few years may average 1 to 2 feedwater transients per year.

Within about ten seconds after the main feedwater system had tripped, increasing reactor pressure caused the pressurizer relief valve to open. This valve then failed to close, causing a small LOCA. The WASH-1400 failure rate estimated for this failure mode was 1×10^{-2} per demand with a factor 10 uncertainty up and down. More recent data in light of the TMI-2 accident indicate three relief vale failures in this mode in about 150 demands, or a failure rate (to reclose) of $\sim2\times10^{-2}$ per demand, again confirming the WASH-1400 failure rate.

At the same time that the relief valve was opening in the primary system, the auxiliary feedwater system was being aligned to the steam generators and auxiliary feedwater flow had commenced successfully shortly thereafter. About 30 seconds later, the operator tripped the reactor manually because of rising pressurizer level.

Reactor pressure did not reach the setpoint of the pressurizer safety valves and they were not called on to open. The ECCS system automatically actuated on low pressure (1600 psi) in the High Pressure Injection (HPI) mode about 1 1/2 minutes after the pressurizer relief valve stuck open. After the HPI system operated successfully for about three minutes, the operator manually terminated HPI. Because of the nature of the transient, this was regarded as successful operation of ECCS. The probability of this category of transient occurring in a B&W reactor, as predicted using WASH-1400 failure data, is estimated as follows:

$$\underset{\substack{\text{Loss of Main}\\ \text{Feedwater/yr.}}}{3} \quad \times \quad \underset{\substack{\text{Relief Valve}\\ \text{Fails to Close}}}{1\text{x}10^{-2}} \quad = \quad 3\text{x}10^{-2} \text{ per reactor year}$$

C. DISCUSSION OF RANCHO SECO TRANSIENT

1. Event Summary - Rancho Seco

On March 20, 1978 an excessive cooldown transient was experienced while operating at 70% power (IE Report 50-132). Non-nuclear instruments were lost including steam generator and pressurizer levels and all RCS temperatures. Loss of RCS hot leg temperature input to the ICS caused termination of feedwater flow. Reduced heat removal in the steam generators caused RCS temperature and pressure to increase. The reactor tripped on high RCS pressure followed by a turbine trip. The secondary sides of both steam generators emptied due to operation of condenser bypass valves, atmospheric dump valves and auxiliary steam loads. Although normal control room indications were lost, the computer typewriter will print alarms when setpoints are reached. In addition, selected plant parameters can be monitored on the ICS computer printout. With the aid of computer indication, pressurizer level was maintained by manual operation of a high-pressure injection pump. "A" steam generator level control initiated emergency feedwater injection (level control was actually lost at time zero, but the channel drifted slowly downward while "B" channel drifted slowly upward). The turbine-driven auxiliary feedwater pump had started on loss of feedwater flow.

RCS cooldown started as a result of emergency feedwater flow to "A" steam generator and possibly main feedwater pump flow (manually operated). Decreasing RCS pressure (1600 psig) actuated HPI pumps and the motor-driven auxiliary feedwater pump. Full auxiliary feedwater was initiated to both steam generators. The RCS reached a minimum of 1475 psig and was then increased and maintained at 2000 psig by manual control of an HPI pump.

Restoration of the non-nuclear instrumentation restored all lost indications and controls. Operating personnel secured the auxiliary feedwater pumps and started RCS pressure reduction using the pressurizer spray.

2. Key Systems Behavior - Rancho Seco

The incident at Rancho Seco on March 20, 1978 involved a loss of main feedwater due to operator-induced failure in the ICS non-nuclear instrumentation. The incident was aggravated by the fact that (1) the plant ICS reacted to erroneous instrument readings causing delays in initiating AFW injection and subsequently allowing excessive AFW injection, and (2) the operators had a very limited number of instrument readings which they could trust to manually bring the plant to an orderly shutdown. Since the reactor was at 70% power and had logged considerable operating time (3 1/2 years of commercial operation), the decay heat to be removed was significant, similar to TMI-2.

Auxiliary feedwater was not available for seven minutes after MFW trip. However, this delay was not as serious as at TMI-2 because there was no small LOCA in progress; i.e., a pressurizer safety valve had opened and closed properly.

The transient was eventually brought under control by the operators' diagnosis of which electrical circuit breakers had opened, and then closing them.

3. Event Tree Evaluation - Rancho Seco

The Reactor Safety Study (RSS) stated that on the average a plant can expect about three main feedwater losses of a few minutes duration per year. This value was obtained from the operating experience available at the time the RSS was in progress. The nature of the three main feedwater losses per year was not discussed in great detail. Therefore, the breakdown of the various causes of feedwater transients (such as the Rancho Seco incident) in quantitative terms is not provided in the RSS.

The NRC has investigated feedwater transients at B&W plants and has reported this information in NUREG-0560. At least five of the main feedwater losses attributable to ICS-related failures or malfunctions were identified in that document. Among these is the Rancho Seco incident. There were many other main feedwater losses which licensees felt were not significant enough to be reportable. It is not known how many of these were ICS or non-nuclear instrumentation failure related. The average failure rate of main feedwater for B&W plants subsequent to RSS was reconfirmed at three per year.

The RSS identified several potential transient-initiating events which are associated with the loss of feedwater. Among those identified were the loss of main feedwater pumps and malfunction of control, loss of condensate pumps, loss of A.C. power to the feedwater system, and others. The probability of occurrence of any one specific initiating event may be small. However, when assembled into appropriate categories, the net probability of a given type of transient may be considerable. In this regard, the probability of the event at Rancho Seco is a small part of the larger probability that the main feedwater system will be lost.

This transient may be classified as belonging to sequence #1 on the event tree shown in Figure 1. However, this ICS/NNI initiated transient could have been more severe than it was. That is, the loss of NNI which resulted in erroneous instrument readings delayed the automatic injection of AFW; perhaps even more significant, operator information on the status of the plant was severely limited throughout the transient. The erroneous instrument readings eventually "drifted" to the point of AFW injection some seven minutes into the transient even though the steam generator was apparently dried out by the end of the first minute. It appears that the capability existed at all times for manual action to initiate AFW injection. If erroneous instrument readings or manual actions had never initiated AFW injection, this event would have followed the path of sequence 10 in Figure 1.

Another sequence of significance for this initiating event is sequence #3. If a pressurizer relief valve had become stuck open, this event could have been worse than the TMI-2 sequence, depending on operator actions, because of the additional problem of a lack of instrument readings. However, the specific initiating event, ICS/NNI failure or malfunction, may be somewhat less likely than main feedwater losses due to other causes. Using WASH-1400 data, the overall sequence #1 would have a probability of occurrence of three times per year per plant; the specific (and potentially more severe) case where the loss of NNI is the cause is expected to be a much smaller subset of this category.

TABLE 1

COMPARISON OF THREE B&W REACTOR INCIDENT EVENT SEQUENCES

	TMI-2 (3/29/79)	DAVIS BESSE (9/24/77)	RANCHO SECO (3/20/78)
REACTOR POWER	97%	9%	70%
REACTOR HISTORY	IN COMMERCIAL OPERATION THREE MONTHS.	~1 FULL POWER DAY OF OPERATION.	IN COMMERCIAL OPERATION 3 1/2 YEARS.
TURBINE	TRIPPED IMMEDIATELY.	DOWN ALREADY.	TRIPPED AFTER 5".
REACTOR TRIP	AUTOMATIC AFTER 8" ON HI REACTOR PRESSURE (2355 PSI).	MANUAL (1 MIN. 47") BECAUSE OF RISING PRESSURIZER LEVEL.	AUTOMATIC AFTER 5" ON HI REACTOR PRESSURE.
MFW	BOTH PUMPS TRIP IMMEDIATELY.	1 PUMP TRIP IMMEDIATELY 1 PUMP TRIP 58" LATER.	REDUCED TO ZERO FLOW BY FAULTY ICS SIGNAL (SOME MFW INITIATION BY OPERATOR PROBABLE AFTER 7 MIN.).

TABLE 1 (CONT.)

	TMI-2 (3/29/79)	DAVIS BESSE (9/24/77)	RANCHO SECO (3/20/78)
AFW	NO AFW FOR 8 MIN.	1 PUMP/SG WORKING WITHIN 46". 1 PUMP "UNAVAILABLE" (TURBINE DEGRADED). AVAILABLE MANUALLY AFTER 12 MIN.	NO AFW FOR 7 MIN.
PRESSURIZER RELIEF VALVE	OPENED AFTER 3" AND STUCK OPEN. BLOCK VALVE CLOSED AFTER 138 MIN.	OPENED AFTER 1 MIN. 6", CYCLED RAPIDLY 9 TIMES IN 23" AND STUCK OPEN (STEM GALLING). BLOCK VALVE CLOSED IN 20 MIN.	GAGGED CLOSED. SRV OPENED AND CLOSED PROPERLY
PRESSURIZER	SEVERELY MISLEADING LEVEL INDICATION.	LEVEL INCREASED OFF SCALE.	NO LEVEL PROBLEM.

TABLE 1 (CONT.)

	TMI-2 (3/29/79)	DAVIS BESSE (9/24/77)	RANCHO SECO (3/20/73)
ECCS	HPI AUTOSTARTED (1600 PSI) AT 2'02". 1 PUMP TRIPPED AFTER RUNNING 2 MIN. 36". OTHER PUMP THROTTLED TO MINIMUM FLOW.	HPI AUTOSTARTED (1600 PSI) AT 2 MIN. 57" AND PERMITTED TO RUN FOR 3 MIN. 5". MANUAL SHUTDOWN BECAUSE PRESSURIZER LEVEL NORMAL.	HPI MANUAL AND INTERMITTENT DURING FIRST 13 MIN. THEN AUTOSTART (1600 PSI)
INSTRUMENTS	MOST O.K.	O.K.	ONLY PRESSURIZER LEVEL AND RCS PRESSURE TRUSTED BY OPERATORS DURING FIRST 75 MIN.

TABLE 2

WASH-1400 FAILURE RATES

	FAILURE RATE
1. MAIN FEEDWATER (TM)	3/YR
2. REACTOR TRIP (K)	3.6×10^{-5}/D*
3. AUXILIARY FEEDWATER (L)	3.7×10^{-5}/D*
4. PRESSURIZER RELIEF VALVE OPENS (P_1)	1×10^{-2}/D
5. SAFETY VALVES OPEN (P_2)	3×10^{-5}/D
6. PRESSURIZER RELIEF VALVE CLOSES (Q_1)	1×10^{-2}/D
7. SAFETY VALVES CLOSE (Q_2)	1×10^{-2}/D
8. ECCS - HI PRESSURE INJECTION (C)	3.7×10^{-3}*
9. ECCS DEGRADED OPERATION (C^1)	$>3.7 \times 10^{-3}$*

*ANALYSIS UNIQUE TO SURRY

Memorandum From F. Rowsome to R. Fraley,
"ACRS Query on Material Relevant to Udall
Letter: Davis-Besse and Rancho Seco Transients,"
February 12, 1980

Attachment C

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

February 12, 1980

MEMORANDUM FOR: Raymond F. Fraley, Executive Director
Advisory Committee on Reactor Safeguards

FROM: Frank H. Rowsome, Deputy Director
Probabilistic Analysis Staff
Office of Nuclear Regulatory Research

SUBJECT: ACRS QUERY ON MATERIAL RELEVANT TO UDALL LETTER:
DAVIS BESSE AND RANCHO SECO INCIDENTS

The following question was posed by Congressman Udall's letter of July 27, 1979:

> "Please determine the probabilities of occurrence that, prior to the events, would have been predicted on the basis of WASH-1400 failure rates and methodology as to the probabilities of the sequences of events that occurred at Davis Besse on September 24, 1977 and at Rancho Seco on March 20, 1978."

Needless to say, the predictive probability for a particular historical event can have any value between one and zero depending upon the breadth of the class of events that is taken to represent it. In most cases, a few classifications appear to be "natural" in the sense that "vertabrates" are a natural and distinct grouping of animals. However, there are commonly several levels of event resolution at which one might consider the problem, analogous to the heirarchy of biological classifications: kingdom, phylum, ... , species.

I shall attempt to address Congressman Udall's question using the level of event sequence resolution most natural to WASH-1400, while attempting to sketch answers to several more useful questions, such as:

- Did WASH-1400 consider or predict accidents of this type?
- Could WASH-1400 methods have alerted analysts to the possibility of such accidents if the methods had been applied to the affected plants?
- What improvements in WASH-1400 methods or data are needed to properly consider such sequences in risk assessment?
- Can WASH-1400 methods serve a useful function in analyzing actual experiences?

The Davis-Besse incident, the Rancho Seco incident, and the accident at TMI all entailed feedwater transients, i.e., cessation in the normal delivery of feedwater to the steam generators. The Reactor Safety Study estimated that feedwater transients can be expected to occur between once a year and ten times a year at each nuclear plant. The best estimate in WASH-1400 is three feedwater transients per reactor year. There were roughly 30 reactor years of experience accumulated at B&W reactor plants as of March 28, 1979, the date of the accident at Three Mile Island. WASH-1400 would have lead us to expect between 30 and 300 feedwater transients, most likely about 100 feedwater transients at B&W plants up to that time. In fact, there were about 150 feedwater transients at B&W plants, in good agreement with WASH-1400 failure rate data.

In two of the incidents, the September 24, 1977 incident at Davis Besse and the accident at Three Mile Island, the pressurizer relief valve opened and failed to close, giving rise to a small loss-of-coolant accident (LOCA). WASH-1400 identified this possibility and estimated that the probability that a pressurizer relief valve, having once opened, would fail to close at somewhere between .001 and .10, with .01 (a one percent chance) as the most likely value. On the other hand, the pressurizer relief valve opens only very rarely during feedwater transients at Westinghouse plants, the kind studied in WASH-1400. Therefore, the Reactor Safety Study did not predict a high expected frequency for failed-open pressurizer relief valves initiated by feedwater transients. Had a WASH-1400 type analysis been performed for a B&W plant and had the authors recognized that almost all feedwater transients cause the opening of this valve in B&W plants (before the TMI-inspired changes), then the analysis would have predicted between zero and five (most likely one) occurrences of a stuck open pressurizer relief valve following a feedwater transient in the 30 B&W reactor years. In fact, there were two: Davis Besse on September 24, 1977 and Three Mile Island on March 28, 1979.

The Reactor Safety Study (RSS) did not attempt to distinguish by probability the many types of faults that can give rise to feedwater transients. These were lumped together in one broad category. However, the RSS did acknowledge that some of the failure mechanisms that can trigger a feedwater transient might also compromise the reliability of the systems called upon to respond to the feedwater transient. One example of such common-cause failures was found to be important to the risk in WASH-1400; it is the loss of all AC power at the station. The failure mechanisms responsible for the March 20, 1978 incident at Rancho Seco was a failure of the "Non-Nuclear Instrumentation" DC power supplies. It is also a common-cause failure that both triggered the feedwater transient and also compromised the reliability of the backup auxiliary feedwater system.

Although this class of common mode failures was described and one example was found to be important in WASH-1400, nothing quite like this scenario was found for Surry in WASH-1400. The Surry plant does not depend upon non-safety grade equipment for the autostart of its auxiliary feedwater system. Therefore, Surry is immune to the class of accidents in which non-safety grade instrument power supply failure trips main feedwater and defeats the normal autostart of emergency feedwater.

At Rancho Seco the failure of the autostart of auxiliary feedwater (AFW) was not regarded as a principal cause for concern emerging from the incident, although the risk assessment perspective suggests that it should have been high among the warning flags raised by the event.

It should be noted that the auxiliary feedwater pumps were started at the outset and that their discharge control values did receive two "open" commands. The first of these occurred when one of the faulted steam generator level signals happened to drift into the range triggering AFW delivery. The second occurred after the overcooling commenced in response to the ECCS actuation signal. Thus, neither of these signals could be counted upon to mitigate the initiating event.

In the event that WASH-1400 methods had been applied to Rancho Seco, it is unlikely that the specifics of the short circuit and fuse failure would have been considered that led to the NNI-Y power supply failure. However, it is reasonable to expect that such a study would have idencified the dependency of the auxiliary feedwater autostart system upon the Integrated Control System, and the dependence of both the ICS and the instruments upon the NNI buses.

In summary, the RSS did identify events of the broad class represented by the DB and TMI incidents: feedwater transients with stuck open pressurizer relief valves. The RSS did identify the class and some examples of common mode failures that cause a feedwater trip and degrade the reliability of the auxiliary feedwater system, as at Rancho Seco, but it did not and could not have been expected to predict the right frequency of occurrence for these classes of accidents at B&W plants. A risk assessment of B&W plants might reasonably have been expected to have identified the high susceptibility to transient-induced LOCA intrinsic in the B&W design - the frequent challenge of the pressurizer relief valve that lead to the Davis Besse and TMI accidents. Had the risk assessment been coupled with a careful review and adequacy assessment for operator emergency procedures, the susceptibility of plants to accidents such as TMI or the Rancho Seco incident could have been foretold.

Risk assessment methods also provide a useful framework for organizing the "what if" questions surrounding an actual, historical incident. Application of these techniques can be used to help identify the safety significance of operating occurrences.

Frank H. Rowsome

Frank H. Rowsome, Deputy Director
Probabilistic Analysis Staff
Office of Nuclear Regulatory Research