ATTACHMENT F

BEAVER VALLEY POWER STATION

NO. 1 AND NO. 2 MOISTURE SEPARATOR-

REHEATER STATUS REPORT

TR 2a

DUQUESNE LIGHT COMPANY
Beaver Valley Power Station

Beaver Valley Power Station No. 1 and No. 2
Moisture Separator-Reheater Status Report

August 23, 1988

Prepared by: Scott T. Deahna
Scott Deahna

Reviewed by: Frank A. Beldecos
Frank A. Beldecos

Approved by: Roger E. Martin REM

BEAVER VALLEY POWER STATION NO. 1 AND 2
MOISTURE SEPARATOR-REHEATER REPORT

TABLE OF CONTENTS

Beaver Valley Power Station No. 1 and 2
Moisture Separator-Reheater Report

I. INTRODUCTION

During the Unit 1 sixth refueling outage, extensive repairs were performed on all four (4) Moisture Separator-Reheaters (MSR's). This report discusses 1) factors which led to the Unit 1 MSR damage, 2) results of post 6-R thermodynamic performance analysis, and 3) the future reliability of the Unit 1 MSR's.

The Unit 2 MSR's were evaluated for similar damage susceptibility and present thermodynamic performance.

II. SUMMARY

During the Unit 1 sixth refueling outage, two (2) types of damage were discovered in the MSR's. The first type of damage was the failure of the reheat steam inlet hemihead partition plate. The hemihead partition plate isolates the top half of the U-tube bundle from the bottom half. Its integrity is required to ensure proper reheat steam flow. The second type of damage is the failure of shellside closure plates. The integrity of the closure plates is required in order to direct the turbine cycle steam through the cheveron type moisture separating sections of the MSR without leaking around the reheater.

The failure of the hemihead partition plate was due to an increase in the tube side (partition plate) pressure drop. Partition plate pressure drop increases as steam velocity (flow) through the U-tubes of the reheater increases. Steam flow through the first pass tubes increases as (1) first pass tubes are plugged, (2) with the addition of the vent condenser modification and/or (3) during interceptor/stop valve testing. During interceptor/stop valve testing, the cycle steam flow to one (1) MSR is shut off and diverted mostly to the opposite side MSR, resulting in significantly higher shellside (cycle steam) velocity (flow) rates and corresponding pressure drops. These pressure drops overstress the shellside closure plates. At the same time, the heat transfer across the three (3) active tube bundles is increased due to higher shellside flow and this causes additional reheat steam to be cooled in the tubes, resulting in larger tubeside pressure drops. The increase of pressure difference across the partition plates, due to the arrangement of the vent condenser plus the added pressure unbalance during valve testing, are the prime causes of the partition plate failures. The cumulative effects from interceptor/stop valve testing are considered the primary cause of the shellside closure plate damage.

The Unit 1 MSR hemihead partition plates which failed were 0.50" thick steel plates, reinforced with a rib on the backside. The repair consisted of completely removing this plate and installing a 1.0" thick steel plate with two (2) reinforcing ribs on the top side. The repair prevents access to the lower half of the tube bundle. Although the wet-vacuum tube test procedure can still be utilized and repairs to the top half tube sheet can be made, any tube leaks or lower half tube to tube sheet erosion cannot be repaired and will, therefore, lead to cumulative unrepairable mechanical degradation. The shellside of the MSR's are separated into eight (8) compartments. All closure plates were 0.250" thick. The current standard for closure plate thickness is 0.620". The top-to-side closure plate joint was additionally reinforced by one (1) vertical gusset in each compartment. This reinforcement was not sufficient to prevent the top closure plate upward displacement from failing the top-to-side closure plate joint in one of the center compartments. An additional 0.250" plate was installed to reinforce the top closure plates in the center two (2) compartments of each MSR. Further failure of either type is not anticipated at Unit 1.

Analysis of 100% power Unit 1 MSR System Test Data, taken on June 20, 1988, indicates that the composite MSR System performance compares reasonably well to design parameters. (See Attachment A for a tabulation of composite test data versus design). The Unit 1 reheaters are presently consuming 6.5% greater than design reheat steam flow and the low pressure turbine inlet temperature averages 8.8°F lower than design. If the low pressure turbine inlet steam temperature was increased to the design temperature, the reheat steam flow would increase to a value which would indicate the actual off-design performance of the MSR's. Individual MSR performance varies. No specific operating problems are noted and no single MSR can be identified as a particularly poor performer, based on the calibrated accuracy of the plant and test instrumentation. Moisture separator flow computer points F2012A and F2032A appear to be indicating higher flows, based on a calculated moisture separator removal effectiveness of greater than 100%. As a result, flow transmitters FT-SD-106B and FT-SD-106D should be examined for calibrated accuracy prior to the next test. Also, new calibrated pressure indicators are needed to indicate crossover pressure at the PI-MS-107B and PI-MS-107D locations. The test data indicates a flow imbalance between the A and C train and the B and D train. The A and C train is utilizing 48 KBH more reheat steam than the B and D train. The A and C reheat steam pressure is higher and the A and C cycle steam outlet temperature is 10°F higher than the B and D train. The difference is believed to be a difference in the lifts of the reheat steam flow control valves FCV-MS-100A (C).

The Unit 1 Moisture Separator-Reheater System Composite Test Data (Attachment A) is suitable for input to an actual <u>baseline</u> thermodynamic heat balance.

Following the discovery of the specific MSR failure modes at Unit 1, an investigation was performed to determine the susceptibility of the Unit 2 MSR's to similar failures. It was determined that the Unit 2 MSR hemihead partition plate is 0.750" thick and the shell separation plate is 0.250" thick. In 1980, the following alterations (See Attachment B, Westinghouse MSR Alteration Drawings) were planned for the Unit 2 MSR's:

a. Cycle steam distribution manifold alteration

b. Deck plate addition between the cheveron sections

c. Cheveron inlet perforated plate addition

d. Tube bundle holddown

e. Reinforce hemihead partition plate (add bracing pipe)

f. Reinforce shellside closure plates

The same alterations were to be made to the Unit 1 MSR's in 1978. During 6R, it was verified that alterations (e) and (f) were not completed. Records could not be found to indicate whether all of the alterations were performed on the Unit 2 MSR's. Alterations (e) and (f) are of significant importance to the Unit 2 MSR reliability.

Unit 2 MSR Operating Data collected on August 16, 1988, indicates that the A-MSR hemihead partition plate may have already completely failed. The A-MSR reheat drain tank indicates throttle steam pressure, reheat drain flow (corrected for improper computer point flow coefficient) is low and cycle steam outlet temperature is low. The B-MSR hemihead partition plate may also be damaged based on a reheater high drain tank pressure.

The Unit 2 Moisture Separator-Reheaters are presently under Westinghouse warrantee. All four (4) Unit 2 MSR's should be completely inspected during 1R. Any damage found should be repaired by Westinghouse at no charge to Duquesne Light Company. Particular attention should be given to shellside closure plate reinforcements since the closure plate thickness does not meet current standards. The shellside top closure plate was to have a rib installed in the horizontal direction, running the length of the plate. The rib should also be welded at its ends to the compartment divider plates. This modification is required to enable the MSR's to withstand turbine valve testing. The reheat steam hemihead partition plate should contain a removable section to allow access to the lower half tube sheet and a bracing pipe should be located underneath the partition plate.

A Unit 2 MSR System Performance Test and Analysis Program will be established, following 1R, to obtain baseline heat balance input data and to trend the system performance to determine when tube testing may be required.

III. CONCLUSIONS AND RECOMMENDATIONS

The Unit 1 Moisture Separator-Reheater System is presently utilizing 6.5% excess reheat steam flow with the low pressure turbine inlet steam temperature an average of 8.8°F below design. Further structural damage is not indicated or anticipated. However, tube leaks and lower U-tube, tube-to-tubesheet erosion will continue to degrade the tubes and tubesheet at an accelerated rate. Once degradation occurs, no repairs are possible due to the inaccessibility of the lower half of the tube bundle. Engineering and Testing and Plant Performance should continue to analyze system performance to ascertain when tube bundle replacement will become necessary.

Unit 2 Moisture Separator-Reheater Operating Data indicates that the reheat steam inlet hemihead partition plates are also susceptible to failure. The Unit 2 MSR's should be completely inspected during 1R to ascertain which alterations were not installed and to repair any visible damage. Engineering, with Testing and Plant Performance, should establish a Unit 2 Moisture Separator-Reheater Test and Analysis Schedule following 1R.

BEAVER VALLEY POWER STATION
Moisture Separator-Reheater Report

ATTACHMENT A

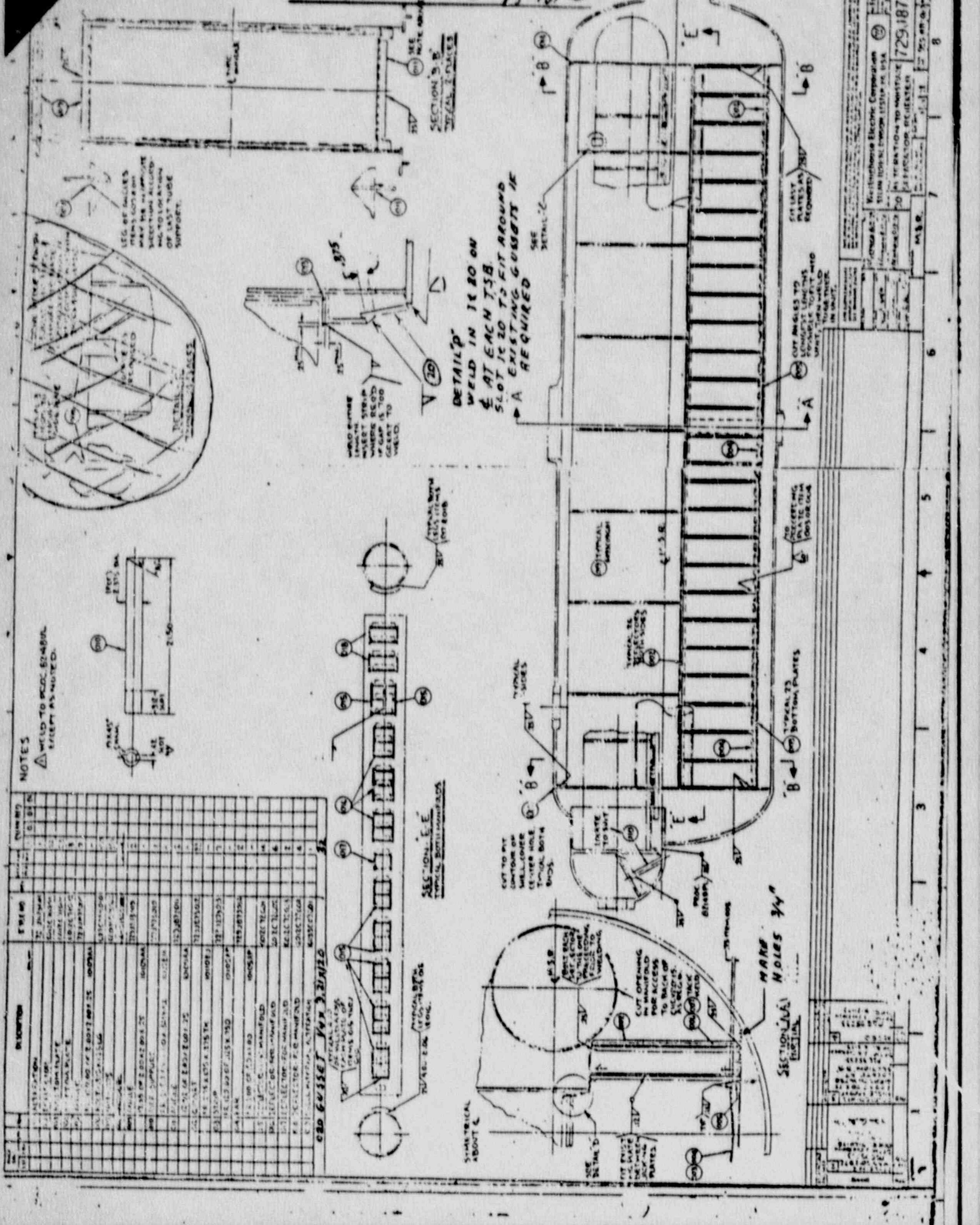
Unit 1 MSR System Composite Test Data Versus Design Values
Design Values from Westinghouse Heat Balance
CT-22484 (2660 MWt)

Parameter	Test Value		Design Value	
Turbine First Stage Pressure	536	PSIA	540	PSIA
Turbine First Stage Flow	10,700	KBH	10,794	KBH
Reheat Steam Flow	772.7	KBH	725.2	KBH
Reheat Steam Pressure	776.9	PSIA	746	PSIA
Reheat Drain Flow	649.9	KBH	572.5	KBH
Reheat Drain Pressure	703.5	PSIA	738	PSIA
Reheat Drain Temperature	503.6	°F	510	°F
Crossunder Pipe Flow	9,179	KBH	9,273.1	KBH
Crossunder Pipe Pressure	216.5	PSIA	218.8	PSIA
Separator Drain Flow	942.4	KBH	877.2	KBH
Separator Drain Temperature	387.8	°F	388	°F
Crossover Pipe Flow	8,236	KBH	8,396	KBH
Crossover Pipe Pressure	185.4	PSIA	202	PSIA
Crossover Pipe Temperature	475.4	°F	484.2	°F

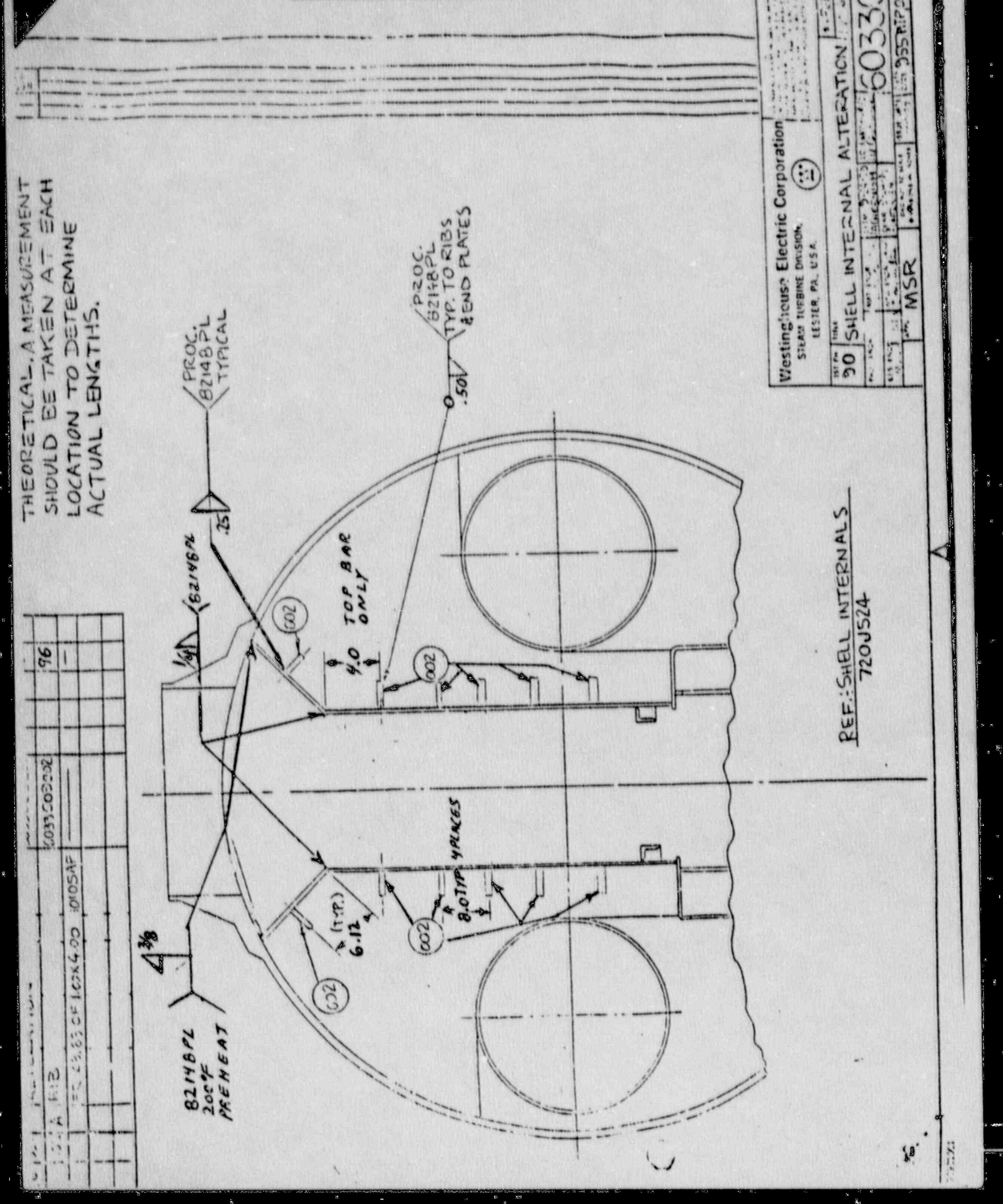
M.S.R. Terminal Temp. Difference	28.3	°F	25	°F
M.S.R. Cycle Steam Pressure Drop	9.55	%	8	%
Low Press Turbine Inlet Superheat	99.9	°F	100	°F

B.U.P.S. Moisture Separator Reheater Report

ATTACHMENT B pg 1 of 2



B.V.P.S. Moisture Separator Reheater Report
ATTACHMENT 13 pg 2 of 2



ATTACHMENT G

[redacted]

ANALYSIS OF THE PROBABILITY OF A NUCLEAR TURBINE REACHING DESTRUCTIVE OVERSPEED

~~8707150693~~

70 pp

TOPICAL REPORT
FOR NRC USE

Copy № 028
WSTG-3-NP-A

ANALYSIS OF THE PROBABILITY OF A NUCLEAR TURBINE REACHING DESTRUCTIVE OVERSPEED

Submitted to:
NUCLEAR REGULATORY COMMISSION
JULY, 1984
JUL 01 1987

Westinghouse Steam Turbine Generator Division

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

FEB 02 1987

Mr. James A. Martin, Fellow Engineer
Generation Technology Systems Division
Westinghouse Electric Corporation
The Quadrangle, MC 203
4400 Alafaya Trail
Orlando, Florida 32826-2399

Dear Mr. Martin:

SUBJECT: APPROVAL FOR REFERENCING OF LICENSING TOPICAL REPORTS WSTG-1-P, MAY 1981, "PROCEDURES FOR ESTIMATING THE PROBABILITY OF STEAM TURBINE DISC RUPTURE FROM STRESS CORROSION CRACKING," MARCH 1974, "ANALYSIS OF THE PROBABILITY OF THE GENERATION AND STRIKE OF MISSILES FROM A NUCLEAR TURBINE", WSTG-2-P, MAY 1981, "MISSILE ENERGY ANALYSIS METHODS FOR NUCLEAR STEAM TURBINES", AND WSTG-3-P, JULY 1984, "ANALYSIS OF THE PROBABILITY OF A NUCLEAR TURBINE REACHING DESTRUCTIVE OVERSPEED"

We have completed our review of the subject topical reports. We find these reports are approved for referencing in license applications to the extent specified and under the limitations delineated in the reports and the associated NRC evaluation which is enclosed. The evaluation defines the basis for the approval of the reports.

We do not intend to repeat our review of the approved matters described in the reports when the reports appear as references in license applications except to assure that the material presented is applicable to the specified plant involved. Our approval applies only to the matters described in the reports.

In accordance with procedures established in NUREG-0390, it is requested that Westinghouse publish approved versions of these reports, proprietary and non-proprietary, within three months of receipt of this letter. The accepted version should incorporate this letter and the enclosed evaluation between the title page and the abstract. The approved version shall include an -A (designating approved) following the report identification symbol.

Contact: S. Lee
X28781

Should our criteria or regulations change such that our conclusions as to the acceptability of the reports are invalidated, Westinghouse and/or the licensees referencing the topical reports will be expected to revise and resubmit their respective documentation, or submit justification for the continued effective applicability of the topical reports without revisions of their respective documentation.

Sincerely,

Charles E. Rossi

Charles E. Rossi, Assistant Director
Division of PWR Licensing-A

Enclosure:
As Stated

cc: W. J. Johnson

5.0 REFERENCES

1. S. H. Bush, "Probability of Damage to Nuclear Components," Nuclear Safety, 14, 3, (May - June) 1973, p. 187; and S. H. Bush, "A Reassessment of Turbine-Generator Failure Probability," Nuclear Safety, 19, 6, (Nov - Dec.) 1978, p. 681.

2. NUREG/CR-1884, "Observations and Comments on the Turbine Failure at Yankee Atomic Electric Company, Rowe, Massachusetts," March 1981.

3. Preliminary Notification of Event or Unusual Occurrence -- PNO - III - 81 - 104 -- "Circle in the hub of the eleventh stage wheel in the main turbine" at Monticello Nuclear Power Station, Nov. 24, 1981.

4. Licensee Event Report No. 82-132, Docket No. 50-361 -- "failure of turbine stop valve 2UV-2200E to close fully" at San Onofre Nuclear Generating Station, Unit 2, Nov. 19, 1982.

5. J. J. Burns, Jr., "Reliability of Nuclear Power Plant Steam Turbine Overspeed Control Systems," 1977 ASME "Failure Prevention and Reliability Conference," Chicago, Illinois (Sept.) 1977, p. 27.

6. D. Kalderon, "Steam Turbine Failure at Hinkley Point A," Proc. Instn. Mech. Engrs., 186, 31/72, 1972, p. 341.

7. W. G. Clark, Jr., B. B. Seth, and D. H. Shaffer, "Procedures for Estimating the Probability of Steam Turbine Disc Rupture from Stress Corrosion Cracking," ASME/IEEE Power Generation Conference Oct. 4-8, 1981, St. Louis, Missouri.

8. Gonea, D. C., "An Analysis of the Energy of Hypothetical Wheel Missiles Escaping from Turbine Casings," General Electric Company - Turbine Department Report, February 1973.

9. S. McHugh, L. Seaman and Y. Gupta, "Scale Modeling of Turbine Missile Impact into Concrete," Final Report NP-2746, February 1983.

10. R. L. Woodfin, "Full-scale Turbine Missile Concrete Impact Experiments," prepared by Sandia National Laboratories under EPRI Research Project 399-1, Final Report NP-2745, February 1983.

11. "Review of Westinghouse Report 1: Procedures for Estimating the Probability of Steam Turbine Disc Rupture from Stress Corrosion Cracking, WSTG-1-P, May 1981," L. J. Teutonico and Y. M. Sanborn, Brookhaven National Laboratory, July 1983. (Proprietary)

12. "Review of Westinghouse Report 2: Analysis of the Probability of the Generation and Strike of Missiles from a Nuclear Turbine, March 1974," L. J. Teutonico, Y. M. Sanborn, and J. G. Almstead, Brookhaven National Laboratory, June 1983. (Proprietary)

13. "Review of Westinghouse Report 3: Missile Energy Analysis Methods for Nuclear Steam Turbines,WSTG-2-P, May 1981," L. J. Teutonico and H. Ming Chen, Brookhaven National Laboratory, December 1983. (Proprietary)

SAFETY EVALUATION REPORT
COMPONENT INTEGRITY SECTION
MATERIALS ENGINEERING BRANCH

WESTINGHOUSE REPORTS:

1. "Procedures for Estimating the Probability of Steam Turbine Disc Rupture from Stress Corrosion Cracking," Westinghouse Steam Turbine Generator Division, WSTG-1-P, May 1981. (Proprietary)

2. "Analysis of the Probability of the Generation and Strike of Missiles from a Nuclear Turbine," Westinghouse Steam Turbine Generation Division, March 1974.

3. "Missile Energy Analysis Methods for Nuclear Steam Turbines," Westinghouse Steam Turbine Generator Division, WSTG-2-P, May 1981. (Proprietary)

4. "Analysis of the Probability of a Nuclear Turbine Reaching Destructive Overspeed," Westinghouse Steam Turbine Generator Division, WSTG-3-P, July 1984. (Proprietary)

SUMMARY AND CONCLUSIONS

The objective of the NRC staff's review of the subject reports was to evaluate and, if appropriate, to approve of the methods and procedures utilized by the Westinghouse Steam Turbine Generator Division (Westinghouse) to determine specific turbine system inspection and testing intervals for their respective utility customers.

During the past few years, the staff has recommended a probabilistic approach to determine turbine rotor inspection intervals and turbine control system maintenance and testing frequencies so as to maintain the as-built turbine system integrity. The Westinghouse reports describe such an approach generically and, to the extent possible, supports it with test and turbine system operating experience data. The staff recognizes that probabilistic analyses based on limited statistical data, especially for a complex system, will include inherent uncertainties. Nevertheless, when the overall approach includes conservative assumptions which overcome the uncertainties, then the ultimate results can be meaningful.

We conclude that the methodology described in the Westinghouse reports is state-of-the-art and is acceptable for use in establishing maintenance and inspection schedules for specific turbine systems. The staff was assisted in its review by Brookhaven National Laboratory, references 11, 12, and 13.

Applicants or licensees who accept Westinghouse's recommendations, based on these reports, should confirm their commitment to the staff and provide a description of their specific maintenance and inspection program including a curve (or curves) of missile probability (P_1) versus service time for their specific turbine rotors.

1.0 BACKGROUND

Although large steam turbines and their auxiliaries are not safety-related systems as defined by NRC regulations, failures that occur in these turbines can produce large, high energy missiles. If such missiles were to strike and to damage plant safety-related structures, systems, and components, they could render them unavailable to perform their safety function. Consequently, General Design Criterion 4, "Environmental and Missile Design Bases," of Appendix A, "General Design Criteria for Nuclear Power Plants," to 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," requires, in part, that structures, systems, and components important to safety be appropriately protected against the effects of missiles that might result from such failures. In the past, with regard to construction permit (CP) and operating license (OL) applications, evaluation of the effects of turbine failure on the public health and safety followed Regulatory Guide 1.115, "Protection Against Low-Trajectory Turbine Missiles," and three essentially independent Standard Review Plan (SRP) Sections 10.2 "Turbine Generator," 10.2.3 "Turbine Disk Integrity," and 3.5.1.3 "Turbine Missiles."

According to NRC guidelines stated in Section 2.2.3 of the SRP and Regulatory Guide 1.115, the probability of unacceptable damage from turbine missiles (P_4) should be less than or equal to about 1 chance in 10 million per year for an individual plant, that is, $P_4 \leq 10^{-7}$ per year. The probability of unacceptable damage resulting from turbine missiles is generally expressed as the product of (1) the probability of turbine failure resulting in the ejection of turbine disc (or internal structure) fragments through the turbine casing (P_1); (2) the probability of ejected missiles perforating intervening barriers and striking safety-related structures, systems, or components (P_2); and (3) the probability of struck structures, systems, or components failing to perform their safety function (P_3).

In the past, analyses assumed the probability of missile generation (P_1) to be approximately 10^{-4} per turbine year, based on the historical failure rate (Ref. 1). The strike probability (P_2) was estimated on the basis of postulated missile sizes, shapes, and energies and on available plant-specific information such as turbine placement and orientation, number and type of intervening barriers, target geometry, and potential missile trajectories (See SRP Section 3.5.1.3 for a description of the evaluation procedures previously recommended by the staff.) The damage probability (P_3) was generally assumed to be 1.0. The overall probability of unacceptable damage to safety-related systems (P_4), which is the sum over all targets of the product of these probabilities, was then evaluated for compliance with the NRC safety objective. This logic places the regulatory emphasis on the strike probability, that is, it necessitates that P_2 be made less than or equal to 10^{-3}, and disregards all the plant specific factors that determine the actual P_1 and its unique time dependency.

Although the calculation of strike probability is not difficult in principle, for the most part being not more than a straightforward ballistics analysis, it presents a problem in practice. The problem stems from the fact that numerous modeling approximations and simplifying assumptions are required to make tractable the incorporation into acceptable models of available data on the (1) properties of missiles, (2) interactions of missiles with barriers and obstacles, (3) trajectories of missiles as they interact with and perforate (or are deflected by) barriers, and (4) identification and location of safety-related targets. The particular approximations and assumptions made tend to have a significant effect on the resulting value of P_2. Similarly, a reasonably accurate specification of the damage probability (P_3) is not a simple matter because of the difficulty in defining the missile impact energy required to render given safety-related systems unavailable to perform their safety functions and the difficulty in postulating sequences of events that would follow a missile-producing turbine failure.

Operating experience shows that nuclear turbine discs crack (Refs. 2 and 3), that turbine stop and control valves fail (Refs. 4 and 5), and that disc ruptures could result in the generation of high-energy missiles (Ref. 6). Analyses (Refs. 5 and 7) show that missile generation can be modeled and the probability can be strongly influenced by inservice testing and inspection frequencies.

During the past few years, the results of turbine inspections at operating nuclear facilities indicate that cracking to various degrees has occurred at the inner radius of turbine discs of Westinghouse design. Within this period, a Westinghouse turbine disc failure occurred at one facility owned by the Yankee Atomic Electric Company (Ref. 2). More recent inspections of General Electric turbines have also discovered disc keyway cracking (Ref. 3). Stress corrosion has been identified by both manufacturers as the operative cracking mechanism.

In view of operating experience and NRC safety objectives, the NRC staff has shifted emphasis in the reviews of the turbine missile issue from the strike and damage probability (P_2xP_3) to the missile generation probablity (P_1) and, in the process, has attempted to integrate the various aspects of the issue into a single, coherent evaluation.

Through experience of reviewing various licensing applications, the staff has concluded that P_2xP_3 analyses provide only "ball park" or "order of magnitude" values. Based on simple estimates for a variety of plant layouts, the staff also concludes that the strike and damage probability product (P_2xP_3) can be reasonably taken to fall in a characteristic narrow range which is dependent on the gross features of plant layout with respect to turbine generator orientation; i.e., (a) for favorably oriented turbine generators P_2xP_3 tends to lie in the range of 10^{-4} to 10^{-3} and (b) for unfavorably oriented turbine generators P_2xP_3 tends to lie in the range 10^{-3} to 10^{-2}. In addition, detailed analyses such as those discussed in this evaluation show that, depending on the specific combination of material properties, operating environment, and maintenance practices, P_1 can have values from 10^{-9} to 10^{-1} per turbine year depending on the turbine test and inspection intervals. For these reasons, in the evaluation of P_4 (= $P_1xP_2xP_3$), the probability of unacceptable damage to safety-related systems from potential turbine missiles, the staff is giving credit for the product of the strike and damage probabilities of 10^{-3} for a favorably oriented turbine and 10^{-2} for an unfavorably oriented turbine, and is discouraging the elaborate calculation of these values.

The staff believes that maintaining an initial small value of P_1 through turbine testing and inspection is a reliable means of ensuring that the objectives precluding turbine missiles and unacceptable damage to safety-related structures, systems, and components can be met. It simplifies and improves procedures for evaluation of turbine missile risks and ensures that the public health and safety is maintained.

To implement this shift of emphasis, the staff recently has proposed guidelines for total turbine missile generation probabilities (Table 1) to be used for determining (1) frequencies of turbine disc ultrasonic inservice inspections and (2) maintenance and testing schedules for turbine control and overspeed protection systems. It should be noted that no change in safety criteria is associated with this change in emphasis.

Table 1. Turbine System Reliability Criteria

	Probability, yr^{-1}		
	Favorably Oriented Turbine	Unfavorably Oriented Turbine	Required Licensee Action
(A)	$P_1 < 10^{-4}$	$P_1 < 10^{-5}$	This is the general, minimum reliability requirement for loading the turbine and bringing the system on line.
(B)	$10^{-4} < P_1 < 10^{-3}$	$10^{-5} < P_1 < 10^{-4}$	If this condition is reached during operation, the turbine may be kept in service until the next scheduled outage, at which time the licensee is to take action to reduce P_1 to meet the appropriate A criterion (above) before returning the turbine to service.
(C)	$10^{-3} < P_1 < 10^{-2}$	$10^{-4} < P_1 < 10^{-3}$	If this condition is reached during operation, the turbine is to be isolated from the steam supply within 60 days, at which time the licensee is to take action to reduce P_1 to meet the appropriate A criterion (above) before returning the turbine to service.
(D)	$10^{-2} < P_1$	$10^{-3} < P_1$	If this condition is reached at any time during operation, the turbine is to be isolated from the steam supply within 6 days, at which time the licensee is to take action to reduce P_1 to meet the appropriate A criterion (above) before returning the turbine to service.

2.0 SCOPE OF REVIEW

There are essentially two modes of turbine failure that can result in turbine failure; one due to rotor material failure at approximately the rated operating speed, or one due to failure of the overspeed protection systems resulting in excessive rotor speeds.

Failures of turbine discs at or below the design speed, nominally 120 percent of normal operating speed, can be caused by small flaws or cracks left during fabrication or those that initiate during operation and grow to critical size either by fatigue crack growth, by stress corrosion crack growth,or by a combination of both of these mechanisms. Cracks in the bore or hub region of turbine discs could eventually lead to disc failure.

Failures of turbine discs at the destructive overspeed can result from a failure of the governor and overspeed protection systems, consisting of: (i) speed sensing and tripping systems and (ii) steam valves. If the turbine is out of control, its speed can increase until failure occurs. For unflawed discs, destructive overspeed is reached at about 180 to 190 percent of the normal operating speed. In general, failures that occur at destructive overspeed are caused by stresses which exceed the materials tensile strength.

In the event of a turbine disc burst, high velocity missile-like fragments may break through the turbine casing, possibly generating secondary missiles. These missiles have a potential of damaging reactor safety systems. Alternately, the disc fragments could be arrested and contained by turbine itself. Hence, in evaluating the risk associated with turbine disc rupture, it is necessary to determine whether or not missiles external to the casing can be generated by postulated disc ruptures.

This SER considers the above possibilities and summarizes the review and evaluation of the Westinghouse reports, listed earlier, which describe Westinghouse procedures for estimating (a) the design speed missile generation probability, (b) the destructive overspeed missile generation probability, and (c) the perforation of the turbine casing by turbine disc burst fragments.

3.0 DISCUSSION/EVALUATION

Following are summaries of evaluations performed by Brookhaven National Laboratory (BNL) as contractor to NRC staff:

3.1 Procedures for Design Speed Failure Probability Calculations (Report 1)

This subsection evaluates the procedures used by Westinghouse for calculating the design speed probabilities of disc rupture and turbine missile generation. The results of the evaluation yield the following conclusions and recommendations:

1. The methodology employed for the calculation of disc rupture and turbine missile generation probabilities is a straightforward application of probabilistic concepts.

2. The use of fracture mechanics to develop a critical crack size model is a standard approach to problems in which criteria are established for fracture instability in the presence of a crack. The modifications introduced by Westinghouse based on their observations of bore and keyway cracks are reasonable.

3. The crack growth rate equation is derived by classical regression methods. The choice of model which relates the natural log of the crack growth rate directly to yield stress and reciprocal temperature is justified by the data.

4. The methodology was checked out in a test case supplied by Westinghouse. There was virtual agreement between the BNL and Westinghouse calculations of the probabilities of disc rupture and turbine missile generation.

5. Our (i.e., BNL's) only reservation concern the input data to the calculations of crack initiation probabilities, critical crack size, and crack growth rate; discussed separately, as follows:

   a) Crack Initiation Probabilities: To evalute the effect of the uncertainties of the crack initiation probability estimates, it is suggested that the turbine missile generation probability be calculated using the conservative estimates of crack initiation probabilities for the turbine units without existing cracks in their discs.

   b) Critical Crack Model: Our concern here is with the calculation of the variance of the critical crack depth. The variance is related to the variations in fracture toughness and bore stress. The variability supplied by Westinghouse for the latter appears reasonable. We have doubts about the former only because the variation of K_{Ic} depends on the values of Charpy energy and yield strength provided by the disc supplier, and we do not know to what extent these have been checked by Westinghouse. In the British work it was found (upon test) that the Charpy energies were significantly lower than the supplied values. If the variability of K_{Ic} is indeed larger, then the variance of a_{cr} is also, and the calculated values of P_1 would be higher. Also, not having seen the data, we do not know if the assumption of variability equal to three (3) standard deviations is justified. Even if the magnitudes of the variabilities are correct, setting them equal to two (2) standard deviations would result in higher values of P_1.

c) Crack Growth Rate: The crack growth rate equation derived by regression is only as good as the raw data on which it is based. The latter contain a number of uncertainties (discussed above), principal of which appears to be the time of crack initiation. The assumption of zero incubation time to initiation underestimates the crack growth rate. Since some of the service times employed in the calculations are only a factor of two (2) or so larger than experimentally determined crack initiation times, the use of a zero incubation time could have a pronounced bearing on the calculation of crack growth rate. The question of incubation time can only be resolved by reinspection. Until that is done, it is recommended that a more conservative estimate of crack growth rate be utilized in the calculation of P_1. Use of a more conservative crack growth rate will increase the value of the turbine missile generation probability P_1.

The NRC staff recognizes BNL's reservations with regard to Report 1. In the past we have reviewed crack initiation probabilities, critical crack sizes and crack growth rates with Westinghouse on numerous occasions during our evaluations of case-specific issues. While there are uncertainties in the above areas, we believe that Westinghouse's overall analysis is conservative and is essentially consistent with the staff's recommendations.

3.2 Overspeed Failure Missile Generation Probabilities (Report 2)

An evaluation is made of the procedures used by Westinghouse for calculating the probability that the turbine will attain the destructive overspeed condition following a full load system separation resulting in the generation of turbine missiles. No discussion of the probability of such a system separation was included; for most of the calculations an average rate of one (1) per year has been assumed.

Calculations were carried out for two (2) confidence levels at 95 and 50%. These confidence levels do not refer to the calculated probabilities P_1 but rather to certain input values used to make the calculations; i.e., confidence bounds on the probability of malfunction for the basic events were obtained and used to generate the P_1 values. Cases 1 and 2 are considered by Westinghouse to be very conservative upper bounds on the overspeed probability. Cases 3 and 4 are considered to be best approximations to a point estimate of the true overspeed probability.

Report 2 proceeds in a logical and straightforward manner: development of a turbine model and a model for overspeed probability, construction of a fault tree for destructive overspeed, calculation of basic event probabilities from service experience or estimates, and direct evaluation of the fault tree (using the basic event probabilities) to obtain P_1, the probability of destructive overspeed.

Although Report 2 appears to present a thorough analysis of the problem of destructive overspeed, a number of points remain to be clarified or resolved:

i) the general applicability of the turbine model to current units should be demonstrated;

ii) the requisite system schematics should be supplied in order to confirm the applicability of the generic fault tree;

iii) with regards to the calculation of the basic event probabilities for which there were not sufficient service data and hence required estimates, a discussion of how the estimates were made and a demonstration of conservatism are needed;

iv) with information supplied as to which basic events are valve specific and which are not, an attempt should be made to resolve the discrepancey between the BNL and Westinghouse calculations of destructive overspeed probability; and

v) with the discrepancy resolved, the quantitative importance of minimal cut sets and components should be determined (since these could point the way toward a possible reduction in P_1).

The NRC staff has considered BNL's comments regarding Report 2. This subject has also been discussed with Westinghouse in the past. The difficulty in doing a generic review of turbine overspeed probability arises because of the variety of overspeed control systems and valve design details found in service. Also, maintenance and testing procedures can differ. Control systems are generally complex and contain redundant elements. Their reliability in commercial applications has been demonstrated to be good. As a consequence, the contribution of potential overspeed failures to P_1 is relatively small and the uncertainties mentioned by BNL do not significantly affect the overall turbine system failure probability. Subsequent to the BNL review of Report 2, Westinghouse submitted Report 4 (which BNL did not review). This latter report addresses BNL's concern. Based on our reviews of specific cases and on our review of Report 4, the staff believes that Westinghouse treats this matter in a reasonable manner.

3.3 Disc Fragment Containment Analysis (Report 3)

This subsection evaluates the procedures used by Westinghouse for calculating the perforability of turbine casings by disc fragments. The evaluation is summarized as follows:

1. The Hagg-Sankey method of containment analysis has been reviewed and found acceptable because the criteria for penetration/containment given in the Hagg-Sankey work are clearly supported by test results.

2. The disc fragment penetration/containment criteria of the Hagg-Sankey method are applicable only to the model structures for which they were derived. The subject report extends the principles of the Hagg-Sankey method to actural turbine structures and utilizes the results of additional testing carried out by Westinghouse during 1979. Modifications to accommodate ring-type stationary structures include: (a) consideration of asymmetric collisions, two-ring collisions, brittle fracture, and piercing, (b) calculation of the effective mass of rings with irregular cross-sections for momentum transfer, and (c) calculation of energy-absorbing capacities in shearing/stretching of rings with bolt joints. The numerous cases and subcases of possible collisions which are presented in the subject report involve calculations of effective target mass, effective heights, effective thicknesses, etc. Although the analytical approach appears reasonable, no correlations are presented between the analytical results and the experimental test results (as in the Hagg-Sankey paper). Hence, one cannot say to what degree the predicative calculations (based on the subject report) will be reliable.

3. It is assumed that the Westinghouse tests were not full scale tests. The question of scalability has been addressed by other investigators. Turbine missile impact experiments were carried

out for both full scale and 1/5 scale models (120° disc sectors for both blunt and piercing impact orientations) and the results published in two (2) recent reports. The results of the scale model experiments agreed well with the results of the full-scale experiments and were sufficient to demonstate scalability.

4. It should be noted that, as far as the calculation of P_1 (the probability of missile generation) is concerned, the only information required is whether or not the fragment is contained. Specific values of the weight, velocity, and kinetic energy of exiting missile fragments have no bearing on the P_1 calculation. For contained fragments, no distinction is made between the case in which a disc bursts but is contained and the case in which no burst is possible, as far as evaluating the risk of missiles is concerned.

Unless a ruptured turbine disc results in a fragment that penetrates the turbine casing and becomes a missile, the potential consequences to facility safety systems is minimal. Therefore, it is desirable to know the probability of various size discs of doing so should they rupture. Unfortunately, this knowledge is impractical to obtain by resorting to many full-scale tests using modern turbine geometry. Hence, one must rely on interpretations of existing data, engineering judgments and analytical models. As Brookhaven acknowledges, Westinghouse has performed tests to validate their model to the extent practical. The staff agrees with Brookhaven that the Westinghouse analytical approach appears reasonable.

3.4 Probability of Reaching Destructive Overspeed (Report 4)

This report is an update of the 1974 report, "Analysis of the Probability of the Generation and Strike of Missiles from a Nuclear Turbine" (Report 2) in the areas relating to destructive overspeed. The effects of valve testing frequency on the destructive overspeed probability are incorporated. A sensitivity study on valve inspection intervals was also made. The values presented in this report for the destructive overspeed probability apply to Westinghouse turbines with either the analog electro-hydraulic (AEH) control system or the digital electro-hydraulic (DEH) Mod 1 and Mod 2 control systems and BB 296 steam chest type main steam inlet features. The probability values reported are based on the service experience where available and estimates and assumptions where such data were not available. When estimates were necessary, every effort was made to be on the conservative side. It is Westinghouse's and our opinion that the probability values reported are conservative.

4.0 CONCLUSIONS AND RECOMMENDATIONS

The interconnections of subjects presented in the subject reports and their relevancy to NRC reviews of the turbine missile issue for plants with Westinghouse turbines are readily apparent from Section 1 of this SER and the above summary discussions. The design speed and destructive overspeed turbine missile generation probabilities described in the reports are to be summed to determine conformance to NRC criteria as outlined in Table 1, and the turbine casing perforability described in Report 3 is to be used together with turbine disc burst probabilities at both design speed and destructive overspeed to obtain the corresponding missile generation probabilities. We conclude that the methodology described in the subject reports is state-of-the-art and is acceptable. Additional comments follow:

4.1 Design Speed Failures

We had two (2) concerns with regard to the subject discussed in Report 1; one is in connection with temperature uncertainties and the other is in connection with crack initiation.

1. During the course of the review, Westinghouse was questioned about their method of analysis to determine the temperature of discs and the effect of temperature uncertainties on the missile generation probability. The Westinghouse response was that they used standard heat transfer techniques and that the effect of temperature uncertainties was negligible. The BNL review showed that indeed small, systematic, uniform errors in the data base temperatures have a negligible effect on the missile generation probability.

2. In their crack growth rate model, Westinghouse assumed that all cracks have a zero initiation time; i.e., for their data base, they calculated the rate of crack growth for cracks in each damaged disc by dividing the depth of the cracks by the total number of operating hours at the time of inspection. Correspondingly, when predicting the probability for a new disc of a crack exceeding the critical crack depth, they assume that if a crack can initiate it will do so when the unit begins service. To support this assumption, Westinghouse states that the non-conservatism introduced in the treatment of the data base is at least off-set by over-conservatism in the application of the probability. The staff agrees.

4.2 Destructive Overspeed Failures

The staff recommends that for a case-specific application, Westinghouse use procedures for calculating destructive overspeed missile generation probabilities which incorporate the turbine governor and overspeed protection system's speed sensing and tripping characteristics, the design and arrangement of main steam control and stop valves and the reheat steam intercept and stop valves, and the lengths of inservice testing and inspection intervals for system components and steam valves. Particular attention should be paid to information as delineated in subsection 3.2 of this evaluation.

4.3 Disc Fragment Containment Analysis

Report 3 addresses the method for the determination of whether or not a disc burst will result in missiles being ejected from the turbine casing, and if so, the external kinetic energy of the exiting missiles.

SUMMARY

This report is an update of the 1974 report, "Analysis of the Probability of the Generation and Strike of Missiles from a Nuclear Turbine" in the areas relating to destructive overspeed. The effects of valve testing frequency on the destructive overspeed probability are incorporated. A sensitivity study on valve inspection intervals was also made. The values presented in this report for the destructive overspeed probability apply to Westinghouse turbines with either the analog electro-hydraulic (AEH) control system or the digital electro-hydraulic (DEH) Mod 1 and Mod 2 control systems and BB 296 steam chest type main steam inlet features. The probability values reported are based on the service experience where available and estimates and assumptions where such data were not available. When estimates were necessary, every effort was made to be on the conservative side. It is our opinion that the probability values reported are very conservative.

In this report, three basic values of the probability of destructive overspeed per loss of load incident are provided as relevant values for Westinghouse turbines. These are 3.1×10^{-9} for weekly valve testing, 1.9×10^{-8} for monthly testing, and 1.6×10^{-6} for yearly testing. To obtain the probability of destructive overspeed per year per unit, one must multiply the above probability by the average number of load rejections per year with sufficient steam flow to go to destructive overspeed.

I. INTRODUCTION

In 1974, the Westinghouse Steam Turbine Division wrote report [4] "Analysis of the Probability of the Generation and Strike of Missiles from a Nuclear Turbine" and made it available to the NRC for review. This earlier report contains a comprehensive probability analysis for the generation and strike of missiles that may arise from overspeed in a nuclear LP turbine. The analysis work and results are reported in various Westinghouse Research Reports [1-3]. This report is in response to the NRC request to update the destructive overspeed probability section of the 1974 report by: adding the LP turbine operating experience accumulated since 1972 and revising the study to account for the effects of valve testing frequency and valve inspection interval. The information in this report was derived from a Westinghouse internal report [5].

The probability values presented in this report for the destructive overspeed in the event of loss of load apply to Westinghouse turbines with either the analog (AEH) or digital (DEH) electro-hydraulic control systems and BB 296 steam chest type main inlet features. The values reported are based on the service experience of Westinghouse turbines where available and estimates and assumptions where such data were not available. As was done before, when estimates were necessary, every effort was made to be on the conservative side. It is the opinion that the probability values reported are conservative.

Section II of this report gives a description of the problem, and Section III describes the model for destructive overspeed in the event of a loss of load and introduces the fault tree representation of the model. Section IV describes the data on operating experience and malfunctions that were collected and analyzed to obtain the basic event probabilities. These are needed in analyzing the destructive overspeed fault tree of section III. Section V presents the values of destructive overspeed probability as a function of the valve testing frequency. Some results on the effect of valve inspection interval are also included in the form of a sensitivity study. Section VI contains discussion and conclusions, and the remaining sections consist of technical appendices and references.

II. PROBLEM DESCRIPTION

There are three areas that need to be discussed in connection with the definition of the problem. The first is the system configuration of the type of turbine-generator being considered. The second is the nature of the overspeed conditions being studied. The third is the precise meaning of the probabilities that are calculated.

Figure 2-1 is a schematic representation of a typical nuclear turbine unit we have considered. The unit consists of one high pressure (HP) and three low pressure (LP) turbines. The steam flow into the HP turbine comes through two independent steam chests, each of which has two throttle (stop) valves on the upstream side and two governor (control) valves on the downsteam side. This steam chest configuration is designated as a BB 296 steam chest in this report. These valves are taken to be plunger type valves of the type currently in use on Westinghouse nuclear units, and each is controlled by a separate servo (Moog) valve. The HP exhausts to moisture separator and reheater (MSR) tanks from which the LP turbines are fed. Each LP turbine has two inlet steam lines, each of which carries a reheat stop valve and an inteceptor valve, in that order. The specifications of the reheat stop valves and interceptor valves are irrelevant to the present study, as the destructive overspeed condition arises independent of whether these valves are closed or not.

The analysis is applicable to a turbine unit equipped with AEH, DEH (MOD 1), or DEH (MOD 2) control system and mechanical trip protection system and with the BB 296 steam chest configuration. The system considered is one in the form that is currently in operation. In addition, the dual drain arrangement for the overspeed protection controller trip and emergency electrical trip consisting of a primary drain backed up with a secondary drain is used as standard. The general process by which a *destructive overspeed* condition is reached will now be described. It begins with a unit load separation from the system. Then, because of a succession of malfunctions in the protection system, the steam supply to the HP and/or LP turbine is not properly interrupted and an overspeed condition occurs. In this report, an assumption is made that the turbine speed will reach the destructive overspeed unless the steam supply to the HP can be stopped by closing throttle and/or associated governor valves. This is a conservative assumption as it does not consider other events which would prevent reaching destructive overspeed.

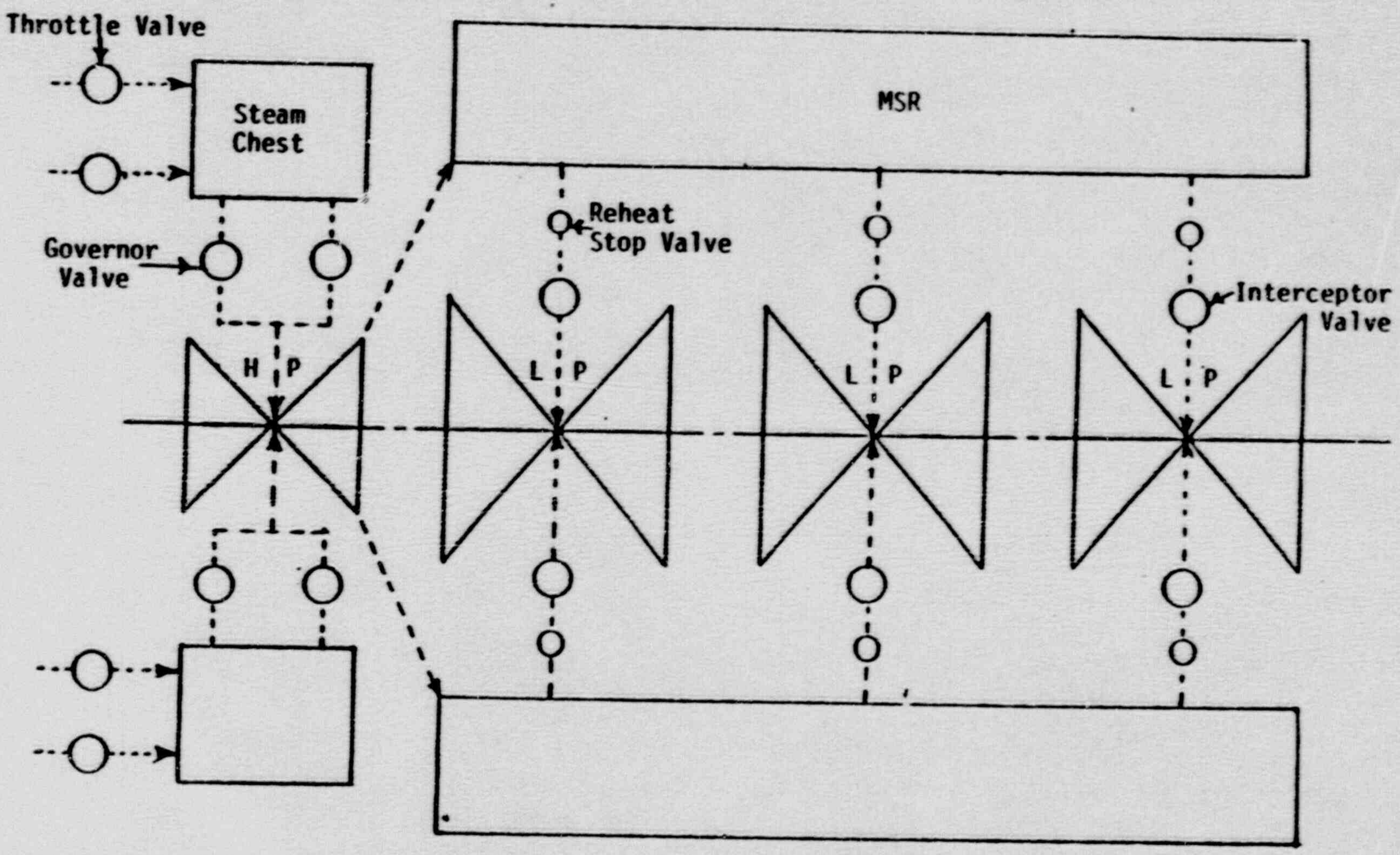
The problem can now be stated in this way: given that a unit load separation from the system has occurred, estimate the probability that the ensuing succession of malfunctions will lead to a turbine condition of destructive overspeed. The definition we have used is as follows:

Destructive overspeed for a specific unit is the lowest calculated speed at which any LP rotor disc will burst based on the average tangential stress being equal to maximum ultimate tensile strength of the disc material, assuming no flaws or cracks in the disc.

Operationally, the destructive overspeed is considered to result only from the failure of at least one steam chest to close the steam inlet path following a load dump due to a system separation. In particular, the failure to close one throttle valve and one associated governor valve of one of the two steam chests is taken as a minimal condition that leads to destructive overspeed.

The probabilities determined are conditional probabilities. That is, the concern is with the probability of a certain event only when it is known that a prescribed circumstance exists. In particular, the probability of destructive overspeed given a load dump due to a system separation is estimated. A second feature of the probabilities being determined here is that they are defensible, conservative bounds on the true probabilities rather than merely point estimates. They are defensible in the sense that all are derived from Westinghouse experience that can be documented, and they are conservative in the sense that all are upper limits on the true probabilities.

It is believed that the true values of the probabilities of destructive overspeed given a load system separation are no greater than, and in many cases are much smaller than, the values presented in this report.



RELEVANT STEAM PATHS SHOWN WITH DASHED LINES

FIGURE 2-1. TURBINE SCHEMATIC AND WESTINGHOUSE BB 296 STEAM CHEST CONFIGURATION FOR PROBABILITY ANALYSIS

III. MODEL FOR DESTRUCTIVE OVERSPEED: FAULT TREE

Presented is a general discussion of how various overspeed conditions can occur during the normal operation of a generating plant. The turbine speed and load are controlled by the amount of steam going into the turbines, and the only way to prevent the turbine from reaching an excessive speed when the load is lost is by stopping the steam flow into the turbines.

Under normal operating conditions, the turbine speed is kept at 100% of its rated speed, and it is controlled by the system frequency. If for any reason the load is lost and the circuit breaker opens, the turbine speed will in most instances increase above the rated speed. If a loss of load occurs when carrying greater than 30% rated unit load and the breakers open, the load drop anticipator function of the overspeed controller (OPC) rapidly closes both the governor and interceptor valves in an attempt to prevent excessive overspeed such that a turbine trip is prevented. The interceptor valves are "modulated" to reduce the speed to rated speed and then the governor valves are opened to maintain synchronous speed. The turbine generator is ready for resynchronizing. If the turbine speed is not arrested and reaches the overspeed trip setting (usually 110% - 111% rated speed), the mechanical emergency trip device should activate and trip close all the governor, throttle, reheat stop and interceptor valves. In addition, the electrical overspeed trip device should activate at approximately the same speed to close the valves.

The overspeed function of the OPC activates if the breakers open and the overspeed reaches 103% rated speed. Both the governor valves and interceptor valves are rapidly closed and operate in the same manner as descrived for the load drop anticipator function.

If all the steam inlet flows are stopped by an emergency trip mechanism, the turbine speed will not exceed the design overspeed of 120%. However, if the steam continues to flow into the turbine due to some malfunction, the turbine speed will continue to go up beyond the 120% level, and it could even reach the destructive overspeed level of around 180%, provided that at least one of the two main steam inlets is not closed.

Presently the concern is with only the destructive overspeed condition. The above model was used to generate a fault tree diagram leading to the "top event" of reaching destructive overspeed given that a loss of load incident has occurred. The fault tree diagram is given in Figure 3-1. There are two basic overspeed protective systems used for Westinghouse turbines. They are distinguished by calling one the "mechanical trip system" and the other the "electrical trip system". The mechanical trip system or the electrical trip system may be combined with either the AEH, DEH (MOD 1), or DEH (MOD 2) control system. The mechanical trip system is used on most units in service at the current time, and this analysis deals with the mechanical trip system. The fault tree corresponds exactly to the diagram in Figure 3-2 with an AEH control system. Its corresponding throttle and governor valve servo actuator assembly diagram is given in Figure 3-3.

In developing the fault tree, 31 different types of basic events are identified in Table 4-1, and of these, basic event nos. 15, 25, and 26 do not appear in the fault tree. The basic event nos. 15 and 25 are identified in the current study so that the basic event numbers are consistent with those appearing in earlier reports [1,4], and the basic event no. 26 was identified as it appears in both DEH (MOD 1) and DEH (MOD 2). Altogether 87 independent basic events (arising from the 31 different types of basic events) actually appear in the fault tree, and they are clearly marked by basic event number on the fault tree. The probabilities of destructive overspeed events will be calculated based on the basic event probabilities obtained in section IV and the fault tree described in this section. The results will be given in section V.

In summary, the turbine may reach destructive overspeed if the following events occur simultaneously: (i) system separation with a sufficient steam supply into the turbine (for example, the load is lost and the breaker opens during normal operation), and (ii) either a combination of failures in the overspeed protection and emergency trip systems or valve failures which cause the main steam inlet to be kept open. Since the destructive overspeed condition can occur only if the main steam inlet is not closed, one needs to consider only the governor valves and throttle valves, and that is why the reheat stop valves and interceptor valves do not appear in the fault tree diagram. The symbols used in fault trees are briefly discussed in Appendix A.

FIGURE 3-1a. FAULT TREE LEADING TO DESTRUCTIVE OVERSPEED: MAIN TREE - Part 1 of 6

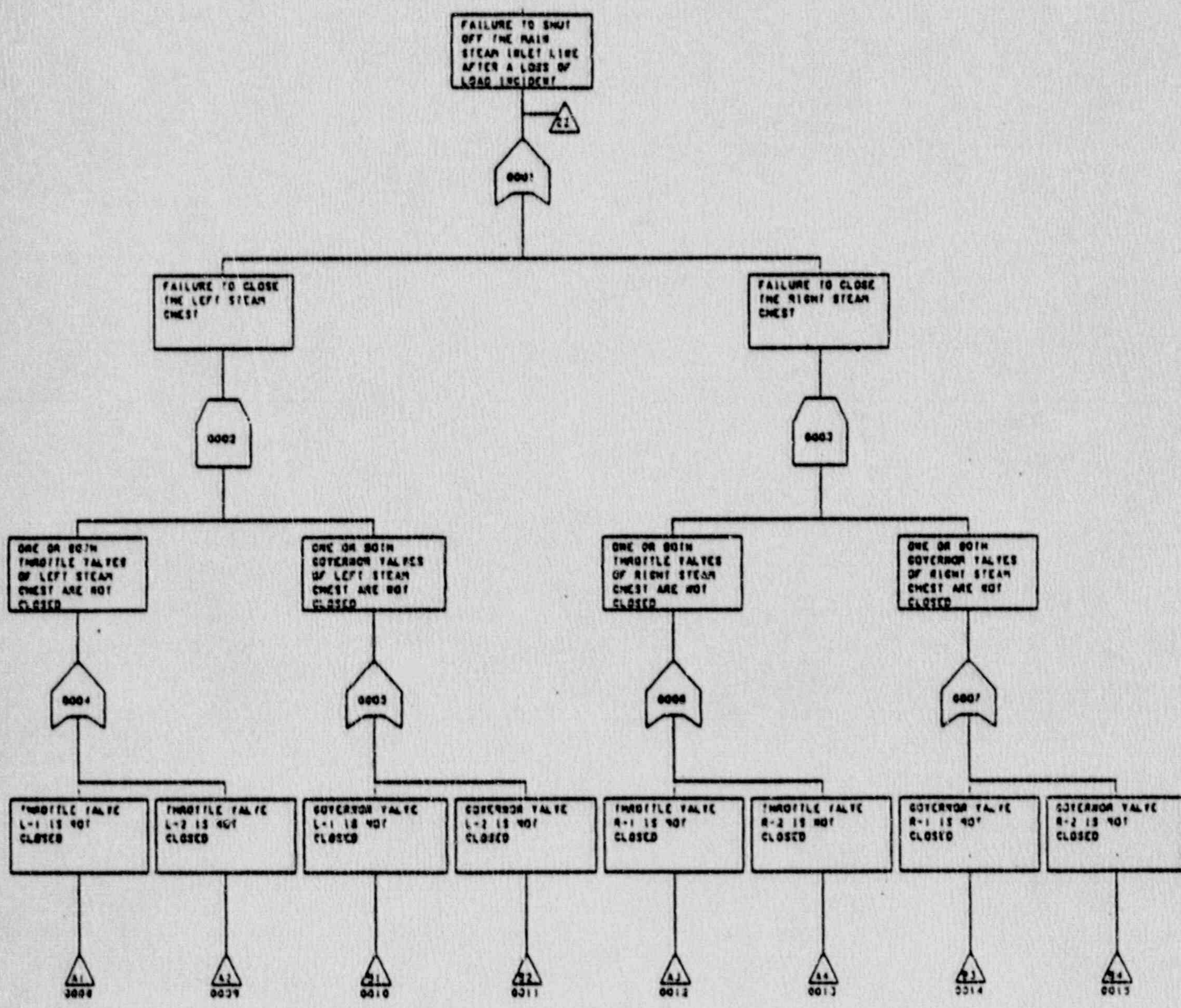


FIGURE 3-1b. FAULT TREE LEADING TO DESTRUCTIVE OVERSPEED: SUBTREES A1 AND A2 - Part 2 of 6

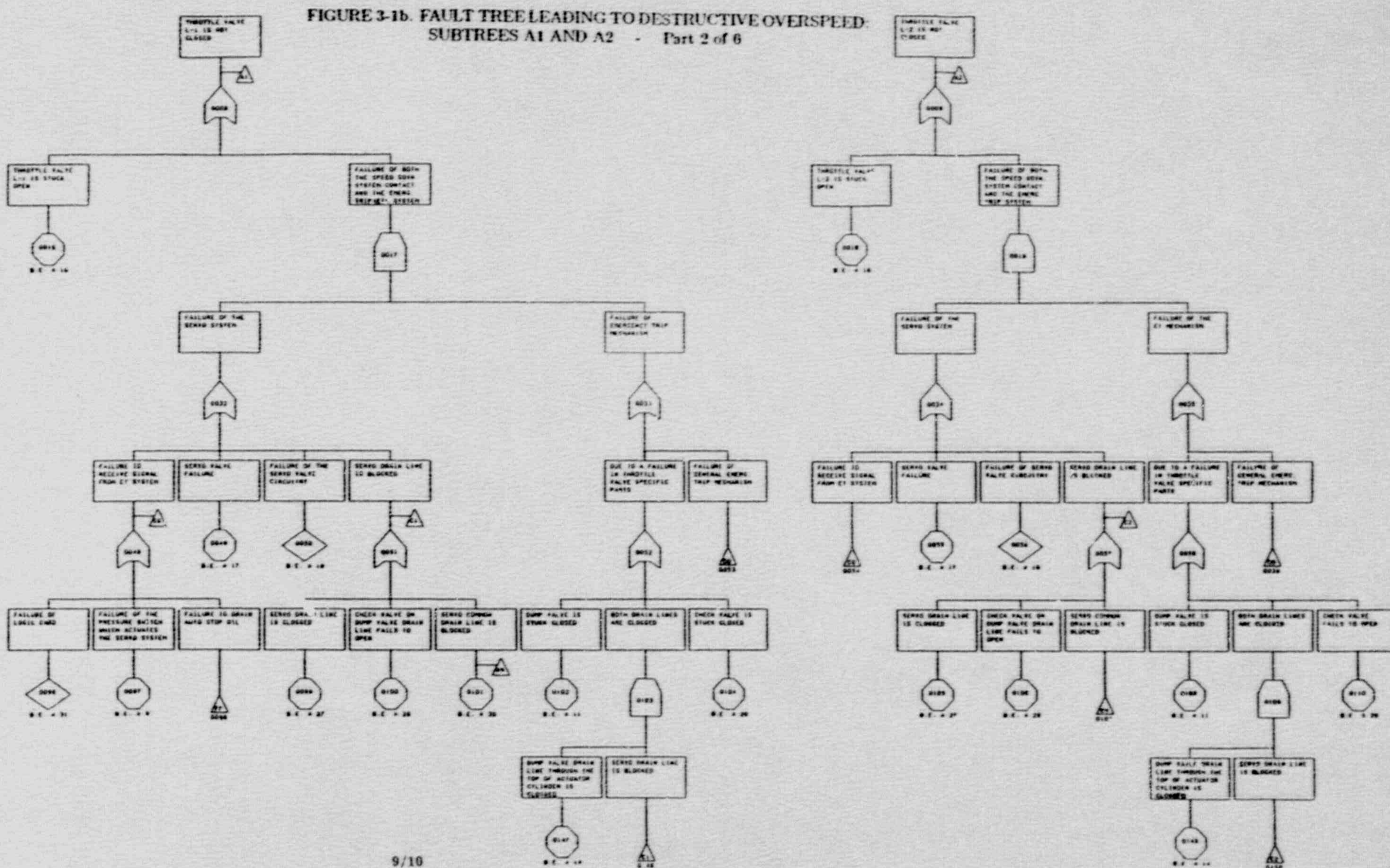


FIGURE 3-1c. FAULT TREE LEADING TO DESTRUCTIVE OVERSPEED: SUBTREES B1 AND B2 - Part 3 of 6

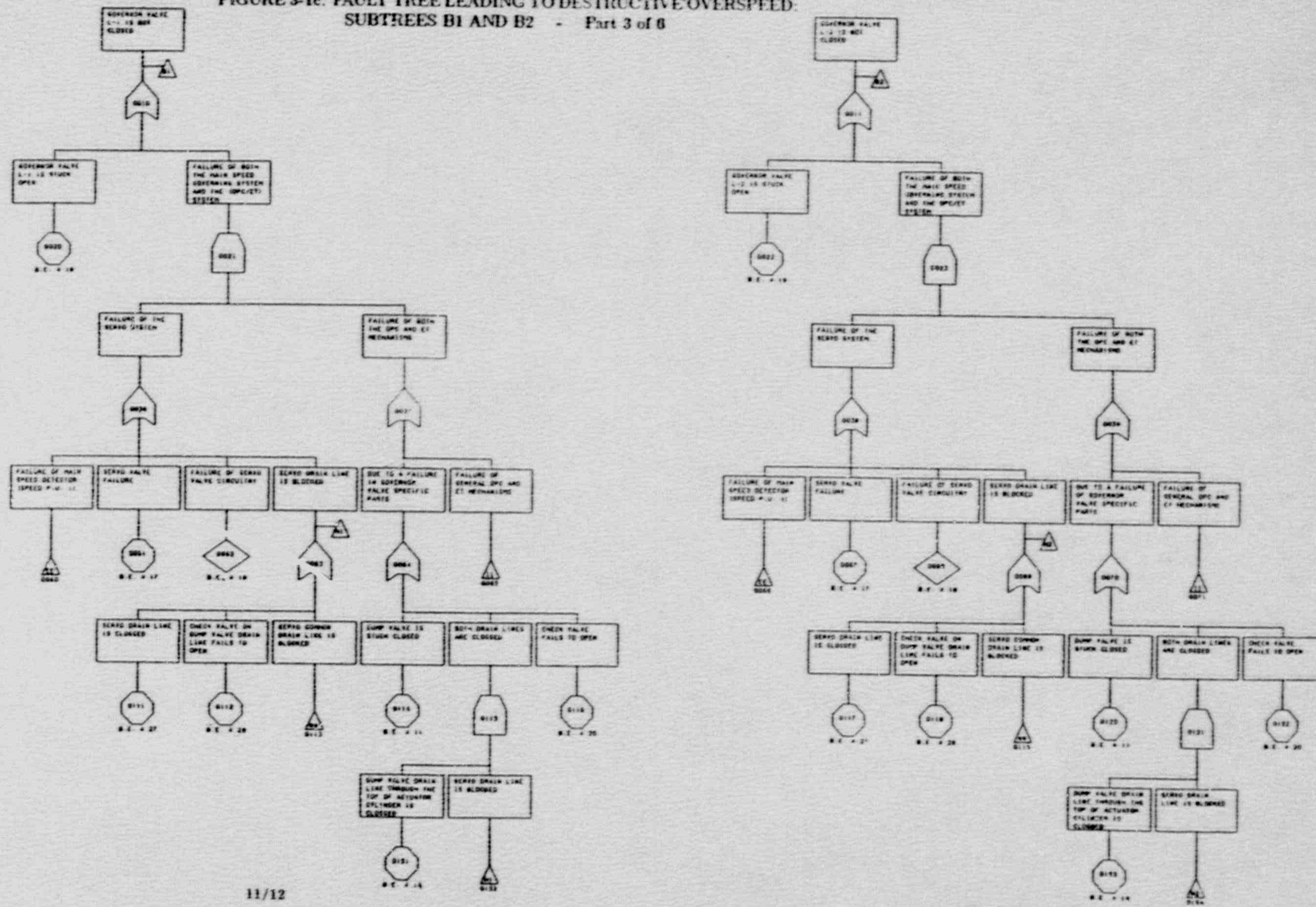


FIGURE 3-1d. FAULT TREE LEADING TO DESTRUCTIVE OVERSPEED: SUBTREES A3 AND A4 - Part 4 of 8

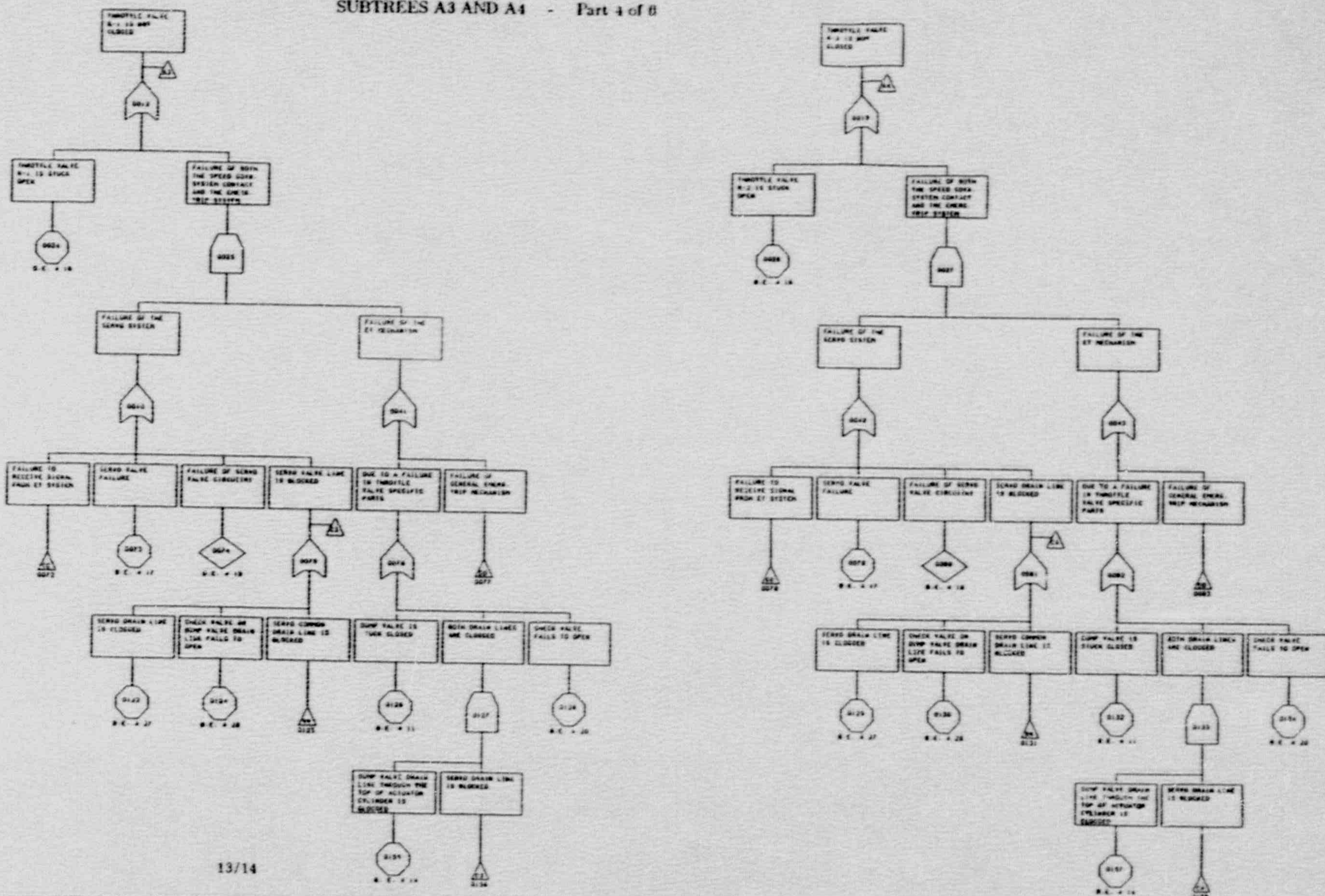


FIGURE 3-1e. FAULT TREE LEADING TO DESTRUCTIVE OVERSPEED: SUBTREES B3 AND B4 - Part 5 of 6

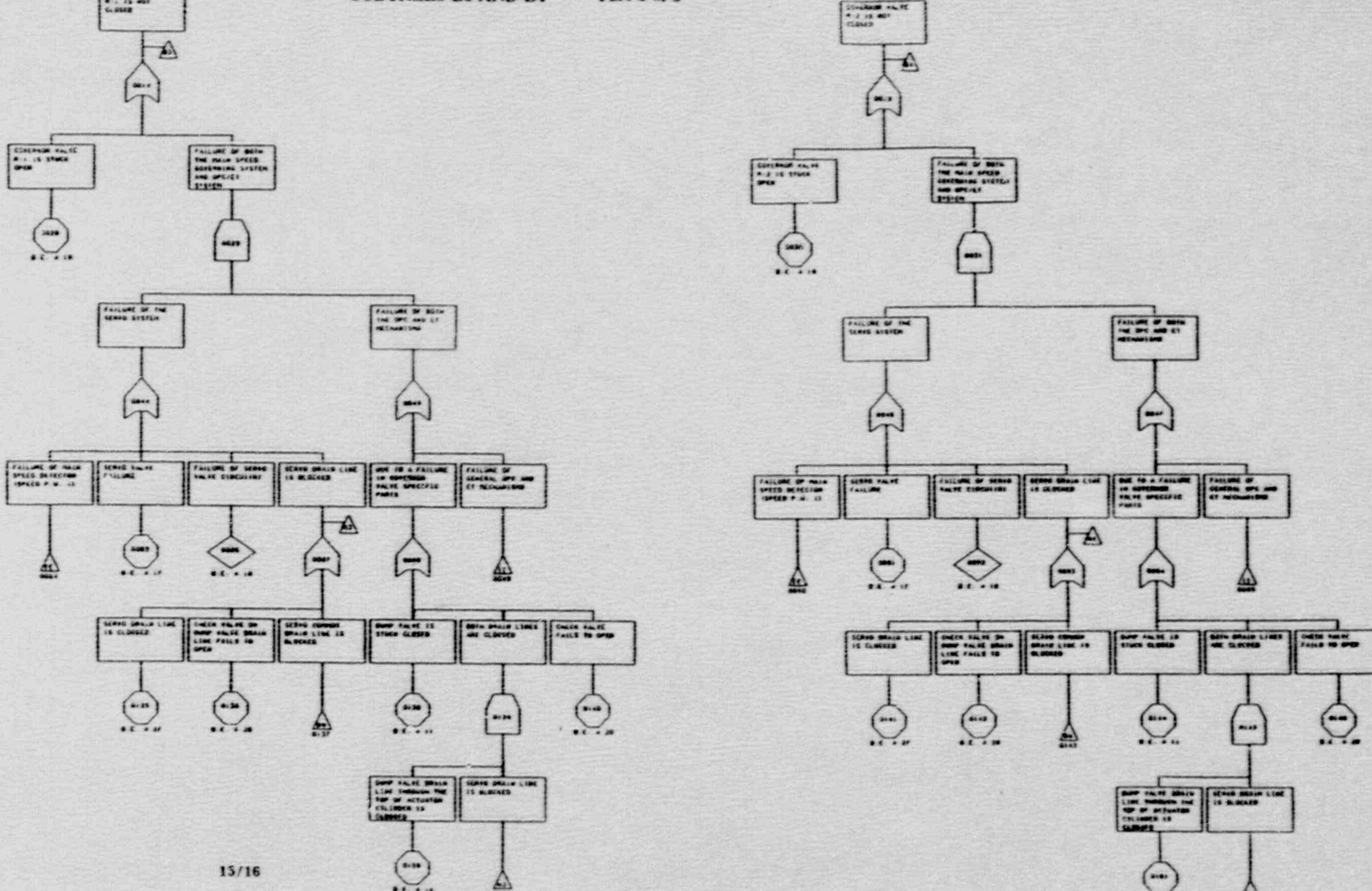
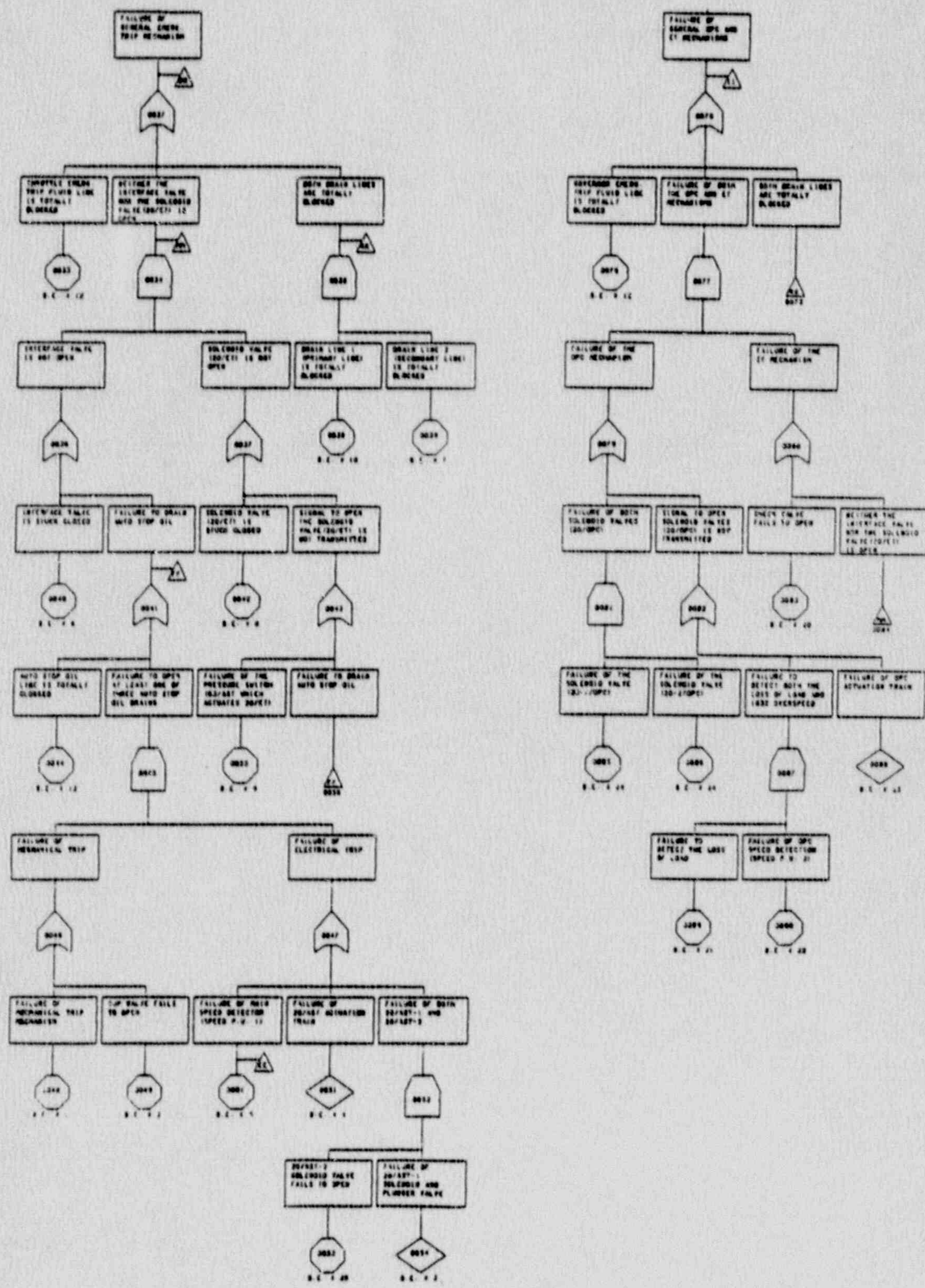


FIGURE 3-1f. FAULT TREE LEADING TO DESTRUCTIVE OVERSPEED: SUBTREES DD AND II - Part 6 of 6



a,c

FIGURE 3-2. EH FLUID SYSTEM AND LUBRICATION DIAGRAMS FOR ANALOG ELECTRO-HYDRAULIC CONTROL SYSTEM

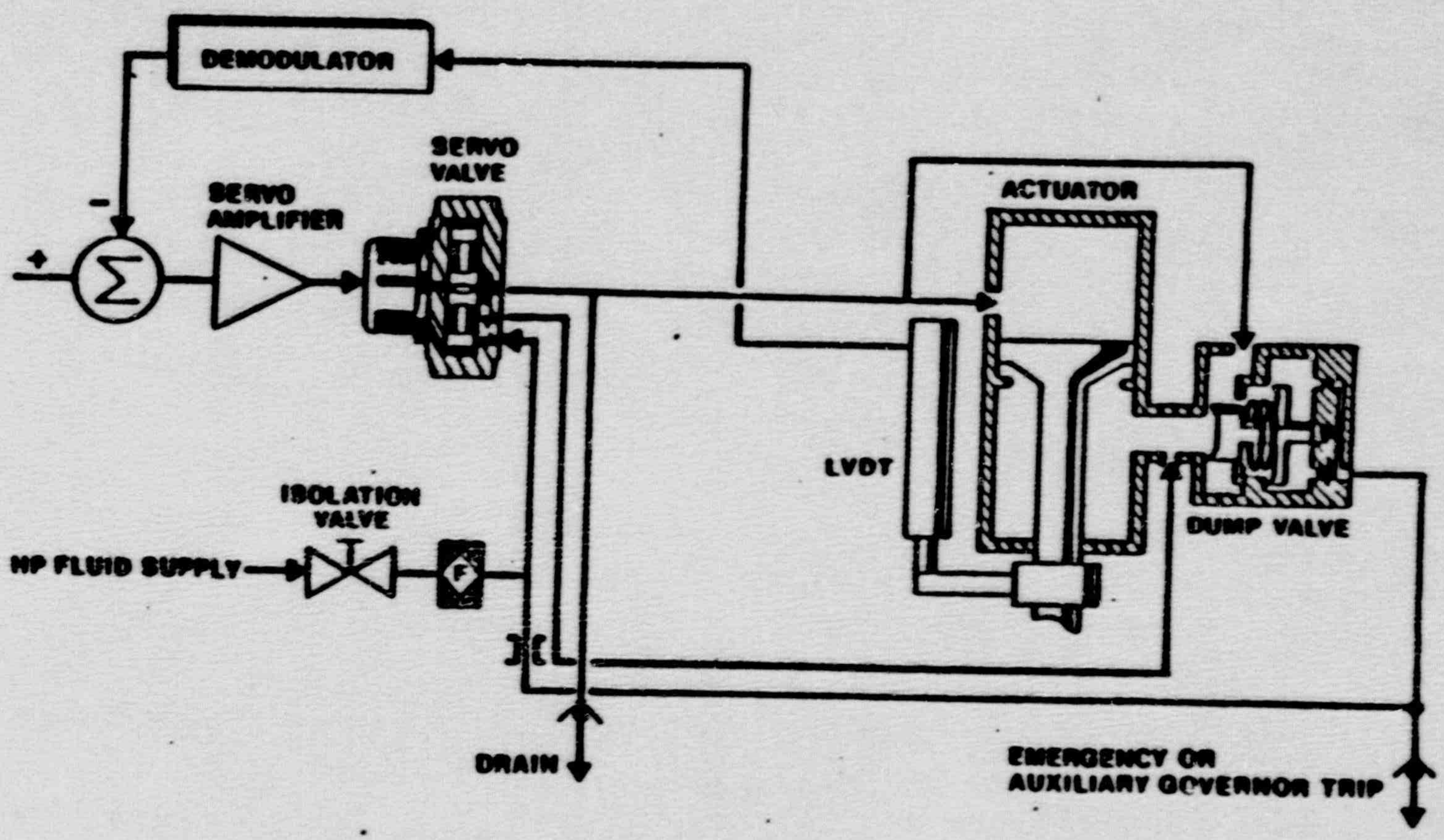


FIGURE 3-3. SCHEMATIC DIAGRAM OF THROTTLE AND GOVERNOR VALVE SERVO ACTUATOR ASSEMBLY

IV. BASIC EVENT PROBABILITIES

The fault tree that is given in detail in the previous section defines 31 basic events or elementary malfunctions. They are elementary in the sense that they do not depend on still other malfunctions (that is, the tree stops branching at the elementary malfunctions). In order to calculate the probability of the top event of the tree, it is necessary to have values for the probabilities of the basic events. The purpose of this section is to present the data on which the basic event probabilities were based and to give an account of their estimation.

The 31 basic events are identified in Table 4-1. A detailed description of these basic events and the effects of their failure can be found in [6]. The data that apply to these events are given in Table 4-2. These data are based on the Westinghouse service experience with the relevent components. For each event, Table 4-2 gives the component-years of service and the number of malfunctions for the components on which the event depends. A malfunction is defined as any failure of the component to perform a designated function when called upon to do so. As applied to the turbine steam inlet valves, a malfunction is defined as failure of the valves to close on demand. Malfunctions can be detected either during system separation (for example, a scheduled shutdown) or during regular testing (for example, monthly testing of the operation of a component while carrying load). Thus, the number of malfunctions given in Table 4-2 for a particular event is the sum of the number of tests and the number of system separations in which the component associated with the event failed to perform properly. Notice that for some events (components) two numbers are given. For these components, inadequacies in the records make the number of malfunctions uncertain; a pair of values which are believed to bracket the correct number are given in such cases. The calculation of basic event probabilities from these data takes two forms depending on the approach taken.

The basic event probability of some components (hereafter called the failure-rate type) is obtained by first estimating their failure rate, and the basic event probability of the remaining components (hereafter called the demand type) is obtained by estimating the frequency of failure to meet a demand for its services. For those basic events which are associated with demand type, the probability of the event is simply the probability of failure of the component given a demand. For the failure-rate type, however, the event that a component fails to perform on demand is visualized in terms of its having failed at some prior time and remained in this state until a demand occurs. In this case, the basic event probability is taken as the unavailability of the component. For such components, the service data are used to find a failure rate which is then used together with an assumed testing frequency to find the unavailability. The relationships among failure rate, testing frequency, unavailability, and basic event probability for this type of component are discussed in Appendix B.

The component-years of service given in Table 4-2 must be interpreted properly for each kind of component. For demand components, it is necessary to know how many demands were required to produce the number of malfunctions observed. An average of one demand per component-year was assumed for all demand components except those associated with events 1 and 2 which were assumed to have an average of 6. Similarly, for failure-rate components it is necessary to know how many years of operation were required to produce the observed number of malfunctions. Based on past experience it was taken that turbines operate about 77.9 percent of the time, that is, each component-year of service was taken to be .779 years of operation for a failure-rate component.

In carrying out the fault tree analysis it was desired to use both "best" values and conservative values for the basic event probabilities. The "best" value is represented here by the upper 50% confidence limit. This is a reasonable choice since a number of components had 0 malfunctions, that is, they would have been assigned failure rates or probabilities of failure of 0 if conventional point-estimates were used. It was decided that even in the "best"-value case, it would not be desirable to use a value that was known to be too small. The conservative value is represented by an upper 95% confidence limit on either the failure rate or the probability of failure. A description of the confidence limit calculations is given in Appendix C.

The results of the calculations based on the data in Table 4-2 are presented in Tables 4-3 and 4-4. Table 4-3 gives the upper 50% and 95% confidence limits (using both the low and high numbers of malfunctions from Table 4-2) on the basic event probabilities for events corresponding to demand-type components. For events which correspond to components of the failure-rate type, Table 4-3 refers to Table 4-4. This table reports the upper 50% and 95% confidence limits (using both the low and high numbers of malfunctions from Table 4-2) on the failure rates. These components are, as usual, identified in the table by the numbers of the events to which they correspond. Table 4-4 also presents the component unavailabilities implied by the given failure rates for various testing frequencies. These component unavailabilities are then used as basic event probabilities in the fault tree analysis.

TABLE 4-1. DESCRIPTION OF BASIC FAULT TREE EVENTS

Event Number	Event Description
1	Mechanical trip mechanism failure
2	Cup valve (auto stop oil) fails to open
3	20/AST-1 solenoid and the plunger valve failure
4	20/AST actuation train failure
5	Main speed detector (speed pick-up 1) failure
6	Interface valve fails to open
7	Secondary drain line is totally blocked
8	20/ET solenoid valve failure
9	63/AST pressure switch (actuates 20/ET) failure
10	Primary drain line is totally blocked
11	Dump valve is stuck closed
12	ET fluid line (to TV or GV) is totally blocked
13	Auto stop oil line is clogged
14	Drain line through top of actuator cylinder is clogged
15	Failure of auxiliary protection system
16	Throttle valve (TV) is stuck open
17	Servo valve failure to connect cylinder to drain
18	Servo valve circuitry failure
19	Governor valve (GV) is stuck open
20	Check valve failure
21	Failure in loss of load detection
22	OPC speed detection (speed pick-up 2) failure
23	OPC actuation train failure
24	20/OPC solenoid valve failure
25	Interceptor (IV) or reheat-stop (RSV) valve is stuck open
26	Turbine supervisory speed detector (speed pick-up 3) failure
27	Servo valve drain line is clogged
28	Check valve on dump valve drain line fails to open
29	20/AST-2 solenoid valve fails to open
30	Common servo valve drain line is clogged
31	Failure of logic card

TABLE 4-2. SERVICE EXPERIENCE FOR COMPONENTS ASSOCIATED WITH BASIC EVENTS

Type*	Event Number	Component-Years of Service	Number of Malfunctions (Low, High)
D	1	[	
D	2		
D	3		
D	4		
D	5		
D	6		
D	7		
D	8		
D	9		
D	10		
D	11		
D	12		
D	13		
FR	14		
•	15		
FR	16		
FR	17		
FR	18		
FR	19		
D	20		
D	21		
D	22		
D	23		
D	24		
•	25		
D	26		
D	27		
D	28		
D	29		
D	30		
D	31		] b,c

* D = Demand, FR = Failure Rate

TABLE 4-3. ESTIMATES OF BASIC EVENT PROBABILITIES USING UPPER CONFIDENCE LIMITS

Event Number	95 Percent Confidence Low Failures	95 Percent Confidence High Failures	50 Percent Confidence Low Failures	50 Percent Confidence High Failures
1	[			
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				
31				] a,c

Note: 8.3E-5 means .000083.

Table 4-4. ESTIMATES OF UNDERLYING FAILURE RATES AND BASIC EVENT PROBABILITIES vs TESTING FREQUENCY

		Failure Rate (Designated FR) or Basic Event Probability			
		95% Confidence		50% Confidence	
Event Number	Testing Frequency	Low	High	Low	High
14	FR	[			
	Yearly				
	Monthly				
	Weekly				
16	FR				
	Yearly				
	Monthly				
	Weekly				
17	FR				
	Yearly				
	Monthly				
	Weekly				
18	FR				
	Yearly				
	Monthly				
	Weekly				
19	FR				
	Yearly				
	Monthiy				
	Weekly				] a,c

Note: 3.9E-4 means .00039.

V. DESTRUCTIVE OVERSPEED PROBABILITY: DEPENDENCY ON VALVE TESTING FREQUENCY AND INSPECTION INTERVAL

The probability of reaching destructive overspeed (given that a loss of load incident had occurred) was estimated by analyzing the fault tree developed in section III and using the basic event probabilities obtained in section IV. Four primary cases were considered, each corresponding to the basic event probabilities given in one of the four columns of Table 4-3. These 4 cases are distinguished by two levels of upper confidence limits (upper 50% and 95% confidence limits) and by two levels for the number of component malfunctions for those components where two bounding values (the low and high number of malfunctions in Table 4-2) are given.

The fault tree for destructive overspeed was analyzed using the Westinghouse internal fault tree quantification routine [7], and the probabilities of destructive overspeed thus obtained are summarized in Table 5-1. The cases selected as representative are given by the top three probability values of Table 5-1, and they correspond to the case of 50% confidence level and high component malfunction.

The unavailability of valves (that is, the probability of their being in the "stuck open" state at a random time) depends on the frequency of valve testing. This is intuitively obvious (infrequent testing allows a failed valve to be unavailable for a longer average time than frequent testing does), and it is clear from the formula for component unavailability that has been given in Appendix B. However, these remarks are about the probability model for valve unavailability. A possible additional source of dependency on testing frequency is that the act of testing itself may alter the failure rate of a valve. A set of data giving valve malfunctions under various testing schedules was examined for evidence of an effect on failure rate in another report[8]. The statistical analysis section from that study is reproduced in Appendix D. The data gave no evidence of a dependency of failure rate on testing schedule. In this report we are assuming constant failure rate for each type of valve and treating testing frequency as having an effect only through the probability model as described above.

In this study, three different valve testing frequencies were considered, namely, weekly, monthly, and yearly testing. The probability of destructive overspeed is then given in terms of these frequencies. For example, Table 5-1 indicates that if both the throttle and governor valves are tested once every month, then the probability of destructive overspeed per loss of load incident is estimated to be 1.88×10^{-8}. As an illustration of obtaining the probability of destructive overspeed per year, suppose that there are on the average 5 load losses per year. In addition, if it is assumed that both the throttle and governor valves are tested once a month, then the probability of destructive overspeed incident per year is given by 5 times 1.88×10^{-8}, or 9.4×10^{-8}.

Given a description of the fault tree and the basic event probabilities, most fault tree analysis routines first obtain all the minimal cut sets leading to the top event and then, using the assumption that all the basic events are mutually statistically independent, calculate the probability of the top event. Two basic events of demand type or one of demand type and the other of failure-rate type are independent. However, two basic events of failure-rate type are not independent since their probabilities are expressed by their unavailabilities which are not independent. In such cases, one has to correct the top event probability obtained by the fault tree analysis routine. Specifically, if a minimal cut set leading to the top event consists of two basic events of the unavailability type and if it contributes significantly to the top event probability, the probability of such a minimal cut set is multiplied by a factor of 4/3 in order to account for the dependence (see Appendix E).

Next consider the effects of valve inspection interval on the probability of destructive overspeed. The current Westinghouse recommendation regarding the turbine valve inspection schedule is that all valves should be inspected once every 39 operating months [9]. The effect of varying inspection intervals on valve reliability can be modeled as follows: A more frequent valve inspection would lead to a longer valve life, which will be reflected by a decrease in valve failure rate; and a less frequent valve inspection would mean an increase in valve failure rate. Although we were able to determine qualitatively how the valve life might be affected by the valve inspection interval, it was not possible at the present time to quantify the effects of valve inspection interval on valve reliability. As a result, the study was limited to that of a sensitivity study.

The following two questions were considered: (1) If both the throttle and governor valves were inspected more frequently than the current schedule and it is assumed that this reduced the valve failure rates by 20%, what would be the effect on the probability of destructive overspeed? (2) On the contrary, if the valves were inspected less frequently and it is assumed that this increased the valve failure rates by 20%, what would be the effect? Table 5-2 gives results of this study. The results show that the 20% change in valve failure rate leads to about 18% change in destructive overspeed probability for weekly valve testing frequency, and the same 20% change leads to about 29% and 36% changes respectively for monthly and yearly valve testing frequencies.

Table 5-3 indicates the major contributors to the probability of destructive overspeed, by specifying the basic events of the minimal cut sets with the greatest contribution to the overall probability. Also given in the table are the percentages of contribution to the overall probability. The three most critical components as judged by their contribution to the probability of destructive overspeed are the governor valves, the throttle valves, and the auto stop oil line, in that order.

TABLE 5-1. PROBABILITY OF DESTRUCTIVE OVERSPEED
(Given A Loss-of-Load Incident)

Case Description			Probability
Confidence Level	Component Malfunction	Valve Testing Frequency	
50%	High	Weekly	3.12×10^{-9}
		Monthly	1.88×10^{-8}
		Yearly	1.56×10^{-6}
50%	Low	Weekly	1.53×10^{-9}
		Monthly	5.54×10^{-9}
		Yearly	3.12×10^{-7}
95%	High	Weekly	2.84×10^{-8}
		Monthly	7.81×10^{-8}
		Yearly	3.01×10^{-6}
95%	Low	Weekly	2.08×10^{-8}
		Monthly	4.11×10^{-8}
		Yearly	8.90×10^{-7}

TABLE 5-2. PROBABILITY OF DESTRUCTIVE OVERSPEED: A SENSITIVITY TO VALVE INSPECTION INTERVAL
(A Parametric Study At 50% Confidence Level And For High Component Malfunctions)

Case Description	Probability
Weekly Valve Testing Frequency	3.12×10^{-9}
Valve failure rates decreased by 20%	2.60×10^{-9}
Valve failure rates increased by 20%	3.70×10^{-9}
Monthly Valve Testing Frequency	1.88×10^{-8}
Valve failure rates decreased by 20%	1.37×10^{-8}
Valve failure rates increased by 20%	2.46×10^{-8}
Yearly Valve Testing Frequency	1.56×10^{-6}
Valve failure rates decreased by 20%	1.04×10^{-6}
Valve failure rates increased by 20%	2.17×10^{-6}

TABLE 5-3. MAJOR CONTRIBUTORS TO THE PROBABILITY OF DESTRUCTIVE OVERSPEED

(At 50% Confidence Level And For High Component Malfunctions)

Case Description	Basic Events in Min Cut Set	% Contribution to Overall Probability
Weekly Valve Testing	[	50%
		17%
Monthly Valve Testing		54%
		36%
Yearly Valve Testing		95%
	] a,c	5%

Note: Basic Event No. [ ] a,c

VI. DISCUSSION, CONCLUSIONS, AND SUMMARY TABLE

The problem of assessing the risk associated with turbine missile generation is generally broken down into three distinct parts with certain customary designations used for the probabilities associated with each part:

P_1: The missile generation probability, which is the probability of turbine failure resulting in the ejection of missiles through the turbine casing;

P_2: The strike probability, which is the probability of a missile perforating intervening barriers and striking a safety-related system;

P_3: The damage probability, which is the probability that the system will be rendered unavailable to perform its safety function.

This report addresses the portion of P_1 resulting from the destructive overspeed condition, that is, the probability of reaching destructive overspeed given a system separation during normal operation with the conservative assumption that a turbine missile is generated with certainty under destructive overspeed condition. This section contains a summary in Table 6-1 of the results obtained in Section V and remarks regarding the nature of the results. As was done in the earlier report [4], the probability values corresponding to 50% confidence level and high component malfunction are selected as representative. These values are reported in Table 6-1, although other cases are also reported in Table 5-1 for comparison.

The turbine operating data used to estimate the basic event probabilities came exclusively from experience with Westinghouse turbines. For some of the components, only the nuclear unit operating experience was used to estimate the component reliability, while for others both the nuclear and fossil operating experiences were combined whenever it was determined that there were enough similarities between the components of nuclear and fossil units. As mentioned earlier, the results are applicable only to Westinghouse turbines with "mechanical trip system" and either AEH, DEH (MOD 1), or DEH (MOD 2) control system and with the BB 296 steam chest configuration.

The numerical values of destructive overspeed probabilities presented in this report were obtained for the AEH control system. However, the DEH (MOD 1) and DEH (MOD 2) systems are very similar to the AEH system analyzed, with a minor difference being in the overspeed detection function. The DEH systems have another speed detection channel in addition to the two speed channels in AEH control system. The three speed signals are continually compared using a 2-out-of-3 check logic in the DEH control systems, while no such comparison is made in AEH control system. Hence, theoretically the destructive overspeed probability of the DEH (MOD 1) and DEH (MOD 2) systems should be smaller than that of the AEH system. However, the main contributors to destructive overspeed probability (that is, the minimal cut sets with a significant contribution to the top event probability of destructive overspeed fault tree) did not involve the basic events associated with overspeed detection, and as a result improving the reliability of overspeed detection in itself would not affect the overall destructive overspeed probability very much. Thus, the numerical results we obtained here for the AEH control system are also applicable to the DEH (MOD 1) and DEH (MOD 2) control systems.

The potential user of the results reported here is again reminded of two important characteristics of the probability values given: (1) The probability is a conditional probability in the sense that it gives the probability of a turbine unit reaching destructive overspeed given a system separation during normal operation. If one is interested in obtaining the probability of destructive overspeed per unit per year of operation, then the probability values of Table 6-1 should be multiplied by the average number of system separations per year. (2) The probability estimates given are upper bounds rather than best point estimates. The 50% upper confidence limit used for a component failure probability or failure rate estimation in itself does not lead to a conservative value. However, the high value was used for the number of component malfunctions, which is an upper bound on the number of malfunctions. The number of service years given in Table 4-2 and the number of demands used, i.e., 6 per year for basic events 1 and 2, and 1 per year for the other basic events, are conservative.

This section is concluded with a brief discussion of the differences between the current study and the earlier study [1,4]. First, the turbine operating experience data has been updated. The earlier study was based on the turbine operating experience through the year 1972, and the current study is based on the turbine operating experience through the end of 1981. During those nine years from 1973 through 1981, a great deal of nuclear unit operating experience as well as electro-hydraulic (EH) system operating experience has been accumulated. Secondly, all the basic events of the fault tree were treated as being of the demand type in our earlier study, and it was not possible to study the effects of valve testing frequency on the probability of destructive overspeed. The current study, however, treats the valves as well as a few other components as being of the failure-rate type and thus we were able to examine the effects of valve testing frequency on the probability of destructive overspeed.

In conclusion, the current study indicates that the throttle and governor valves are the two most critical components followed by the auto stop oil line. This result seems to contradict the earlier finding, in which other components were found to be most critical. This apparent discrepancy results from the two factors: (1) the operating experience of the additional nine years amounts to a large portion of the overall EH system experience and (2) both the nuclear and fossil experiences were used for the valves and many other components, and the additional nine years did not add very much to the overall operating experience of these components; however, for those few components for which only the EH system operating experience was used, the additional nine years amounted to be the major portion of the overall operating experience of these components.

TABLE 6-1. PROBABILITY OF DESTRUCTIVE OVERSPEED AND MAJOR CONTRIBUTORS TO DESTRUCTIVE OVERSPEED PROBABILITY

(At 50% Confidence Level And For High Component Malfunctions)

Valve Testing Frequency	Probability	Major Contributors Basic Events in Min Cut Set	% Contribution to Overall Probability
Weekly	3.12×10^{-9}		
			50%
			17%
Monthly	1.88×10^{-8}		
			54%
			36%
Yearly	1.56×10^{-6}		
			95%
			5% a,c

Note: Basic Event No. a,c

VII. APPENDICES

A: Fault Tree Diagram Symbols

B: Determining Basic Event Probabilities for Components of Failure-Rate Type

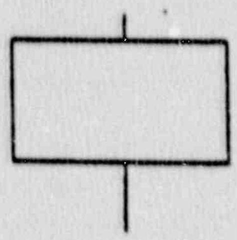
C: Confidence Limits for Failure Rates and Probabilities of Failure

D: Statistical Evaluation of Valve Testing Interval and Valve Failure

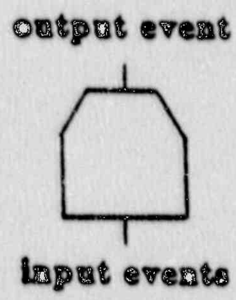
E: Correction of Fault Tree Results for Dependent Basic Events

Appendix A: Fault-Tree Diagram Symbols

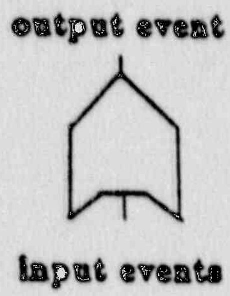
A fault-tree is a convenient and pratical tool for evaluating the reliability characteristics of a system. It is a graphical representation in which all combinations of fault events or conditions that can lead to a system failure are organized deductively and systematically. The fault-tree technique can be used to depict and evaluate the reliability or availability of a system or the probability of an event which is the consequence of the occurrence of other events. A fault-tree begins with an identification of the "top event", an undesirable event, which in our case is the destructive overspeed (given that a loss-of-load incident has occurred). Then one identifies all possible combinations of events that would lead to the occurrence of the top event, and the combinations of events are expressed graphically in the form of a tree. Good documentation on fault-tree methodology can be found in [10]. A brief description of the fault-tree symbols used in this report is presented below:



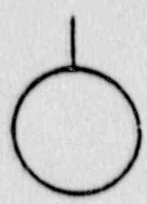
RECTANGLE



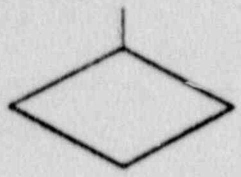
AND GATE



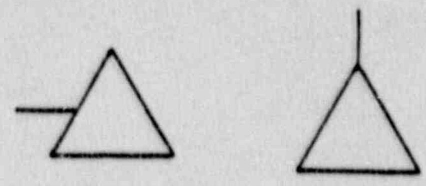
OR GATE



CIRCLE



DIAMOND



Transfer-out Transfer-in

TRANSFER

RECTANGLE: identifies an event, usually a malfunction or an undesirable event.

AND GATE: describes the logical situation whereby the output is realized if all the input events occur.

OR GATE: describes the logical situation whereby the output is realized if one of the input events occur.

CIRCLE: designates a basic fault event that requires no further development and whose probability can be quantified.

DIAMOND: designates a fault event that is considered to be basic in a given fault-tree but for which the causes have not been fully developed.

TRANSFER: the triangle is used as a transfer symbol to connect identical portions of the fault-tree.

Appendix B: Determining Basic Event Probabilities for Components of Failure-Rate Type

Consider a component (a valve, for example) with an exponential failure-time distribution. That is, if the component is put into operation and T is the time to failure, then T is distributed with probability density given by

$$f(t) = \lambda e^{-\lambda t} \tag{1}$$

and distribution function given by

$$F(1) = 1 - e^{-\lambda t} \tag{2}$$

This well known and often used assumption has a number of implications. Basically, it corresponds to the component failing purely at random. A good description of this distribution and its use in reliability contexts is available in Chapter 3 of [11]. For present purposes, we need to know that λ is the *failure rate* for the component. (In this report, failure rates are in failures per year).

As a simple example to help fix ideas, suppose $\lambda = .01$ for some component. The probability that such a component would fail in a given year is found from equation (2) by letting t have the value 1. By definition, $F(1)$ is the probability that the time to failure for the component will not exceed 1 year. Thus the desired probability is $1 - e^{-.01}$. Using the well known approximation that $e^{-x} = 1 - x$ for small x, the probability is very nearly .01, that is, a component with a failure rate of .01 (per year) has a probability of failing in any one year of about .01.

In the present context, the probabilities of interest are the *basic event* probabilities. The connection between *basic events* and *component failure* is that if a demand (that is, a system separation) occurs when a *component* is in the failed state then the *basic event* associated with that component is defined to have occurred. The connection between the *probability* of a basic event and component failure is this: the probability that a demand at some future random time will coincide with a component's being in a failed state is simply the long run proportion of the time that the component is in such a state. This proportion is known as the *unavailability* of the component. In other words, evaluating component unavailabilities yields basic event probabilities directly.

Recall that the components being discussed in this appendix (failure-rate components) are assumed to be tested regularly. Their unavailability depends on their failure rate and frequency of testing. To see that testing frequency is a factor, notice that infrequent testing implies that failed components will not be discovered and repaired for a relatively long time. A well known result in reliability theory is that the long run unavailability of a component is given by the expected value of the time it spends in the failed state expressed as a proportion of the total time the system is in operation. The essential task then is to evaluate the expected "downtime" for a component given its failure rate and testing frequency.

Consider the previous example again briefly. The component had a failure rate of .01 and was tested yearly. To find its expected downtime we will make use of the following fact: given that a failure has occurred in a particular year, the distribution of its time of occurrence within the year is uniform. Thus the expected time of failure within a year in which a failure is known to have occurred, is mid-year. The conditional expected downtime during such a year then, is 0.5 years. The unconditional expected downtime (that is, the expected value for any year) is the product of this and the probability of failure in any year. Previously this probability was seen to be .01. Therefore the expected value we seek is .005. Moreover this is also the unavailability since it is the expected years of downtime in a year of operation and the divisor is therefore unity. Hence, the component is unavailable (on the average) 5 years out of a thousand, and the probability that it will be down at a random time in the future is .005. In words, the unavailability of a component is the product of the probability of its failing in the time interval between tests and 0.5 (the ratio of the half-length to the full length of the testing interval). That is,

$$\text{unavailability} = 0.5\lambda t,$$

where

λ is the failure rate in failures per year,

and

t is the testing interval in years.

This result involves several approximations. One, mentioned above, is that e^{-x} is approximately equal to $1 - x$ for small x. Considering the very small values of λ that occur in this work, the use of this approximation is entirely justified. The other approximation was used in the above derivation of the expected downtime given that a failure has occured. There are two approaches to the exact result.

First, one can use the exponential density given in equation (1). If T is the time of failure and the interval is 1 year, we need the conditional expectation of $1 - T$ given that $T \leq 1$. This is the ratio of two integrals involving the density in (1) and it evaluates to

$$\frac{1}{1-e^{-\lambda}} - \frac{1}{\lambda}.$$

This can be approximated very closely by $\frac{1}{2}$ using the fact that $1 - e^{-\lambda}$ is very nearly $\lambda - \lambda^2/2$ and λ is very small.

The other approach uses the fact that the exponential failure times can be thought of as the times between randomly arriving failure events, i.e., a Poisson process. It is this picture that leads to the result mentioned earlier that conditional on a failure arriving in an interval, its location within the interval is uniformly distributed. The approximation enters here because to get the exact expected downtime by this route it is necessary to condition not only on 1 failure but also on 2, 3, 4, and so on. When the interval has two arrivals, for example, it is the first one that represents component failure and its average location in the (1 year) interval is at the one-third point not the one-half point. In this approach, the exact expected downtime is the probability of exactly one failure times the implied average downtime, 1/2, plus the probability of exactly two failures times the implied average downtime, 2/3, plus, and so on. The approximation in this approach consists of ignoring the extra "failures" because their probability of occurrence is very small.

A good reference for the uniform distribution results used above is Chapter 3 of [1?]. For availability (and hence unavailability) see Chapter 7 of [12].

Appendix C: Confidence Limits for Failure Rates and Probabilities of Failure

The basic event probabilities used in this report are based on estimated *failure rates* (per year) for some components and estimated *probabilities of failure* (per demand) for other components. The approach that was used to estimate these parameters will be described in this appendix.

The data for both types of components are presented in Table 4-2 where they are listed by basic event. For each event, Table 4-2 gives the number of component-years of exposure that were accumulated by the components associated with the event, and the number of malfunctions that were experienced by those components. Let r be the number of malfunctions and N the number of component-years of exposure (in calendar-years).

Probabilities of failure will be discussed first. They are approached by regarding each year of experience with a component as representing a certain number of performance demands (depending on the type of component) and treating the data as resulting from Bernoulli trials with probability of failure, p. Thus, for a type of component which receives m demands per year, r malfunctions in N component-years of exposure corresponds to r failures in mN Bernoulli trials; the distribution of r is binomial with parameters p and mN. The problem is to obtain 50 and 95 percent upper confidence limits on p.

This problem is classical; good discussions on confidence limits for a binomial parameter are available in many places (for example, [13], [14], [15]). Briefly, the idea is to use the data from a given type of component to find the largest value of p that is consistent with that data. The essential problems in implementing this idea involve giving meaning to the concept "consistent". It is not the purpose of this appendix to derive statistical results from first principles, but a certain amount of explanation is probably worthwhile.

Consider an example. If there were 1 failure in 10 demands then clearly 0.1 would be a consistent value for p. Just as clearly, there is nothing very unreasonable about the value $p = 0.15$. The question is, "for increasing p, at what point does the value become unreasonable?". The answer is taken to be--that value of p for which the probability of one or fewer failures (the present result or a more extreme one) is on the threshold of being too small. The threshold is set by the choice of the confidence coefficient. A choice of 0.95, for example, means that the threshold was set at .05;

a choice of 0.50 means that it was set at 0.50. The first of these produces a larger value of p as being consistent with a given set of data than the second one does. For future use, let $p(c)$ be the upper 100c %confidence limit for p. We are interested in $p(0.50)$ and $p(0.95)$.

The references cited above show that to calculate $p(c)$ given r (number of malfunctions) and mN (number of demands) one must find the value of p (probability of malfunction) for which the probability of r or fewer malfunctions equals $1 - c$, and set $p(c)$ equal to that value. In the case where $r = 0$, the result is given by a simple formula:

$$p(c) = 1 - (1 - c)^{\frac{1}{mN}}. \tag{1}$$

For $r > 0$, the simplest approach is to use the tabled values of a statistical distribution known as the F-distribution. This family of distributions is indexed by two parameters, D_1 and D_2, known as degrees-of-freedom. Given r and mN, the particular distribution that applies to $p(c)$ is given by the relations,

$$D_1 = 2(r + 1), \quad \text{and}$$

$$D_2 = 2(mN - r).$$

To complete the calculation it is necessary to find that value which is at the 100c percent point of the distribution. Let $F(c; D_1, D_2)$ represent this value. Then, for $r > 0$,

$$p(c) = \frac{(r + 1)F(c; D_1, D_2)}{(mN - r) + (r + 1)F(c; D_1, D_2)}. \tag{2}$$

Formulas (1) and (2) were used to compute the upper 50 and 95 percent confidence limits on p for those component types that are characterized by a probability of failure per demand.

For the other types of component involved in this report, it is necessary to estimate failure rates. This stems from the assumption of an exponential time-to-failure distribution for these components. The single parameter in this family of distributions will be denoted by λ in this appendix. As above, the estimates will be in the form of upper 50 and 95 percent confidence limits. The observational material remains the same as it was for the other components, namely, r malfunctions in N component years of exposure. Now, however, each component is viewed as being exposed to failure during the time it is in service. Since the raw data is in calendar-years of exposure, it is necessary to correct for the fact that components are not in constant operation. This is handled by multiplying N by the proportion of the time that the turbines operate. Let the reduced exposure be represented by $N' = kN$. In the calculations for the report, k was taken as 77.9 percent.

The theory for confidence limits on λ is more involved than that for p because there are a number of practical distinctions in how the data are collected. A good discussion of these matters is given in Chapter 3 of [11]. The present case falls into the category known as type II censoring with replacement, that is, there are a number of samples of a given component on "test", when there is a failure the unit is repaired or replaced, and the "test" is terminated after a certain amount of exposure. The theory in this case appeals to the relationship between an exponential failure-time distribution and the Poisson arrival process for failure occurrences. The data consist of the number of malfunctions (r) in a fixed amount of exposure (N'), and r has a Poisson distribution with parameter $N'\lambda$. The problem is thus transformed into finding upper 50 and 95 percent confidence limits on a Poisson parameter. Let $\lambda(c)$ be the upper $100c\%$ confidence limit on λ. We want $\lambda(0.50)$ and $\lambda(0.95)$.

This problem is just like the corresponding problem for the binomial parameter p that was discussed above. It is discussed not only in [11] in the present context but also in [13] in a general setting. These references show that to find $N'\lambda(c)$ given r and N', one must find that value of the Poisson parameter for which the probability of r or fewer malfunctions equals $1-c$, and set $N'\lambda(c)$ equal to that value. One may then solve for $\lambda(c)$ of course. Just as before, when $r=0$ a simple formula can be given. It is

$$\lambda(c) = -\frac{\ln(1-c)}{N'}. \tag{3}$$

When $r > 0$, it is simplest to use the fact that the Chi-square distribution gives the sum of Poisson probabilities (just as before it was the F-distribution giving the sum of binomial probabilities). Let $\chi^2(c; D_1)$ be the $100c$ percent point of the Chi-square distribution with D_1 degrees-of-freedom. For r malfunctions, the particular Chi-square distribution that applies to $\lambda(c)$ is given by

$$D_1 = 2(r+1).$$

The formula is

$$\lambda(c) = \frac{\chi^2(c; D_1)}{2N'}. \tag{4}$$

Appendix D: Statistical Evaluation of Valve Testing Intervals and Valve Failure

The throttle and governor valve operating data on nuclear units can be summarized as follows:

Testing schedule	Exposure (valve-hours)	Failures
Weekly	[	
Monthly		
Every 2 weeks		
Not regular		] b,c

These data invite the computation of failure rates (number of failures per valve-hour) for each testing schedule followed by appropriate comparison. The question of whether the calculated rates are sufficiently different to constitute evidence of real differences among schedules naturally arises. The purpose of this appendix is to discuss this question and related issues.

The working assumption for this discussion is that within any testing schedule, failures occur randomly over time at a constant rate which is characteristic of the particular schedule. This is a very natural assumption that is used frequently in dealing with data involving the occurrence of a more or less rare event over time. Based on this assumption, the number of failures in exposure-time t while using a given testing schedule has a Poisson distribution with parameter $\mu = \lambda t$. The quantity λ is the failure rate mentioned above and supposed constant within any testing schedule. Using the weekly schedule as an example, there is 1 failure in about [10^6] valve-hours. Denoting parameter estimates as $\hat{\mu}$ and $\hat{\lambda}$ we have

$\hat{\mu} = 1$

$\hat{\lambda} =$ [ ] b,c failures per valve-hour.

Once an estimate for λ, i.e., $\hat{\lambda}$, is available, one can estimate the parameter of the Poisson distribution that would govern the number of failures under a weekly testing schecule for any number of valve-hours of exposure. For example, the number of failures in [3×10^6] valve-hours would be estimated to have a Poisson distribution with parameter

a,c

$\hat{\mu} = \hat{\lambda}$[ ] a,c

Notice that the monthly schedule had an exposure of about [ ] b,c valve-hours and only 1 failure was observed. Does this mean that the monthly schedule involves a lower failure rate than the weekly, or does the variability inherent in the Poisson distribution readily explain this much discrepancy? This exemplifies the kind of question to be dealt with in the remainder of this appendix.

One way to summarize the information about the underlying failure rate (λ) contained in a given set of data is to compute a confidence interval for this unknown parameter. Using classical method one can state that if 1 failure has been observed then a 95% confidence interval for the Poisson parameter μ is

$$.025 \leq \mu \leq 5.57.$$

Since $\mu = \lambda t$ this means that

$$\frac{.025}{t} \leq \lambda \leq \frac{5.57}{t}$$

with 95% confidence. For the weekly data then, since $t =$ [ ] b,c we find

[ ] a,c (weekly)

while for the monthly data ($t =$ [ ] b,c we find

[ ] a,c (monthly).

These intervals convey what is known about the values of λ under the two schedules in a way that reveals the uncertainty involved. Each interval gives the values of λ that are reasonably consistent with the corresponding set of data. The chosen confidence coefficient of 95% sets the standard for what is to be regarded as "reasonable". For given data, increasing the coefficient merely enlarges the the interval. A value of 95% is more or less standard.

The confidence intervals for the failure rates under weekly and monthly testing have a considerable overlap. This says that the difference between the observed rates [ ] failures per million valve-hours for weekly and monthly testing, respectively) could easily arise from chance alone in the absence of any real difference. While the two confidence intervals are of interest in themselves as a summary of what the data say about the individual failure rates, a more direct approach for the comparison of the two failure rates is available. Under the Poisson assumption, it is possible to calculate a confidence interval for their ratio. The ratio of the weekly to the monthly failure rate may be estimated from the data to be $\hat{\rho} =$ [ ] a,c and the 95% confidence interval is b,c

[ ] a,c (weekly/monthly).

For the failure rates to be judged different on the present data, this interval would have to exclude 1. This shows once again that even though the observed rates are
a,c | different[ ]such a result is quite consistent with the true rates being equal ($\rho = 1$). Of course, the confidence interval is quite broad. This means that the amount of data is not sufficient to give a very precise comparison of the two rates. Ironically, the precision would improve if there were more failures. On the other hand, a greater exposure would not help the precision of the comparison. Greater exposure would, however, help the precision of the estimates of the individual rates. This points up the importance of considering the magnitude of the individual rates as well as their comparison. If they are both quite small, it is not possible to make a precise comparison; corespondingly, in such a case it probably does not matter which rate is larger.

The data for the other testing schedules do not add much to the above analysis. The every-other-week schedule is based on only one unit and hence does not have a sufficiently broad base to be analyzed by itself while the non-regular testing regimen suffers from the data-paucity syndrome mentioned above (i.e., 0 failures). For completeness the first three data sets are combined into one which represents the practice of regular testing and compare with the remaining set which represents the absence of a regular testing schedule. The data may then be represented as

Regular Testing	Exposure (valve-hours)	Failures
Yes	[	
No		] b,c

The 95% confidence inter[illegible]or the individual falure rates are:

[ ] (regular) a,c

[ ] (not-regular). a,c

Again there is considerable overlap between these intervals, and therefore the data fail to reject the proposition that the two testing regimens have the same underlying failure rates. The 95% confidence interval for the ratio of the two failure rates is

[ ](regular/not-regular) a,c

with an estimated value of $\hat{\rho} = 1.12$. The interval does not exclude 1 and therefore provides no basis for concluding that the underlying rates are different.

The overall failure rate estimate based on all the data (that is, assuming there is no dependence of failure rate on testing regimen) is $\hat{\lambda} =$[ ]failures b,c per million valve-hours. The 95% confidence interval for this overall λ is

a,c

[ ] (overall).

Based on this analysis we conclude that these data give no evidence of a dependence of failure rate on tesing regimen. Moreover, under the assumption of a single failure rate these data would put that rate at between [ ] failures per million valve-hours.

a,c

Appendix E: Correction of Fault Tree Results for Dependent Basic Events

The top event probabilities given in Table 5-1 were calculated by a fault-tree analysis program. In doing these calculations, whenever it is necessary to find the probability of an event which is represented in the tree as two events joined by an "and gate", the program uses the simple product rule from probability calculus; that is, the program treats the two events as (probabilistically) independent. This is not necessarily correct even though one is willing to assume that components fail independently. The difficulty is that basic-event probabilities and probabilities of component failure are the same only for what we have called demand components. For failure-rate components, as has been pointed out elsewhere in this report, basic event probabilities are component unavailabilities. It is simply not true that the joint unavailability of components which fail independently is given by the product of their separate unavailabilities. In this appendix we indicate the correct approach and describe the correction that was applied to the results of the fault tree analysis program.

In the case of two components with failure rates λ_1 and λ_2 and a common test interval t, their separate unavailabilities (as was seen in Appendix B) are $\lambda_1 t/2$ and $\lambda_2 t/2$ respectively. To get at their joint unavailability we return to the definition, i.e., the average fraction of t during which both are in the failed state. This, of course, is quite analogous to the situation in Appendix B where a formula for the unavailability of a single component was developed. We begin by finding the expected joint downtime in a time interval of length t given that both components have in fact failed during the interval. As was stated in Appendix B, given that a component has failed in a specified interval, the distribution of its time of failure within that interval is uniform. Since the two components being discussed here are assumed to fail independently, their two times of failure are independently, uniformly distributed within the specified interval. Now, the components are jointly down for the amount of time during which the second one to fail is down. To know the expected value of this quantity we need to know the expected value of the largest of two independent uniform observations. This well known result is $2t/3$, that is, on the average the second failure will occur at the point which is one-third of the length of the interval from its end. The joint unavailability of the two components in intervals of length t where they both fail is thus given by 1/3 (the time during which both are down, divided by the length of the interval). To get the joint unavailability in general (that is, not conditional on the two components failing in a specified interval) we must multiply the conditional value by the probability of the condition.

The probability of the condition is the probability of both components failing in the interval. Since they fail independently with exponentially distributed failure times, the result is the product of $1 - \exp(-\lambda_1 t)$ and $1 - \exp(-\lambda_2 t)$ or $\lambda_1 t \lambda_2 t$ using the usual approximation. Finally then, the correct joint unavailability is the product of this probability and the above factor of 1/3, that is,

$$\frac{1}{3}\lambda_1 t \lambda_2 t.$$

Meanwhile, for reasons explained above, the fault tree analysis program will use the result,

$$\frac{1}{2}\lambda_1 t \frac{1}{2}\lambda_2 t.$$

To correct for this, we have hand-adjusted the affected results from the program by the factor 4/3.

VIII. REFERENCES

b,c

[1] [

[2] [

[3] [ ]

[4] Westinghouse STDE, "Analysis of the Probability of the Generation and Strike of Missiles from a Nuclear Turbine", March 1974.

b,c

[5] [

[6] [

[7] [

[8] [ ]

[9] Westinghouse STG, "Valve Inspection for Fossil and Nuclear Units", Steam Turbine Information Manual, Section 13 CT-24038, October 1983.

[10] USNRC, Fault Tree Handbook, NUREG-0492, March 1980.

[11] Bain, Lee J., Statistical Analysis of Reliability and Life Testing Models–Theory and Methods, New York: Marcel Dekker, 1978.

[12] Barlow, Richard, E., and Proschan, Frank, Statistical Theory of Reliability and Life Testing–Probability Models, New York: Holt, Rinehart, and Winston, 1975.

[13] Brownlee, K. A., Statistical Theory and Methodology In Science and Engineering, 2nd ed. New York: John Wiley and Sons, 1965.

[14] Mood, Alexander M. and Graybill, Franklin A., Introduction to the Theory of Statistics, 2nd ed. New York: McGraw-Hill, 1963.

[15] Kempthorne, Oscar and Folks, Leroy, Probability, Statistics and Data Analysis, Ames, Iowa: The Iowa State Univ. Press, 1971.