

EEG-59



**AN ANALYSIS OF THE ANNUAL PROBABILITY  
OF FAILURE OF THE WASTE HOIST BRAKE  
SYSTEM AT THE WASTE ISOLATION PILOT PLANT  
(WIPP)**

Moses A. Greenfield and  
Thomas J. Sargent

Environmental Evaluation Group  
New Mexico

November 1995

AN ANALYSIS OF THE ANNUAL PROBABILITY OF FAILURE  
OF THE WASTE HOIST BRAKE SYSTEM AT THE  
WASTE ISOLATION PILOT PLANT (WIPP)

Moses A. Greenfield, Ph.D.  
Consultant to Environmental Evaluation Group  
Professor Emeritus, University of California, Los Angeles

Thomas J. Sargent, Ph.D.  
Professor, University of Chicago  
and  
Hoover Institution, Stanford University

Environmental Evaluation Group  
7007 Wyoming Blvd., NE, Suite F-2  
Albuquerque, New Mexico 87109

and

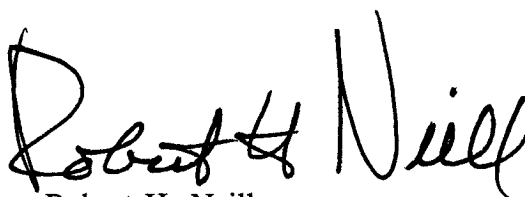
505 North Main Street, P.O. Box 3149  
Carlsbad, New Mexico 88221-3149

November 1995

## FOREWORD

The purpose of the New Mexico Environmental Evaluation Group (EEG) is to conduct an independent technical evaluation of the Waste Isolation Pilot Plant (WIPP) Project to ensure the protection of the public health and safety and the environment. The WIPP Project, located in southeastern New Mexico, is being constructed as a repository for the disposal of transuranic (TRU) radioactive wastes generated by the national defense programs. The EEG was established in 1978 with funds provided by the U.S. Department of Energy (DOE) to the State of New Mexico. Public Law 100-456, the National Defense Authorization Act, Fiscal Year 1989, Section 1433, assigned EEG to the New Mexico Institute of Mining and Technology and continued the original contract DE-AC04-79AL10752 through DOE contract DE-ACO4-89AL58309. The National Defense Authorization Act for Fiscal Year 1994, Public Law 103-160, continues the authorization.

EEG performs independent technical analyses of the suitability of the proposed site; the design of the repository, its planned operation, and its long-term integrity; suitability and safety of the transportation systems; suitability of the Waste Acceptance Criteria and the generator sites' compliance with them; and related subjects. These analyses include assessments of reports issued by the DOE and its contractors, other federal agencies and organizations, as they relate to the potential health, safety and environmental impacts from WIPP. Another important function of EEG is the independent environmental monitoring of background radioactivity in air, water, and soil, both on-site and off-site.

A handwritten signature in black ink, reading "Robert H. Neill". The signature is written in a cursive style with a large initial "R" and "N".

Robert H. Neill

Director

## **EEG STAFF**

Sally C. Ballard, B.S., Laboratory Scientist  
William T. Bartlett, Ph.D., Health Physicist  
Radene Bradley, Secretary III  
Lokesh Chaturvedi, Ph.D., Deputy Director & Engineering Geologist  
Thomas M. Clemo, Senior Scientist  
Patricia D. Fairchild, Secretary III  
Donald H. Gray, M.A., Environmental Specialist  
Jim W. Kenney, M.S., Environmental Scientist/Supervisor  
Lanny King, Assistant Environmental Technician  
Betsy J. Kraus, M.S., Technical Editor/Librarian  
William W.-L. Lee, Sc.D., P.E., D.E.E., Senior Scientist  
Robert H. Neill, M.S., Director  
Jill Shortencarier, Administrative Secretary  
Matthew K. Silva, Ph.D., Chemical Engineer  
Susan Stokum, Administrative Secretary  
Ben A. Walker, B.A., Quality Assurance Specialist  
Brenda J. West, B.A., Administrative Officer

## **ACKNOWLEDGMENTS**

The authors wish to thank Jill Shortencarier for very expert typing of a difficult manuscript. We are grateful to Betsy Kraus for careful editing which clarified the text and eliminated extraneous words. We thank our colleagues Robert Neill, Lokesh Chaturvedi, and William Lee for many helpful suggestions.

## TABLE OF CONTENTS

FOREWORD . . . . .	iii
EEG STAFF . . . . .	iv
ACKNOWLEDGMENTS . . . . .	v
SUMMARY . . . . .	x
RECOMMENDATIONS . . . . .	xiv
I. INTRODUCTION . . . . .	1
<u>Historical Review</u> . . . . .	1
<u>DOE Revised Design, 1994</u> . . . . .	3
II. DATA SOURCES . . . . .	5
III. FAILURE MODES FOR THE BRAKE SYSTEM . . . . .	6
IV. CALCULATIONS FOR REVISED DESIGN . . . . .	11
<u>DOE Calculations</u> . . . . .	11
<u>EEG Calculations</u> . . . . .	14
<u>Numerical Results of EEG Calculations</u> . . . . .	26
DISCUSSION . . . . .	30
REFERENCES . . . . .	31
LIST OF ACRONYMS . . . . .	33
APPENDIX 1 . . . . .	37
APPENDIX 2 . . . . .	41
APPENDIX 3 . . . . .	43
LIST OF EEG REPORTS . . . . .	51

## LIST OF TABLES

TABLE 1.	HISTORICAL REVIEW, WASTE HOIST BRAKE SYSTEM AT WIPP . . .	1
TABLE 2.	EVENT PROBABILITIES FOR VARIOUS FAILURE MODES (FROM PRELIMINARY DRAFT REPORT WCAP-13800, PAGE A3-4) . . . . .	7
TABLE 3.	RESULTS OF THE REVISED DESIGN ANALYSIS (FROM PRELIMINARY DRAFT REPORT WCAP-13800, PAGE 3-6) . . . . .	8
TABLE 4.	FAILURE RATES FOR COMPONENTS, REVISED DESIGN AND B-2 DESIGN . . . . .	9
TABLE 5.	CUTSETS FOR ANNUAL FAILURE RATES (WCAP-13800, PAGE A3-4) . . . . .	12
TABLE 6.	COMPARISON OF FAILURE RATES FOR COMPONENTS AS LISTED IN NPRD-91 AND NPRD-95 . . . . .	15
TABLE 7.	LISTING OF REFERENCE NUMBERS, ASSOCIATED EP NUMBERS AND MISSION TIMES . . . . .	16
TABLE 8.	COMPONENTS AND DESCRIPTORS . . . . .	20
TABLE 9.	CALCULATIONS FOR LOGNORMAL PARAMETERS, REVISED DESIGN (NPRD-95) . . . . .	22
TABLE 10.	COMMON CAUSE CALCULATIONS (NPRD-95); (WIPP-13800, SECTION A5.3.3) . . . . .	24
TABLE 11.	VALUES OF THE PARAMETERS $\mu$ , $\sigma$ FOR THE REVISED DESIGN (NPRD-95). . . . .	25
TABLE 12.	COMPARISON OF MEANS AND STANDARD ERRORS (NPRD-95) . . .	26
TABLE 13.	PERCENTILES AND PROBABILITY VALUES OF THE GRAND TOTAL OF THE SIXTEEN RANDOM VARIABLES . . . . .	27
TABLE A1-1.	APPROXIMATE AND TRUE MEANS AND STANDARD ERRORS . . . .	40
TABLE A3-1.	VALUES OF $\mu$ AND $\sigma$ . . . . .	45
TABLE A3-2.	VALUES OF PROBABILITY (P) VS. PERCENTILES . . . . .	47

## LIST OF FIGURES

FIGURE 1.	FUNCTIONAL BLOCK DIAGRAM OF THE BRAKE SYSTEM, REVISED DESIGN (FROM PRELIMINARY DRAFT REPORT WCAP-13800, PAGE 2-4). . . . .	4
FIGURE 2.	CUMULATIVE DISTRIBUTION FUNCTION FOR PROBABILITY OF FAILURE OF BRAKE SYSTEM, REVISED DESIGN . . . . .	28
FIGURE A3-1.	CUMULATIVE DISTRIBUTION FUNCTION FOR PROBABILITY OF FAILURE OF WASTE HOIST (SENSITIVITY CASE 1, CHAN ET AL, 1987, UNPUBLISHED REPORT) . . . . .	48



## SUMMARY

The Environmental Evaluation Group (EEG) previously analyzed the probability of a catastrophic accident in the waste hoist of the Waste Isolation Pilot Plant (WIPP) and published the results in Greenfield (1990; EEG-44) and Greenfield and Sargent (1993; EEG-53). The most significant safety element in the waste hoist is the hydraulic brake system, whose possible failure was identified in these studies as the most important contributor in accident scenarios. Westinghouse Electric Corporation, Waste Isolation Division (WEC-WID, 1994) has calculated the probability of an accident involving the brake system based on studies utilizing extensive fault tree analyses. This analysis conducted for the U.S. Department of Energy (DOE) used point estimates to describe the probability of failure and includes failure rates for the various components comprising the brake system. An additional controlling factor in the DOE calculations is the mode of operation of the brake system. This factor enters for the following reason. The basic failure rate per annum of any individual element is called the Event Probability (EP), and is expressed as the probability of failure per annum. The EP in turn is the product of two factors. One is the "reported" failure rate, usually expressed as the probability of failure per hour and the other is the expected number of hours that the element is in use, called the "mission time". In many instances the "mission time" will be the number of operating hours of the brake system per annum. However since the operation of the waste hoist system includes regular "preoperational check" tests, the "mission time" for standby components is reduced in accordance with the specifics of the operational time table.

The reported failure rates vary in both source and form. Any given element, whether it is a valve, a relay, a filter, or a heat exchanger, may be utilized by many users, both commercial and military. The nature of the use can be extremely varied as well; in flight, on seagoing vessels, on land with difficult or benign conditions, in laboratories with controlled environments, or in nuclear power plants. The data from a given kind of user will generally be described by a type of probability distribution (lognormal, exponential, etc.).

In earlier reports (Banz, et al., 1985; Chan, et al., 1987), DOE relied on relatively older performance reliability data reported by the Institute of Electrical and Electronics Engineers (IEEE). These reliability data reported by the IEEE were usually from Nuclear Power Generating Stations. There are some difficulties and ambiguities in the IEEE data used in those

DOE reports which are discussed in detail by Greenfield and Sargent (1993). The failure rates of key components in the IEEE data are much smaller than the values quoted in more recent sources. Greenfield and Sargent (1993) calculated an annual probability of failure for the brake system that ranged from  $10^{-6}$  to  $10^{-4}$  and described a methodology for calculating probability distributions to evaluate the risk of failure of the brake system. This approach provides the mean value for the probability of failure as well as the estimates of uncertainties.

EEG recommended that the DOE use more current information about the failure rates for the most important components of the system and follow the recommendation of the Nuclear Regulatory Commission to include mean estimates and to "take into account the potential uncertainties that exist so that an estimate can be made on the confidence level to be ascribed to the quantitative results." (Greenfield and Sargent, 1993).

WEC-WID (1994) addressed a number of the concerns described above. The report presents a simplified and improved design of the brake system using recently published failure data to calculate the probability of failure. These calculations are based on an extensive fault tree analysis. The failure data used is taken from a series of reports titled "Nonelectronic Parts Reliability Data" (NPRD). The NPRD data are revised and updated periodically. WEC-WID (1994) used data from NPRD-91 (Denson et al., 1991). NPRD-95 (Denson et al., 1994) was published a few months after the publication of WEC-WID (1994), but fortunately only a few relatively small changes occurred in components relevant for the report. An advantage of the NPRD series is that the information is listed not only in terms of a failure rate of a generic part, but also in terms of the environment in which the part is used. A user can choose the data with an appropriate environment. Furthermore, the NPRD reports state that all the failure data can be described by a lognormal probability distribution function which allows one to make estimates of the confidence level to be ascribed to quantitative results.

In the revised design (WEC-WID, 1994), realistic failure data from NPRD-91 (Denson et al., 1991) for certain critical valves were used which were an order of magnitude or more higher than the values used for the Design Option B-2 described in the earlier DOE reports. Despite this, the final calculated value of the annual failure rate for the brake system in the revised design is given as approximately  $1.3 (E-7)$  (1/yr), only slightly better than the  $2.2 (E-7)$  (1/yr) for Design Option B-2. How is this explained?

The answer is found in the revision of the mission times for the standby components as contrasted with operating components. The event probability (EP) used in computing annual failure rates, is given by the product of the failure rate per hour (obtained from NPRD) and the mission time in (hrs/yr). The mission time depends on the mode of operation. Mission times for *operating* components are 1000 (hrs/yr) based on current operating experience of 7,000 round trips per year for the waste hoist. However the situation is quite different for *standby* components. A most important factor in the operating procedures is the use of preoperational checks at the start of each shift for the entire waste hoist system. This mode of operation results in the use of a mission time of 12 hours for standby components. Twelve rather than eight hours is used since shifts are sometimes extended. This mission time of 12 hours is assumed for standby components in the analysis of the revised design (WEC-WID, 1994). This factor helps to account for the calculation of an annual failure rate of the brake system in the revised design of  $1.3 (E-7) (1/yr)$ , despite the use of higher failure rates for key components like the emergency dump valves.

The change in the mission time assumption reflects a substantial improvement in the safety of the waste hoist operation because of the investment of time and energy in the preoperational testing of the entire system at the start of each shift. Since this is a crucial element in this analysis, EEG's Jim Kenney has reviewed the preoperational checks being conducted at the waste hoist at the start of each shift and has confirmed that they are indeed being conducted (Kenney, personal communication).

This report (EEG-59) presents new calculations of the annual failure probability of the brake system using the new mission time for standby components. The methodology is the same as that employed in EEG-53 (Greenfield and Sargent, 1993), and is described in detail in Appendix 1 of this report. This method evaluates the risk of failure of a system in terms of the probability functions describing failure rates which are applicable to individual components in the system. This approach provides not only the mean values for the probability of failure of the brake system but also provides estimates of uncertainties. The results are stated in terms of a Cumulative Distribution Function (CDF), which gives a probability of failure for a given level of confidence. This is in accord with standard engineering practice. Calculations were made for the data from NPRD-95 (Denson et al., 1994) and also from NPRD-91 (Denson et al., 1991) for comparison.

The results of the calculations are summarized, and are compared with the annual mean failure rate calculated by WEC-WID (1994).

WEC-WID (1994) for NPRD-91 Data	$1.3 \times 10^{-7}$
EEG (for NPRD-91 data)	$1.18 \times 10^{-7}$
EEG (for NPRD-95 data)	$1.30 \times 10^{-7}$

The mean failure rate of  $1.3 \times 10^{-7}$  (for NPRD-95 data) corresponds to an 82 confidence level; i.e. there is an 82% likelihood that the failure rate is less than  $1.3 \times 10^{-7}$ . Correspondingly there is an 18% likelihood that the failure rate is greater than  $1.3 \times 10^{-7}$ . The deviations of 82 percent and 18 percent from 50 percent measure the skewness of the probability distribution. At the 95 percentile, the probability of failure is  $4.5 \times 10^{-7}$ ; i.e. there is a 95% likelihood that the annual failure rate is less than  $4.5 \times 10^{-7}$ . For an annual failure rate of  $1.0 \times 10^{-6}$ , the percentile is 98.2; i.e. there is a 98.2% likelihood that the failure rate is less than  $1.0 \times 10^{-6}$ .

The conclusion of this report is that, based on the information supplied by WEC-WID (1994) on the data sources NPRD-91 and NPRD-95, the fault tree analysis and the resulting structure of the cutset probability calculations, the predicted mean failure rate of the waste hoist is less than  $1.0 \times 10^{-6}$ . This improvement in the predicted failure rate is largely due to the DOE instituting preoperational checks at the waste hoist at the start of each shift, and remains valid so long as such checks are continued. This report does not evaluate the potential for accidents due to material defects, or improper construction or maintenance.

## RECOMMENDATIONS

The approximate annual failure probability of the brake system is  $4.5 \times 10^{-7}$  at 95% confidence level, i.e., there is a 95% likelihood that the failure rate per annum is less than  $4.5 \times 10^{-7}$ . A key element in achieving this degree of assurance of an acceptable failure rate is the use by DOE of preoperational checks of the entire waste hoist system at the start of each shift. Accordingly the following suggestions are made:

- 1) A periodic oversight should be maintained to assure that the preoperational checks are in fact being accomplished.
- 2) An annual review of the preoperational procedures should be made to ascertain whether changes or improvements are warranted.
- 3) Since the performance of preoperational check tests of the whole waste system is of paramount importance, it is recommended that such tests be made a Technical Safety Requirement in the Safety Analysis Report.
- 4) For all studies involving calculation of failure probabilities at WIPP, account should be taken of the uncertainties in the basic data, so that levels of confidence can be ascribed to the quantitative results.

## I. INTRODUCTION

### Historical Review

The Department of Energy (DOE) has worked to improve the design and operation of the waste hoist brake system at the Waste Isolation Pilot Plant (WIPP) over the years. Reports of various designs have been issued by DOE since 1985. Table 1 lists a number of these reports, along with the stated annual probability of failure of the brake system.

TABLE 1. HISTORICAL REVIEW, WASTE HOIST BRAKE SYSTEM AT WIPP

Case	Source	Probability Brake System Failure
Generic case	Banz et al. 1985, WTSD-TME-063, Westinghouse E.C.	$3.7 \times 10^{-7}$ (1/yr)
Base case	Chan et al. 1987; Section 6 in ORR, DOE/WIPP-88-022, V. 2, 1988 (Unpublished Draft)	$2.7 \times 10^{-2}$ (1/yr)
Sensitivity Case 1	Chan et al. Dec. 1987; (Unpublished Draft)	$1.5 \times 10^{-6}$ (1/yr)
Design Option B-2	FSAR, App 7B, 1990. IRA DOE/WIPP-89-010 (1990)	$2.2 \times 10^{-7}$ (1/yr)
Revised Design	WCAP-13800, February, 1994 (Preliminary Draft Report)	$1.3 \times 10^{-7}$ (1/yr)

The Environmental Evaluation Group (EEG) reviewed the Banz et al. (1985) report in 1985 (Greenfield, 1985, App.) and criticized it on the basis of quality assurance (QA) oversight, quality of maintenance, assumption of human factors, and assumption of operator errors. DOE rejected these suggestions, especially the possibility of human factors (12/20/1985 letter from W.R. Cooper to R.H. Neill, Greenfield, 1985, Appendices).

A serious incident occurred on July 25, 1987. Valve #45 of the waste hoist had leaked; a contractor was called in who changed the valve. After powering the hoist, it freewheeled 30 feet, then stopped by itself. The contractor noted the valve could be installed with a reversed orientation. This was done, followed by a powering of the hoist. This time a freewheeling of

300 feet occurred, and again the hoist stopped by itself. The DOE issued an Unusual Occurrence Report (UOR) (DOE 1987) on 8/11/87 and also conducted a Class C investigation on 10/15/87 (Westinghouse, 1987). With the valve reversed, it was in a dead center position, blocking the release of oil pressure, and causing the freewheeling. DOE listed a number of mistakes as human errors committed by supervisors, workers and contractors. The DOE report also criticized the absence of QA.

Following the 1987 incident, an engineering study of the waste hoist braking system was prepared (Chan et al., 1987) but not published. The report analyzed two cases, the Base Case and Sensitivity Case 1. The Base Case was a re-analysis of the so-called Generic Case of the Banz et al., 1985 report. Chan et al. found the Base Case to have an annual probability of failure of  $2.7 \times 10^{-2}$ , in contrast with the Generic Case claim of  $3.7 \times 10^{-7}$ . The flawed Generic Case assumed that two components of the braking system were independent, when in fact they were not, as demonstrated by the 1987 freewheeling incidents. The Chan et al. (1987) study recommended a re-design which included the concept of emergency dump valves to relieve the oil pressure. The re-design was called Sensitivity Case 1, and the annual failure probability of the braking system was  $1.5 \times 10^{-6}$ . This analysis included the possibility of human error.

DOE continued redesigning the braking system, including the important emergency dump valve feature and published two reports in 1990, one of which was Design Option B-2. The computed annual failure probability of the braking system was now  $2.2 \times 10^{-7}$ . Greenfield and Sargent (1993) analyzed the two DOE reports (USDOE, 1990; Westinghouse, 1990) on the status of the waste hoist brake system at the WIPP and demonstrated that the calculated failure probability of the brake system depends sensitively on the assumed failure rate of certain valves, but especially on motor operated valve 108. That fact prompted a careful review of the data sources quoted by the IRA and the FSAR for the design designated as B-2. Greenfield and Sargent (1993) cited several additional pertinent data sources not included in the DOE reports. These sources discussed imperfections in the failure rates data and gave a range of an order of magnitude of failure rates for the motor operated valves.

An additional problem arose from DOE using older data for the manual ball valves (56 Series) in NPRD-2 (Reliability Analysis Center, 1981). This reference was superseded by the more recent NPRD-3 (Rossi, 1985) which included the older data from NPRD-2, and contained

additional data for manual ball valve failure rates that were an order of magnitude higher than the older values.

A final difficulty with the DOE reports is the reliance on point estimates rather than including probability distributions, which take account of uncertainties in the basic failure data. The use of probability distributions makes it possible to compute cumulative distribution functions.

As a consequence of using older data sources and large uncertainties in the basic failure rates, Greenfield and Sargent (1993) could only assign a range of failure probabilities for the brake system, with the worst case scenario being annual failure rates far in excess of  $10^{-6}$ .

#### DOE Revised Design, 1994

It appears that DOE was not satisfied with the status of Design B-2. The DOE has pursued a policy of improving the design and making improvements in the waste hoist operation. A number of important changes were made subsequent to the B-2 Option. These are described in a preliminary draft DOE report WCAP-13800 (WEC-WID, 1994). This Revised Design introduced simplifications in piping and manifolds, installed more robust brakes, and most importantly, installed emergency dump valves to provide an additional path to the reservoir for the hydraulic fluid during the brake setting operation. The emergency relief paths were routed directly to the operating reservoir. The re-design of the brake manifolds and inlet piping involved removing the 56 Series (manual ball type) valves. Following earlier recommendations "an emergency relief path has been routed to the reservoir through emergency dump valves 52.1, 52.2. A diverter valve previously identified as valve 108 and recently identified as 45.2 has been installed. The diverter valve is a solenoid-operated 4 way valve and has no blocked center port position."

Figure 1 (taken from WCAP-13800, WEC-WID, 1994, Figure 2.1-2a, page 2-4) shows the position of the emergency dump valves 52.1 and 52.2 as well as the solenoid operated emergency diverter valve 45.2. Note that the emergency dump valves have a direct path to the reservoirs via the diverter valve 45.2 (no blocked center port position). The normal relief path is via the solenoid-operated 4-way valves 25.2.4 and 25.1.3.



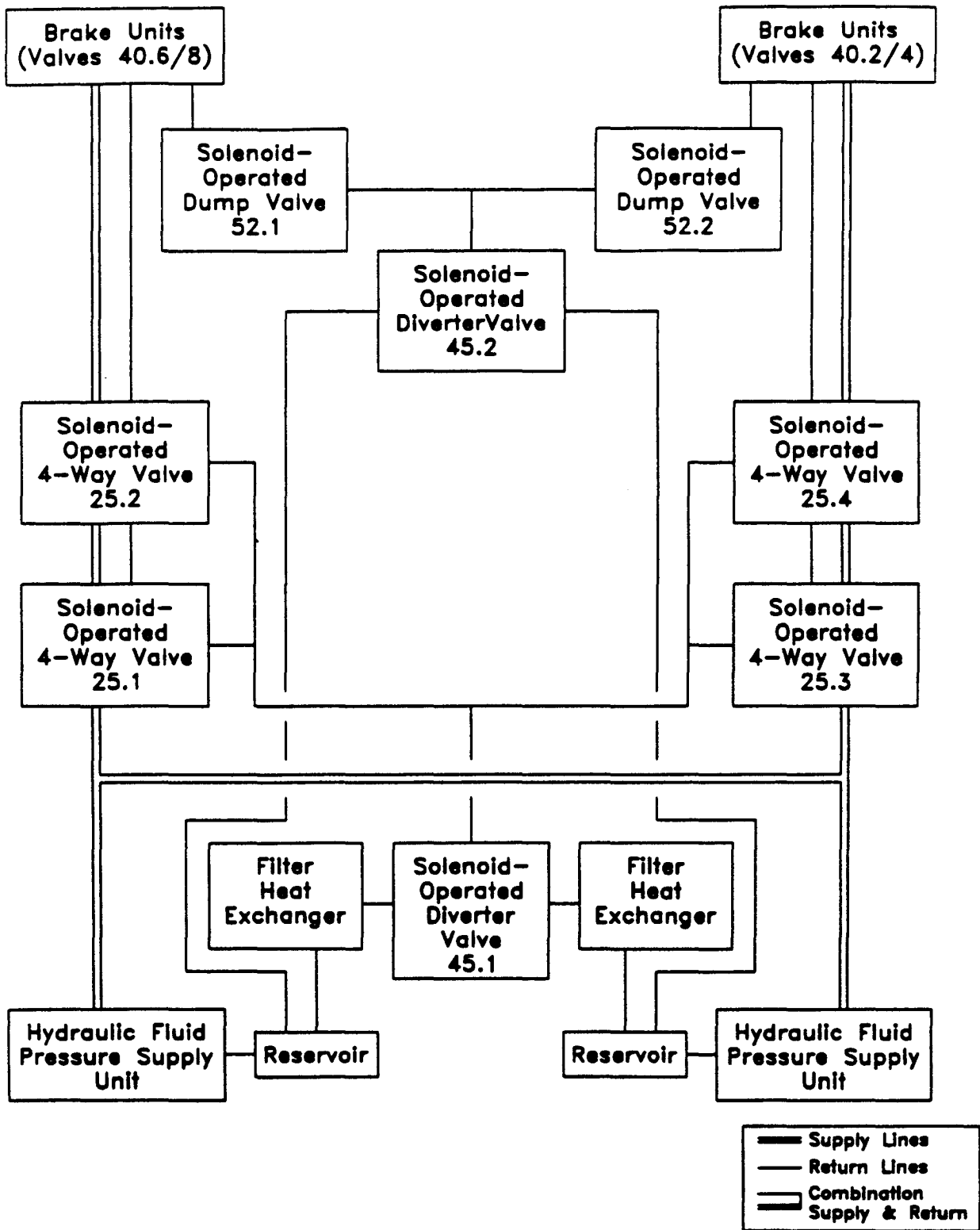


FIGURE 1. FUNCTIONAL BLOCK DIAGRAM OF THE BRAKE SYSTEM, REVISED DESIGN (FROM PRELIMINARY DRAFT REPORT WCAP-13800, WEC-WID, 1994, PAGE 2-4).

## II. DATA SOURCES

The authors of WEC-WID (1994) used a good source for valve failure data and other components of the brake system, the NPRD series. They used NPRD-91 (Denson et al., 1991) published in May, 1991. This was the latest NPRD publication available to WEC-WID (1994), which appeared in February, 1994. However NPRD-95 (Denson et al., 1994) was published in July, 1994. Fortunately most of the component failure data in NPRD-91 (Denson et al., 1991) used in WEC-WID (1994) are unchanged from those listed in Denson et al. (1994). However, there is a small change of +5% in the failure rate for the most important valves, the emergency dump valves 52.1 and 52.2, discussed in WEC-WID (1994). This information will be utilized later in this report to determine the sensitivity of the overall failure rate of the brake system to the failure rate of the emergency dump valves.

NPRD-95 and NPRD-91 (Denson et al., 1994, 1991) are the latest in the series previously published as NPRD-3 (Rossi, 1985) in 1985, and NPRD-2 (Reliability Analysis Center, 1981) in 1981 (both cited in EEG-53). The NPRD series has several advantages as a source of failure data. The information is listed not only in terms of failure rates for a generic part, but also in terms of the environment in which the part is used (airborne, naval, ground benign, ground fixed, ground mobile, spaceflight, etc.). Each environment is defined so that the user can pick and choose the appropriate data. The source of the data is also listed. Another indicator is the quality level denoted by Mil (parts procured in accordance with military specifications), Com (commercial quality parts) or Unk (unknown, data from a device of unknown quality level).

Most important is the statement in NPRD-91 (Denson et al., 1991) (and repeated in NPRD-95) that the data "estimate" the expected failure rates, and that the "true" values lie in some confidence intervals about these estimates. The following statement is a quote from NPRD-91 (Denson et al., 1991), page 1-6: "To give NPRD-91 users a better understanding of the confidence they can place in the presented estimated failure rates, an analysis was performed on the variation in observed failure rates. It was concluded that, for a given generic part type, the natural logarithm of the observed failure rate is normally distributed with a sigma ( $\sigma$ ) = 1.5. This indicates that 68 percent of actual failure rates will be between 0.22 and 4.5 times the mean value. Similarly, 90% of actual failure rates will be between 0.08 and 11.9 times the presented value."

These numbers arise from the following elementary properties of a lognormal distribution. For a normal distribution 68% of the failure rates will be between  $\pm \sigma (=1.5)$ .

$$\begin{array}{l} \text{But } e^{1.5} = 4.5 \\ \text{and } e^{-1.5} = 0.22 \end{array} \left. \vphantom{\begin{array}{l} \text{But } e^{1.5} = 4.5 \\ \text{and } e^{-1.5} = 0.22 \end{array}} \right\} \text{approximately}$$

Similarly 90% of the failure rates for a normal distribution will be between  $\pm 1.645 \sigma \doteq 2.47$

$$\begin{array}{l} e^{2.47} = 11.8 \\ \text{and } e^{-2.47} = 0.08 \end{array} \left. \vphantom{\begin{array}{l} e^{2.47} = 11.8 \\ \text{and } e^{-2.47} = 0.08 \end{array}} \right\} \text{approximately}$$

### III. FAILURE MODES FOR THE BRAKE SYSTEM

The authors of the preliminary draft WCAP-13800 (WEC-WID, 1994) prepared a complete fault tree analysis of the "Revised Design," setting out the possible failure modes. The report describes some 200 cutsets of different, possible modes of failure. Each cutset may involve two, three or four separate failures of individual components to make one failure mode (or cutset). The sum of the full 200 cutsets quoted by the report is  $1.265 \text{ E}(-07)$  (i.e.  $1.265 \times 10^{-7}$ ). However, just the first 16 cutsets (see Table 2) sums up to  $1.262 \text{ E}(-07)$ , which is 99.8% of the sum of the total of 200 cutsets. For that reason this report will concern itself with an analysis of the first 16 cutsets. Indeed the first five cutsets account for 96.5% of the total. Table 3 shows that the first five cutsets all include failure of the emergency dump valves, 52.1.2. The first three cutsets involve failures of the emergency dump valves combined in various ways with failures of the "normal relief path" solenoid-operated 4-way valves 25.1, 25.2, 25.3, 25.4. The sum of just these three cutsets is 89.6% of the total of 200 cutsets. Clearly the failure modes are dominated by these first listed cutsets, and especially by the emergency dump valves 52.1 and 52.2.

# WIPP WASTE HOIST BRAKE SYSTEM ANALYSIS - PRELIMINARY REPORT

PAGE 1 TREE NAME: whbs  
 CUTDES VER.1.7, 11-17-89  
 INPUT FILE: whbs.cds

CUT SETS FOR GATE G0001 WITH CUTOFF PROBABILITY OF 1.00E-15  
 GATE G0001 IS: FAILURE OF 3 OF 4 BRAKE PAIRS TO SET APT BRAKE RELEASE

NUMBER	CUTSET PROB.	BASIC EVENT NAME	EVENT PROB.	IDENTIFIER
1.	6.91E-08	HYDRAULIC VALVES 25.2 & 25.4 TOTALLY BLOCKED BY COMMON CAUSE BOTH EMERGENCY DUMP VALVES FAIL TO DE-ENERD DUE TO C.C	2.40E-03 2.88E-05	WHV25.24CM WSV52.12CM
2.	2.76E-08	SOLENOID OPERATD HV 25.1.2.3 & .4 FAIL TO DE-ENERD DUE TO C.C BOTH EMERGENCY DUMP VALVES FAIL TO DE-ENERD DUE TO C.C	9.60E-04 2.88E-05	WHV25---CM WSV52.12CM
3.	1.66E-08	SOLENOID OPERATD HV 25.4 FAILS RESULTING IN TOTAL BLOCKAGE BOTH EMERGENCY DUMP VALVES FAIL TO DE-ENERD DUE TO C.C SOLENOID OPERATD HV 25.2 FAILS RESULTING IN TOTAL BLOCKAGE	2.40E-02 2.88E-05 2.40E-02	WHV25.4-OC WSV52.12CM WHV25.2-OC
4.	7.00E-09	FILTER 15.1 PLUGGED, DUE TO LOCAL FAULTS BYPASS CHECK VALVE 15.1 FAILS CLOSED BOTH EMERGENCY DUMP VALVES FAIL TO DE-ENERD DUE TO C.C	3.20E-02 7.60E-03 2.88E-05	WFL15.1-PL WCV15.1-OC WSV52.12CM
5.	1.73E-09	HEAT EXCHANGER 13.1 PLUGS, BLOCKING FLOW BY-PASS CHECK VALVE 14.1 FAILS CLOSED BOTH EMERGENCY DUMP VALVES FAIL TO DE-ENERD DUE TO C.C	7.90E-03 7.60E-03 2.88E-05	WHX13.1-PL WCV14.1-CC WSV52.12CM
6.	9.73E-10	OVERTRAVEL RELAY FOR HOIST RAISING ROT FAILS TO OPEN RELAY MXE FAILS TO OPEN ON ESTOP SITUATION	3.12E-05 3.12E-05	WREROT--CC WREMXE--CC
7.	9.73E-10	OVERTRAVEL RELAY FOR HOIST LOWERING LOT FAILS TO OPEN RELAY MXE FAILS TO OPEN ON ESTOP SITUATION	3.12E-05 3.12E-05	WRELOT--CC WREMXE--CC
8.	3.98E-10	SOLENOID OPERATD HV 25.4 FAILS RESULTING IN TOTAL BLOCKAGE BOTH EMERGENCY DUMP VALVES FAIL TO DE-ENERD DUE TO C.C HV 25.2 FAILS TO DE-ENERGIZE DUE TO LOCAL FAULT SOLENOID OPERATD HV 25.1 FAILS, RESULTING IN TOTAL BLOCKAGE	2.40E-02 2.88E-05 2.40E-02 2.40E-02	WHV25.4-OC WSV52.12CM WHV25.2-FA WHV25.1-OC
9.	3.98E-10	SOLENOID OPERATD HV 25.4 FAILS RESULTING IN TOTAL BLOCKAGE BOTH EMERGENCY DUMP VALVES FAIL TO DE-ENERD DUE TO C.C HV 25.2 FAILS TO DE-ENERGIZE DUE TO LOCAL FAULT SOLENOID OPERATD HV 25.1 FAILS TO DE-ENERGIZ DUE TO LOCAL FAULTS	2.40E-02 2.88E-05 2.40E-02 2.40E-02	WHV25.4-OC WSV52.12CM WHV25.2-FA WHV25.1-FA
10.	3.98E-10	SOLENOID OPERATD HV 25.4 FAILS TO DE-ENERGIZE DUE TO LOCAL FAULTS SOLENOID OPERATD HV 25.3 FAILS, RESULTING IN TOTAL BLOCKAGE BOTH EMERGENCY DUMP VALVES FAIL TO DE-ENERD DUE TO C.C SOLENOID OPERATD HV 25.2 FAILS RESULTING IN TOTAL BLOCKAGE	2.40E-02 2.40E-02 2.88E-05 2.40E-02	WHV25.4-FA WHV25.3-OC WSV52.12CM WHV25.2-OC
11.	3.98E-10	SOLENOID OPERATD HV 25.4 FAILS TO DE-ENERGIZE DUE TO LOCAL FAULTS HV 25.3 FAILS TO DE-ENERGIZE DUE TO LOCAL FAULTS BOTH EMERGENCY DUMP VALVES FAIL TO DE-ENERD DUE TO C.C SOLENOID OPERATD HV 25.2 FAILS RESULTING IN TOTAL BLOCKAGE	2.40E-02 2.40E-02 2.88E-05 2.40E-02	WHV25.4-FA WHV25.3-FA WSV52.12CM WHV25.2-OC
12.	1.99E-10	HYDRAULIC VALVES 25.2 & 25.4 TOTALLY BLOCKED BY COMMON CAUSE SOLENOID OPERATD EMERGENCY DUMP VLV 52.2 FAILS TO DE-ENERGIZE SOLENOID OPERATD EMERGENCY DUMP VLV 52.1 FAILS TO DE-ENERGIZE	2.40E-03 2.88E-04 2.88E-04	WHV25.24CM WSV52.2-CC WSV521--CC
13.	1.26E-10	SOLENOID OPERATD HV 25.4 FAILS RESULTING IN TOTAL BLOCKAGE BOTH EMERGENCY DUMP VALVES FAIL TO DE-ENERD DUE TO C.C HV 25.2 FAILS TO DE-ENERGIZE DUE TO LOCAL FAULT CHECK VALVE 37.1 FAILS CLOSED	2.40E-02 2.88E-05 2.40E-02 7.60E-03	WHV25.4-OC WSV52.12CM WHV25.2-FA WCV37.1-CC
14.	1.26E-10	SOLENOID OPERATD HV 25.4 FAILS TO DE-ENERGIZE DUE TO LOCAL FAULTS CHECK VALVE 37.2 FAILS CLOSED BOTH EMERGENCY DUMP VALVES FAIL TO DE-ENERD DUE TO C.C SOLENOID OPERATD HV 25.2 FAILS RESULTING IN TOTAL BLOCKAGE	2.40E-02 7.60E-03 2.88E-05 2.40E-02	WHV25.4-FA WCV37.2-CC WSV52.12CM WHV25.2-OC
15.	9.73E-11	OVERTRAVEL RELAY FOR HOIST RAISING ROT FAILS TO OPEN RELAYS MXX1 AND MXX2 FAIL TO OPEN DUE TO COMMON CAUSE	3.12E-05 3.12E-06	WREROT--CC WREMX1.2CM
16.	9.73E-11	OVERTRAVEL RELAY FOR HOIST LOWERING LOT FAILS TO OPEN RELAYS MXX1 AND MXX2 FAIL TO OPEN DUE TO COMMON CAUSE	3.12E-05 3.12E-06	WRELOT--CC WREMX1.2CM

TABLE 2. EVENT PROBABILITIES FOR VARIOUS FAILURE MODES (FROM PRELIMINARY DRAFT REPORT WCAP-13800, WEC-WID, 1994, PAGE A3-4).

**Results of the Revised Design Analysis**

The probability of failure of the revised design is 1.3E-07/yr. The first five cutsets are listed below. System failure is dominated by the following combinations of events, or cutsets, and corresponding failure probabilities. Complete results from this analysis is provided in Appendix 2.

<b><u>Cutset – Revised Design</u></b>	<b><u>Annual Probability of Failure</u></b>	<b><u>Percentage Contribution To Total</u></b>
1. Hydraulic valves 25.2 & 25.4 are totally blocked by common cause; Both emergency dump valves fail to de-energize due to common cause	6.91E-8	54.6%
2. Solenoid-Operated Hydraulic valves 25.1.2.3 & .4 fail to de-energize due to common cause; Both emergency dump valves fail to de-energize due to common cause	2.76E-08	21.8%
3. Solenoid-Operated Hydraulic valve 25.4 fails resulting in total blockage; Both emergency dump valves fail to de-energize due to common cause; Solenoid-Operated Hydraulic valve 25.2 fails resulting in total blockage	1.66E-08	13.1%
4. Filter 15.1 plugged, due to local faults; Bypass check valve 15.1 fails closed; Both emergency dump valves fail to de-energize due to common cause	7.00E-09	5.5%
5. Heat exchanger 13.1 plugs, blocking flow; Bypass check valve 14.1 fails closed; Both emergency dump valves fail to de-energize due to common cause	1.73E-09	1.4%
	Contribution of these cutsets to total	96.4%

TABLE 3. RESULTS OF THE REVISED DESIGN ANALYSIS (FROM PRELIMINARY DRAFT REPORT WCAP-13800, WEC-WID, 1994, PAGE 3-6).

The cutset calculations in WCAP-13800 (WEC-WID, 1994) are based on "point estimates" of the failure rates given by NPRD-91 (Denson et al., 1991). No account is taken of the dispersion of failure data corresponding to a lognormal distribution, with a sigma ( $\sigma$ ) = 1.5.

The calculations of the cutsets in the Revised Design utilized failure rates given in NPRD-91 (Denson et al., 1991). A few examples of failure rates for important components are listed in Table 4. For comparison the failure rates for motor operated valve 108 and manual ball valve 56 used in the B-2 design are also listed.

TABLE 4

<u>Failure Rates for Components, Revised Design</u>	
<u>Component</u>	<u>Failure Rate</u>
Solenoid operated valve; e.g. 52.1, 52.2	2.4 x E(-5) 1/hr.
Filter plugged	3.2 x E(-5) 1/hr.
Electromechanical relays	2.6 x E (-6) 1/hr.
Bypass check valve fails closed	7.6 x E (-6) 1/hr.
Heat exchanger plugs	7.9 x E (-6) 1 hr.
<u>Failure Rates for Components, B-2 Design</u>	
<u>Component</u>	<u>Failure Rate</u>
Solenoid operated valve; motor operated valve 108	6 x E (-8) 1/hr.
Manual ball valves 56.3.6	0.65 x E (-6) 1/hr.

Comparison of the failure rates in Table 4 shows that the values in the Revised Design are one or more orders of magnitude greater than those listed for Design B-2. Despite this, the final calculated value of the annual failure rate for the brake system in the Revised Design is given

as approximately 1.3 (E-7) (1/yr), better than the 2.2 (E-7) (1/yr) for Design Option B-2 by almost a factor of two. How is this explained?

The answer is found in the revision of mission times for the operating components and for the standby components. Note that the EP per year utilized in computing the cutsets is given by the product of the failure rate per hour and the mission time in (hrs/yr). In the B-2 design the mission times for key components were taken as 2,048 (hrs/yr) (essentially 40 hrs/wk x 50 wks/yr). This number has been reduced to 1,000 (hrs/yr) for operating components on the basis of current operating experience of 7,000 round trips per year. A most important second factor has been the use of preoperational checks at the start of each shift for the entire waste hoist system. This has resulted in the use of a mission time of 12 hours for standby components. Twelve rather than eight hours is used for mission times since shifts are sometimes extended. This mission time of 12 hours is utilized for standby components in the analysis of the Revised Design in WCAP-13800 (WEC-WID, 1994).

These changes in mission times have achieved the counter balance to the larger (more realistic) failure rates for components to produce essentially the same annual failure rate of the brake system for the Revised Design as had been calculated for the previous B-2 Design.

These changes in the mission times are not simply changes in numbers to secure a desired result in calculations. They represent substantial improvements in the safety operation of the waste hoist because of the preoperational testing of the entire waste hoist system at the start of each shift. Since this is an important and crucial element in the analysis of the overall safety of the brake system, EEG resident engineer Jim Kenney reviewed the preoperational checks ongoing at the waste hoist system at the start of each shift. He reported positively on this matter. On this basis, the allotted mission times for the standby components are accepted, and will be used in this analysis. See Appendix 2.

## IV. CALCULATIONS FOR REVISED DESIGN

### DOE Calculations

A summary is now presented for the DOE calculations of the Revised Design, as it appears in WCAP-13800 (WEC-WID, 1994). This will be followed by the EEG analysis using the same basic failure data for components, with the added feature of using lognormal distributions, as described by NPRD-91 and NPRD-95 (Denson et al., 1991, 1994). The calculations in WCAP-13800 (WEC-WID, 1994) are based on the failure data listed in NPRD-91 (Denson et al., 1991). The EEG analysis will include both NPRD-91 and NPRD-95 (Denson et al., 1991, 1994) as two separate cases for comparison purposes.

A sample of the cutset calculations in WCAP-13800 (WEC-WID, 1994) is given in Table 5. Only the first five cutsets are listed, which together account for 96.5% of the total of 200 cutsets. The sum of the 200 cutsets is  $1.265 \times 10^{-7}$  for the annual probability of failure of the brake system. The sum for the first five is  $1.220 \times 10^{-7}$ .

The cutset probability is the combined product of the event probabilities (EP). Each EP is in turn the product of a failure rate and a mission time. A number of EP values will now be calculated to illustrate the process. Consider cutset number 1. The generic failure rate, Q, for a solenoid hydraulic valve is given by NPRD-3 (Rossi, 1985), page 2-156 as:

$$Q = 2.39 \times 10^{-5} \text{ (1/hr)}$$

WCAP-13800 (WEC-WID, 1994) used the rounded value  $2.4 \times 10^{-5}$ . See Table 4.

For common cause failure of two solenoid hydraulic valves one computes the common cause failure rate,  $P_{cc}$ , as follows (see WCAP-13800, WEC-WID, 1994, section A5.3.3):

$$P_{cc} = \beta Q ; \beta = 0.1$$
$$\text{Hence } P_{cc} = 2.4 \times 10^{-6} \text{ (1/hr)}$$



TABLE 5. CUTSETS FOR ANNUAL FAILURE RATES  
(WCAP-13800, WEC-WID, 1994, PAGE A3-4)

Number	Cutset Prob	Basic Event	(EP) Event Prob
1.a	6.91 x E(-8)	Hydraulic valves 25.2 & 25.4 totally blocked by common cause (c.c.);	2.40 x E(-3)
b		Both emergency dump valves fail to de-energize due to c.c.	2.88 x E(-5)
2.a	2.76 x E(-8)	Solenoid operated HV 25.1.2.3.4 fail to de-energize due to c.c.;	9.60 x E(-4)
b		Both emergency dump valves fail to de-energize due to c.c.	2.88 x E(-5)
3.a	1.66 x E(-8)	Solenoid operated HV 25.4 fails	2.40 x E(-2)
b		Both emergency dump valves fail de-energize due to c.c.	2.88 x E(-5)
c		Solenoid operated HV 25.2 fails	2.40 x E(-2)
4.a	7.00 x E(-9)	Filter 15.1 plugged, local faults	3.20 x E(-2)
b		Bypass check valve 15.1 fails closed	7.60 x E(-3)
c		Both emergency dump valves fail to de-energize due to c.c.	2.88 x E(-5)
5.a	1.73 x E(-9)	Heat exchanger 13.1 plugs, blocking flow	7.90 x E(-3)
b		Bypass check valve 14.1 fails closed	7.60 x E(-3)
c		Both emergency dump valves fail to de-energize due to c.c.	2.88 X E(-5)
<b>Sum = 1.220 x E(-7)</b>			

The mission time for this event is 1,000 hrs (WEC-WID, 1994, page A3-3)

$$\text{thus EP} = P_{cc} \times 10^3 = 2.4 \times E(-3)$$

This is the value for EP in number 1a, Table 5.

For number 1b the value for  $P_{cc}$  is:

$$P_{cc} = 2.4 \times E(-6) \text{ (1/hr), as above.}$$

However, the mission time is now 12 hours (WEC-WID, 1994, page A3-3).

$$EP = P_{cc} \times 12 = 2.88 \times E(-5)$$

This is the value for EP in number 1b.

For cutset 2a, the generic failure rate for a solenoid, hydraulic valves is:

$$Q = 2.4 \times E(-5)$$

For the failure of four valves  $P_{cc}$  is given by:

$$P_{cc} = 6\beta_2Q^3 + 4\beta_3Q^2 + \beta_4Q \text{ (WCAP-13800, section A.5.3.3)}$$

$$\beta_2 = 0.1, \beta_3 = 0.05, \beta_4 = 0.04.$$

Retaining the last term only:

$$\begin{aligned} P_{cc} &= \beta_4Q = 0.04 \times 2.4 \times E(-5) \\ &= 9.6 \times E(-7) \end{aligned}$$

Again, mission time = 1,000 hrs.

$$EP = 9.6 \times E(-7) \times 1,000 = 9.6 \times E(-4)$$

This is the value for EP listed in number 2a, Table 5.

Number 2b is the same as number 1b.

For number 3a, the generic failure rate  $Q = 2.4 \times E(-5)$ .

Mission time is 1,000 hrs;  $EP = 1,000 Q = 2.4 \times E(-2)$ .

Number 3b is the same as 2b and 1b.

Number 3c is the same as 3a.

Number 4a has  $Q = 3.2 \times E(-5)$ ; see Table 4.

Mission time is 1,000 hrs;  $EP = 1,000 Q = 3.2 \times E(-2)$ .

Number 4b has  $Q = 7.6 \times E(-6)$ ; see Table 4.

Mission time is 1,000 hrs;  $EP = 1,000 Q = 7.6 \times E(-3)$

Number 4c is the same as 3b, etc.

Number 5a has  $Q = 7.9 \times E(-6)$ , see Table 4.

Mission time is 1,000 hrs;  $EP = 1,000 Q = 7.9 \times E(-3)$

Numbers 5b,c are the same as numbers 4,b,c.

In each of the five cutsets, the combined products of the EP values produce the values listed for the Cutset Probability in Table 5.

### EEG Calculations

For clarity in following the computations for the Revised Design, a format will be used that is similar to the table on page A3-4, WIPP Waste Hoist Brake System Analysis, WCAP-13800 (WEC-WID, 1994). The calculations will be based on the data obtained from NPRD-95 (Denson et al., 1994), which differ in some cases from NPRD-91 (Denson et al., 1991). Table 6 lists the values for both NPRD's, so that the differences may be noted. All the components appearing in the 16 cutsets used in this calculation are listed in Table 6. The numbers in parentheses in columns 2 and 3 are the page numbers in the NPRD's (Denson et al., 1991, 1994). The failure rates listed in columns 2 and 3 are per  $10^6$  hours.

TABLE 6. COMPARISON OF FAILURE RATES FOR COMPONENTS AS LISTED IN NPRD-91 AND NPRD-95

Component	NPRD-91	NPRD-95
Valve, hydraulic, solenoid (Summary)	(2-156) 23.8627	(2-230) 25.0590
Valve, hydraulic, check (Unk - GF)	(2-153) 7.5884	(2-227) 7.5884
Valve, hydraulic, needle	(2-154) 4.1463	(2-229) 4.1463
Relay, electromechanical (General purpose, Com, GF)	(2-113) 2.5679	(2-169) 2.5679
Mechanical filter, hydraulic (Summary)	(2-89) 31.5593	(2-134) 29.7370
Heat exchanger, radiator (Unk - GF)	(2-74) 7.8829	(2-112) 7.88929
Valve, hydraulic, relief (Unk)	(2-155) 2.4551	(2-229) 2.4551

Note that the changes occur only for the solenoid, hydraulic valve, with an increase of +5.0%, and for the hydraulic, mechanical filter, with a decrease of -5.8%. The solenoid, hydraulic valve is the most important component, since its failure rate appears in most of the cutsets. In fact its failure rate appears in all the event probabilities of the first five cutsets.

Each EP is associated with either a 1,000 hr or a 12 hr mission time. Table 7 lists the reference numbers along with the associated cutset numbers (in parentheses) and the mission times in hours. These reference numbers will appear with each associated cutset number in the computation tables to follow, Table 7, 8, and 9. The reference numbers are taken from DOE report WCAP-13800 (WEC-WID, 1994), and refer to a type of component failure.

Both NPRD-91 and NPRD-95 (Denson et al., 1991, 1994) state that the data listed represent estimates of the expected failure rates. See page 1-6 in NPRD-91, and page 1-7 in NPRD-95. "For a given generic part type, the natural logarithm of the observed failure rate is normally distributed with a sigma ( $\sigma$ ) of 1.5."

The analysis of the data will assume such a lognormal distribution with a sigma ( $\sigma$ ) = 1.5.

TABLE 7. LISTING OF REFERENCE NUMBERS, ASSOCIATED EP NUMBERS AND MISSION TIMES

<u>Reference Number</u>	<u>Mission Time (hrs)</u>
050 (8c, 9c, 9d, 10a, 11a, 11b, 13c, 14a)	1000
056 (4a)	1000
059 (5a)	1000
064 (2a)	1000
071 (3a, 3c, 8a, 8d, 9a, 10b, 10d, 11d, 13a, 14d)	1000
074 (1a, 12a)	1000
077 (4b, 5b, 13d, 14b)	1000
051 (12b, 12c)	12
067 (6a, 6b, 7a, 7b, 15a, 16a)	12
072 (15b, 16b)	12
087 (1b, 2b, 3b, 4c, 5c, 8b, 9b, 10c, 11c, 13b, 14c)	12

A general form for the lognormal distribution with the two parameters,  $\mu$ ,  $\sigma$  is given by (Aitchison and Brown, 1969):

$$d \Lambda(x) = \frac{1}{(x \sigma \sqrt{2\pi})} \exp \left\{ -\frac{1}{(2\sigma^2)} (\log x - \mu)^2 \right\} dx \quad (1)$$

Where  $\Lambda$  is the cumulative distribution function (CDF).

The median of the distribution is given by:  $x_{md} = e^\mu$  (2)

The mean is given by:  $x_{mn} = e^{\mu + (\frac{1}{2})\sigma^2}$  (3)

According to the NPRDs (Denson et al., 1991, 1994)  $\sigma$  is known, equal to 1.5; the mean value  $x_{mn}$  is listed in the NPRD tables. This permits one to calculate the parameter  $\mu$ :

$$e^\mu = x_{mn} \times e^{-\left(\frac{1}{2}\right)\sigma^2} \quad (4)$$

Since  $\sigma = 1.5$ ,  $e^\mu = 0.3247 \times x_{mn}$  and  $\mu = \ln(0.3247 \times x_{mn})$

With knowledge of  $\mu, \sigma$  one may calculate the corresponding lognormal distribution, including the density function and the cumulative distribution function (CDF).

Table 5 indicates that each cutset probability is the product of two or more EP probabilities. Each of these EP probabilities will be represented by a lognormal distribution function. Using a theorem from Aitchison and Brown (1969, Theorem 2.2, p. 11), the product of lognormal distributions is also a lognormal distribution. (This theorem is called the "reproductive theorem").

If  $X_1$  is  $\Lambda(\mu_1, \sigma_1^2)$ ;  $X_2$  is  $\Lambda(\mu_2, \sigma_2^2)$  then  $X_1X_2$  is  $\Lambda(\mu_1 + \mu_2, \sigma_1^2 + \sigma_2^2)$ . (5)

Similarly  $X_1X_2X_3\dots X_n$  is  $\Lambda(\mu_1 + \mu_2 + \mu_3 + \dots + \mu_n, \sigma_1^2 + \sigma_2^2 + \sigma_3^2 + \dots + \sigma_n^2)$ . (6)

This theorem, applied to the  $\mu, \sigma$  values corresponding to the EP values for a given cutset, will permit the calculation of a lognormal distribution for each of the 16 cutsets.

Table 8 is a listing of the descriptors connecting the cutset numbers with the appropriate NPRD-95 (Denson et al., 1994) page number, the reference number (Ref), brief description of the component and the mode of failure, and the mission time in hours. Table 9 presents the calculations of the desired parameter  $\mu$  and  $\sigma (=1.5)$  for each EP, based on data from NPRD-95 (Denson et al., 1994).  $Q_{\text{mean}}$  is the failure rate of the component and is taken directly from NPRD-95 (Denson et al., 1994) (Table 8 gives the page number). In those instances for which common cause (c.c.) is the cause of failure, indicated in Table 8, a calculation of  $P_{\text{cc}}$ , the common cause failure rate, is made and the value is listed in column 4 of Table 9. The details of the calculation are given in Table 10, and are taken from WCAP-13800 (WEC-WID, 1994), section A 5.3.3. However Table 10 uses data from NPRD-95 rather than NPRD-91 (Denson et al., 1994, 1991). Column 5 of Table 9 gives the value of the Event Probability ( $EP_{\text{mean}}$ ), and is the product of either  $Q_{\text{mean}}$  or  $P_{\text{cc}}$ , as appropriate, and the mission time, listed in column 5 of Table 8. Column 6 of Table 9 is simply column 5 ( $EP_{\text{mean}}$ ) multiplied by the factor  $E(9)$  to produce more convenient numbers, without the exponential factors. In the final expression for the combined cutset probability the factor  $E(-9)$  will be introduced. Column 6 gives the values for  $e^{\mu + \frac{1}{2}\sigma^2}$  and must be multiplied by  $e^{-\frac{1}{2}\sigma^2}$  ( $=0.3247, \sigma=1.5$ ) to yield  $e^\mu$ , listed in column 7. Column 8,  $\mu$ , is calculated as the ln of the numbers listed in column 7. Column 9 lists the value of  $\sigma=1.5$ , for each cutset number.

It was stated previously that each cutset probability is the product of two or more EP probabilities (see Table 5). Since each of the EP probabilities is represented by a lognormal distribution function, one may use the "reproductive theorem" to obtain the lognormal distribution of the products. See equation (6). Let  $P_i$  be the lognormal probability distribution

for cutset number  $i$  ( $i=1,2,\dots,15,16$ ). Table 11 lists the values of  $\mu_i$ ,  $\sigma_i$  for each  $P_i$ , using equation (6). These values for  $\mu_i$ ,  $\sigma_i$  are computed from equation (6) as follows:

$$\mu_i = \mu_{ia} + \mu_{ib} + \text{etc} .$$

$$\sigma_i^2 = \sigma_{ia}^2 + \sigma_{ib}^2 + \text{etc} .$$

The values of  $\mu_{ia}$ ,  $\mu_{ib}$ , ...  $\sigma_{ia}$ ,  $\sigma_{ib}$  ... are listed in columns 8 and 9, Table 9.

The failure distribution,  $P$ , can now be expressed as the grand sum of 16 lognormal random variables.

$$P = 10^{-9} \times \sum_{i=1}^{i=16} P_i$$

The factor  $10^{-9}$  is introduced to cancel the  $10^{+9}$  used in column 6 of Table 9. The methods used to compute the failure distribution functions are described in detail in Appendix 1.



TABLE 8. COMPONENTS AND DESCRIPTORS

Cutset No.	NPRD-95 Page	Ref	Component, Failure Mode	Mission Time (Hrs)
1a	2-230	074	Hydraulic valves 25.2.4 blocked, common cause (c.c.)	1,000
b	2-230	087	Both emergency dump valves fail, c.c.	12
2a	2-230	064	Solenoid HV 25.1.2.3.4 fail, c.c.	1,000
b	2-230	087	Both emergency dump valves fail, c.c.	12
3a	2-230	071	Solenoid HV 25.4 fails	1,000
b	2-230	087	Both emergency dump valves fail, c.c.	12
c	2-230	071	Solenoid HV 25.2 fails	1,000
4a	2-134	056	Filter 15.1 plugged, local faults	1,000
b	2-227	077	Bypass check valve 15.1 fails closed	1,000
c	2-230	087	Both emergency dump valves fail, c.c.	12
5a	2-112	059	Heat exchanger 13.1 plugs, blocking flow	1,000
b	2-227	077	Bypass check valve 14.1 fails closed	1,000
c	2-230	087	Both emergency dump valves fail, c.c.	12
6a	2-169	067	Overtravel relay ROT fails to open	12
b	2-169	067	Relay MXE fails to open on ESTOP	12
7a	2-169	067	Overtravel relay LOT fails to open	12
b	2-169	067	Relay MXE fails to open on ESTOP	12
8a	2-230	071	Solenoid HV 25.4 fails	1,000
b	2-230	087	Both emergency dump valves fail, c.c.	12
c	2-230	050	HV 25.2 fails, local fault	1,000
d	2-230	071	Solenoid HV 25.1 fails	1,000
9a	2-230	071	Solenoid HV 25.4 fails	1,000
b	2-230	087	Both emergency dump valves fail, c.c.	12
c	2-230	050	HV 25.2 fails, local fault	1,000
d	2-230	050	Solenoid HV 25.1 fails, local fault	1,000
10a	2-230	050	Solenoid HV 25.4 fails, local fault	1,000
b	2-230	071	Solenoid HV 25.3 fails	1,000
c	2-230	087	Both emergency dump valves fail, c.c.	12
d	2-230	071	Solenoid HV 25.2 fails	1,000

TABLE 8. COMPONENTS AND DESCRIPTORS (Continued)

Cutset No.	NPRD-95 Page	Ref	Component, Failure Mode	Mission Time (Hrs)
11a	2-230	050	Solenoid HV 25.4 fails, local fault	1,000
b	2-230	050	HV 25.3 fails, local fault	1,000
c	2-230	087	Both emergency dump valves fail, c.c.	12
d	2-230	071	Solenoid HV 25.2 fails	1,000
12a	2-230	074	HVs 25.2 and 25.4 blocked, c.c.	1,000
b	2-230	051	Solenoid emergency dump valve 52.2 fails	12
c	2-230	051	Solenoid emergency dump valve 52.1 fails	12
13a	2-230	071	Solenoid HV 25.4 fails	1,000
b	2-230	087	Both emergency dump valves fail, c.c.	12
c	2-230	050	HV 25.2 fails, local fault	1,000
d	2-227	077	Check valve 37.1 fails closed	1,000
14a	2-230	050	Solenoid HV 25.4 fails, local fault	1,000
b	2-227	077	Check valve 37.2 fails closed	1,000
c	2-230	087	Both emergency dump valves fail, c.c.	12
d	2-230	071	Solenoid HV 25.2 fails	1,000
15a	2-169	067	Overtravel relay ROT fails to open	12
b	2-169	072	Relays MXX1 and MXX2 fail to open, c.c.	12
16a	2-169	067	Overtravel relay LOT fails to open	12
b	2-169	072	Relay MXX1 and MXX2 fail to open, c.c.	12

TABLE 9. CALCULATIONS FOR LOGNORMAL PARAMETERS,  
REVISED DESIGN (NPRD-95)

Cutset No.	Ref	$Q_{mean}$ (1/hr)	$P_{cc}$ (1/hr)	$EP_{mean}$	$10^9 EP_{mean} =$ $e^{\mu + \frac{1}{2}\sigma^2}$	$e^\mu$	$\mu$	$\sigma$
1a	074	25.06E(-6)	2.506E(-6)	2.506E(-3)	25.06	8.1370	2.0964	1.5
b	087	25.06E(-6)	2.506E(-6)	3.007E(-5)	3.007	0.9764	-0.0239	1.5
2a	064	25.06E(-6)	1.002E(-6)	1.002E(-3)	10.02	3.2535	1.1797	1.5
b	087	25.06E(-6)	2.506E(-6)	3.007E(-5)	3.007	0.9764	-0.0239	1.5
3a	071	25.06E(-6)		2.506E(-2)	2.506	0.8137	-0.2062	1.5
b	087	25.06E(-6)	2.506E(-6)	3.007E(-5)	3.007	0.9764	-0.0239	1.5
c	071	25.06E(-6)		2.506E(-2)	2.506	0.8137	-0.2062	1.5
4a	056	29.74E(-6)		2.974E(-2)	2.974	0.9657	-0.0349	1.5
b	077	7.588E(-6)		7.588E(-3)	7.588	2.4638	0.9017	1.5
c	087	25.06E(-6)	2.506E(-6)	3.007E(-5)	0.3007	0.9764-1	-2.3265	1.5
5a	059	7.883E(-6)		7.883E(-3)	7.883	2.560	0.9400	1.5
b	077	7.588E(-6)		7.588E(-3)	7.588	2.464	0.9018	1.5
c	087	25.06E(-6)	2.506E(-6)	3.007E(-5)	0.03007	0.9764-2	-4.6291	1.5
6a	067	2.568E(-6)		3.082E(-5)	3.082	1.0007	0.0007	1.5
b	067	2.568E(-6)		3.082E(-5)	0.3082	1.0007-1	-2.3019	1.5
7a	067	2.568E(-6)		3.082E(-5)	3.082	1.0007	0.0007	1.5
b	067	2.568E(-6)		3.082E(-5)	0.3082	1.0007-1	-2.3019	1.5
8a	071	25.06E(-6)		2.506E(-2)	2.506	0.8137	-0.2062	1.5
b	087	25.06E(-6)	2.506E(-6)	3.007E(-5)	3.007	0.9764	-0.0239	1.5
c	050	25.06E(-6)		2.506E(-2)	2.506	0.8137	-0.2062	1.5
d	071	25.06E(-6)		2.506E(-2)	0.02506	0.8137-2	-4.8113	1.5
9a	071	25.06E(-6)		2.506E(-2)	2.506	0.8137	-0.2062	1.5
b	087	25.06E(-6)	2.506E(-6)	3.007E(-5)	0.03007	0.9764-2	-4.6291	1.5
c	050	25.06E(-6)		2.506E(-2)	2.506	0.8137	-0.2062	1.5
d	050	25.06E(-6)		2.506E(-2)	2.506	0.8137	-0.2062	1.5

TABLE 9. CALCULATIONS FOR LOGNORMAL PARAMETERS,  
REVISED DESIGN (NPRD-95) (Continued)

Cutset No.	Ref	$Q_{\text{mean}}$ (1/hr)	$P_{\text{ce}}$ (1/hr)	$EP_{\text{mean}}$	$10^9 EP_{\text{mean}} =$ $e^{\mu + \frac{1}{2}\sigma^2}$	$e^{\mu}$	$\mu$	$\sigma$
10a	050	25.06E(-6)		2.506E(-2)	2.506	0.8137	-0.2062	1.5
b	071	25.06E(-6)		2.506E(-2)	2.506	0.8137	-0.2062	1.5
c	087	25.06E(-6)	2.506E(-6)	3.007E(-5)	0.03007	0.9764-2	-4.6291	1.5
d	071	25.06E(-6)		2.506E(-2)	2.506	0.8137	-0.2062	1.5
11a	050	25.06E(-6)		2.506E(-2)	2.506	0.8137	-0.2062	1.5
b	050	25.06E(-6)		2.506E(-2)	2.506	0.8137	-0.2062	1.5
c	087	25.06E(-6)	2.506E(-6)	3.007E(-5)	0.03007	0.9764-2	-4.6291	1.5
d	071	25.06E(-6)		2.506E(-2)	2.506	0.8137	-0.2062	1.5
12a	074	25.06E(-6)	2.506E(-6)	2.506E(-3)	2.506	0.8137	-0.2062	1.5
b	051	25.06E(-6)		3.007E(-4)	3.007	0.9764	-0.0239	1.5
c	051	25.06E(-6)		3.007E(-4)	0.03007	0.9764-2	-4.6291	1.5
13a	071	25.06E(-6)		2.506E(-2)	2.506	0.8137	-0.2062	1.5
b	087	25.06E(-6)	2.506E(-6)	3.007E(-5)	3.007	0.9764	-0.0239	1.5
c	050	25.06E(-6)		2.506E(-2)	2.506	0.8137	-0.2062	1.5
d	077	7.588E(-6)		7.588E(-3)	0.007588	0.2464-2	-6.0060	1.5
14a	050	25.06E(-6)		2.506E(-2)	2.506	0.8137	-0.2062	1.5
b	077	7.588E(-6)		7.588E(-3)	7.588	2.464	0.9018	1.5
c	087	25.06E(-6)	2.506E(-6)	3.007E(-5)	0.3007	0.9764-1	-2.3265	1.5
d	071	25.06E(-6)		2.506E(-2)	0.02506	0.8137-2	-4.8113	1.5
15a	067	2.568E(-6)		3.082E(-5)	3.082	1.0007	0.0007	1.5
b	072	2.568E(-6)	2.568E(-7)	3.082E(-6)	0.03082	1.0007-2	-4.6059	1.5
16a	067	2.568E(-6)		3.082E(-5)	3.082	1.0007	0.0007	1.5
b	072	2.568E(-6)	2.568E(-7)	3.082E(-6)	0.03082	1.0007-2	-4.6059	1.5

TABLE 10. COMMON CAUSE CALCULATIONS (NPRD-95);  
(WCAP-13800, WEC-WID, 1994, SECTION A5.3.3)

<p>Ref: 074            Event: WHV 25.2.4CM, hydraulic valve blocked  <math>Q = 25.06E(-6) (1/hr)</math>  <math>P_{cc} = \beta Q; \beta = 0.1</math>  <math>P_{cc} = 2.506E(-6) (1/hr)</math></p>
<p>Ref: 087            Event: both emergency dump valves fail  <math>Q = 25.06E(-6) (1/hr)</math>  <math>P_{cc} = \beta Q; \beta = 0.1</math>  <math>P_{cc} = 2.506E(-6) (1/hr)</math></p>
<p>Ref: 064            Event: solenoid HV 25.1.2.3.4 fail  <math>Q = 25.06E(-6)(1/hr)</math>  <math>P_{cc} = 6\beta_2 Q^3 + 4\beta_3 Q^2 + \beta_4 Q</math>  <math>\beta_2 = 0.1, \beta_3 = 0.05, \beta_4 = 0.04</math>            Calculate last term only.  <math>P_{cc} = \beta_4 Q = 0.04 \times 25.06E(-6)</math>  <math>= 1.002E(-6) (1/hr)</math></p>
<p>Ref: 072            Event: relays MXX1 and MXX2 fail to open  <math>Q = 2.568E(-6) (1/hr)</math>  <math>P_{cc} = \beta Q; \beta = 0.1</math>  <math>P_{cc} = 2.568E(-7) (1/hr)</math></p>

TABLE 11. VALUES OF THE PARAMETERS  
 $\mu$ ,  $\sigma$  FOR THE REVISED DESIGN (NPRD-95)

$P_i$	$\mu_i$	$\sigma_i$
1	2.0725	2.1213
2	1.1558	2.1213
3	-0.4363	2.5981
4	-1.4597	2.5981
5	-2.7873	2.5981
6	-2.3012	2.1213
7	-2.3012	2.1213
8	-5.2477	3.0000
9	-5.2477	3.0000
10	-5.2477	3.0000
11	-5.2477	3.0000
12	-4.8592	2.5981
13	-6.4423	3.0000
14	-6.4423	3.0000
15	-4.6052	2.1213
16	-4.6052	2.1213

$$P = 10^{-9} \times \sum_{i=1}^{i=16} P_i$$

$$dP_i(x) = \frac{1}{(x\sigma_i\sqrt{2\pi})} \exp \left\{ -\frac{1}{(2\sigma_i^2)} (\log x - \mu_i)^2 \right\} dx$$

This is a lognormal distribution, with parameters  $\mu_i$ ,  $\sigma_i$ .

## Numerical Results of EEG Calculations

Since it is possible to compute the true means and variances of each of the 16 component distributions, a comparison was made with the corresponding means and variances of the 16 approximating discrete distributions. This gives some idea of the sources of approximation errors. These data are listed in Appendix 1, Table A1-1, without the factor ( $10^9$ ).

For the grand total of the sixteen random variables the approximating and true means and standard errors are as follows, without the factor ( $10^9$ ):

TABLE 12. COMPARISON OF MEANS AND STANDARD ERRORS (NPRD-95).

Approximating Mean	130.0014
True Mean	137.4896
Approximating standard error	680.0873
True standard error	970.0158

Note that the approximate distribution has a smaller mean and lower standard deviation than the true one.

Table 13 lists the percentile values for the approximating probability distribution of the grand total of the sixteen random variables.

TABLE 13. PERCENTILES AND PROBABILITY VALUES OF THE GRAND TOTAL OF THE SIXTEEN RANDOM VARIABLES

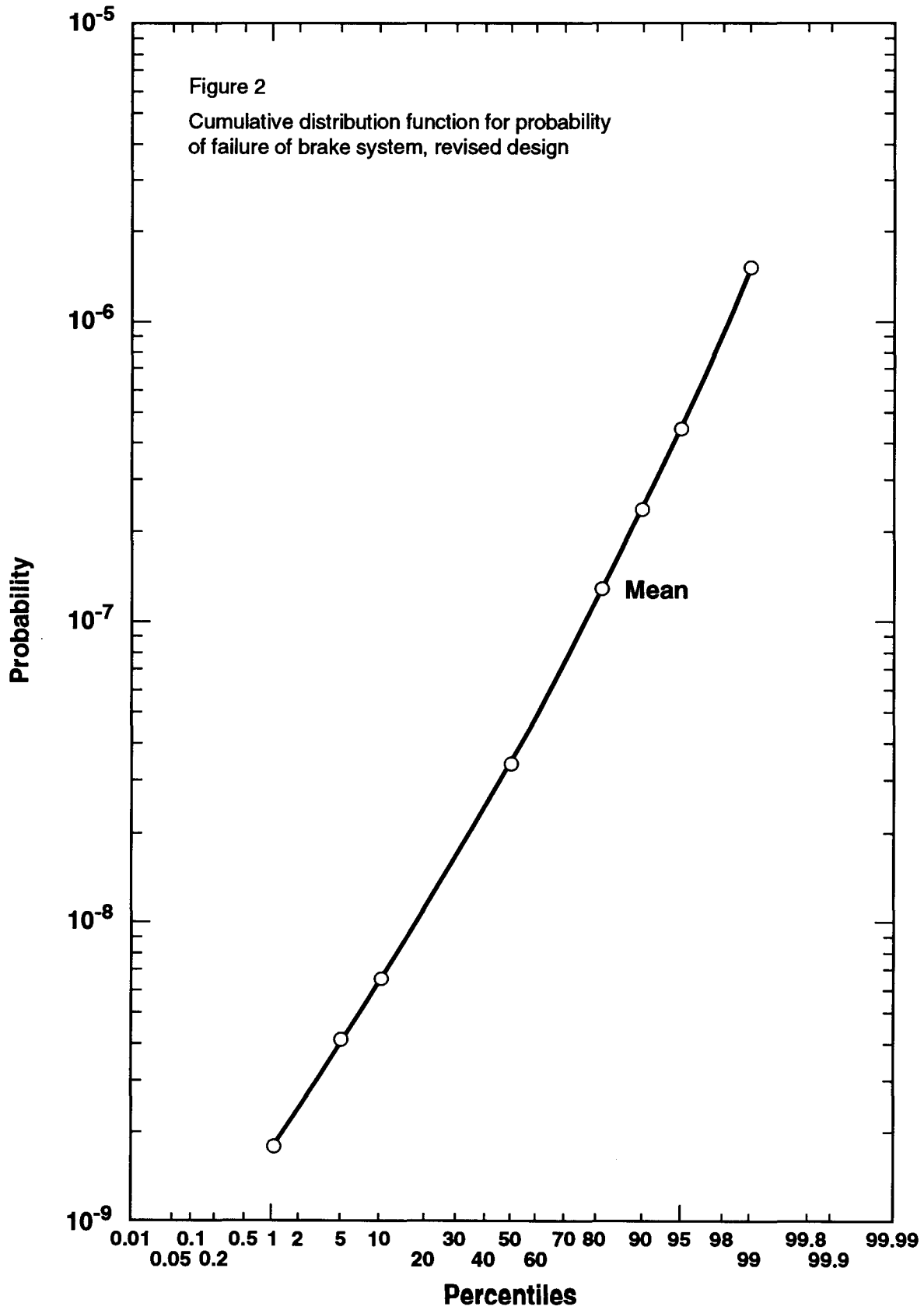
Percentile	Probability $\times 10^9$	
	NPRD-95	NPRD-91
1	1.8	
5	4.2	3.6
10	6.6	5.6
50	33.6	30.5
Mean	130.0	117.7
90	238.2	215.4
95	445.8	403.2
99	1569.0	1484.3

The values of the probability for NPRD-91 (Denson et al., 1991) are listed for comparison. The differences are relatively small, an order of 10% above the 10 percentile range up to the 95 percentile. Since the failure rates of the hydraulic valves have a +5% change, from NPRD-91 to NPRD-95 (see NPRD-95 (Denson et al., 1994), page 2-230, and NPRD-91 (Denson et al., 1991), page 2-156), and these valve types appear twice in the first several important cut-sets (see Table 8), the approximate 10% change in the probability values is not unexpected. It should be noted that the values of the probability in Table 13 are no more accurate than the means and standard errors of Table 12. The data in Table 13 for the probability and the percentiles have been plotted on "probability-log" graph paper; see Figure 2.

Some interesting statements may be made, based on Figure 2:

- (a) When the probability is  $10^{-6}$ , the percentile value is 98.2; i.e., there is a 98.2% likelihood that the failure rate per annum is less than  $1.0 \times 10^{-6}$ .





(b) At the 95 percentile, probability is  $4.5 \times 10^{-7}$ ; i.e., there is a 95% likelihood that the failure rate per annum is less than  $4.5 \times 10^{-7}$ .

(c) The mean failure rate is  $1.3 \times 10^{-7}$ , and corresponds to a percentile value of almost 82; i.e., there is an 82% likelihood that the failure rate is less than  $1.3 \times 10^{-7}$ . If one selects the "true" mean failure rate of  $1.37 \times 10^{-7}$  (from Table 12), the corresponding percentile is almost the same, just slightly more than 82. Rounded to the nearest whole percentile, one obtains the same percentile for either the approximate or the true mean.

It is interesting to compare the approximate and true means for NPRD-95 and NPRD-91 (Denson et al., 1994, 1991) with the failure rate quoted in WCAP-13800 (WEC-WID, 1994) (based on NPRD-91 (Denson et al., 1991)) of  $1.3 \times 10^{-7}$ .

	<u>NPRD-95</u>	<u>NPRD-91</u>
Approximate mean	$1.30 \times 10^{-7}$	$1.18 \times 10^{-7}$
True mean	$1.37 \times 10^{-7}$	$1.25 \times 10^{-7}$

## DISCUSSION

The analysis in this report is based on failure data obtained from NPRD-95 (Denson et al., 1994). This is in contrast to the calculations in the DOE report WCAP-13800 (WEC-WID, 1994) based on NPRD-91 (Denson et al., 1991). Fortunately the change in the reported failure rates for the important solenoid, hydraulic valve is relatively small, about 5%. This change in the failure rate of this valve led to a change in the mean failure rate of the brake system of only 10%.

The mean failure rate for the brake system stated in the DOE report, WCAP-13800 (WEC-WID, 1994), is  $1.3 \times 10^{-7}$ . This is close to the mean rates calculated herein as  $1.30 \times 10^{-7}$  (approximate) and  $1.37 \times 10^{-7}$  (true). However, the mean rates by themselves do not reveal the level of confidence to be associated with these numbers. As stated in the report a confidence level of 95% corresponds to a failure probability of  $4.5 \times 10^{-7}$  (approximate). The true value is greater. If one were to select a confidence level of 99%, the failure probability rises to  $1.5 \times 10^{-6}$  (approximate). It is the responsibility of DOE to select the confidence level at which it desires to operate.

A word about approximate and true values of the means (calculated in this EEG report) is appropriate. Note the approximate and true means of the 16 component distributions (see Table A1-1). If one compares the first two (most important) sets of values, the means differ by only 1-1/2% and 1%. The standard errors differ by 21% and 13%. These differences are not expected to affect the final results by a significant amount. Indeed the difference between the calculated failure rates of the brake system (true vs. approximate) is only 5%. However one should note that the true values are greater than the approximate ones.

It is to be noted that calculations based on point estimates alone, as done by DOE in WCAP-13800 (WEC-WID, 1994), do not permit a determination of the level of confidence to be ascribed to the quantitative results.

Finally, we emphasize the importance of the preoperational checks of the entire hoist system at the start of each shift, that allowed for mission times of twelve hours for standby components. This choice of mission times for these important components made possible the value of  $1.3 \times 10^{-7}$  for the mean annual failure rate of the brake system.

## REFERENCES

- Aitchison, J. and Brown, J.A.C., 1969. The lognormal distribution. Cambridge University Press, NY, NY.
- Banz, I., Buchberger, S.G., and Rasmussen, D.G., 1985. Probability of a catastrophic hoist accident at the Waste Isolation Pilot Plant. WTSD-TME-063, Westinghouse Electric Corporation.
- Chan, J.K.K., Iacovino, J.M. and Maher, S.T., 1987. "Quantitative fault tree analysis of the Waste Isolation Pilot Plant waste hoist hydraulic brake system." Section 6 in Operation Readiness Review, Final Draft (unpublished draft), V. 2. 1988, DOE/WIPP-88-022, Westinghouse Electric Corporation.
- Denson, W., Chandler, G., Crowell, W. and Wanner, R., 1991. Nonelectronic Parts Reliability Data. NPRD-91, Griffis A.F.B., NY.
- Denson, W., Chandler, G., Crowell, W., Clark, A. and Jaworski, P., 1994. Nonelectronic Parts Reliability data. NPRD-95, Griffis A.F.B., NY.
- Greenfield, Moses A., 1990. Probabilities of a catastrophic waste hoist accident at the Waste Isolation Pilot Plant. EEG-44, Environmental Evaluation Group.
- Greenfield, M.A. and Sargent, T.J., 1993. A probabilistic analysis of a catastrophic transuranic waste hoist accident at the Waste Isolation Pilot Plant. EEG-53, Environmental Evaluation Group.
- Reliability Analysis Center, Rome Air Development Center, 1981. Nonelectric Parts Reliability Data, NPRD-2, Griffis A.F.B., NY.
- Rossi, M.J., 1985. Nonelectronic Parts Reliability Data. NPRD-3, Griffis A.F.B., NY.
- U.S. Department of Energy, 1987. Unusual Occurrence Report 8/11/87 involving the waste handling hoist. UOR:87:003.
- U.S. Department of Energy, Albuquerque Operations Office, 1990. WIPP Integrated Risk Assessment, Vol. II, Section 4.3. DOE/WIPP-89-010.
- Westinghouse Electric Corporation, Waste Isolation Division, 1987. Uncontrolled Movement of Waste Hoist, Investigation Report, July 25, 1987, Class "C" Investigation, Final Report.

Westinghouse Electric Corporation, Waste Isolation Division, 1990. Final Safety Analysis Report, Volume III, Chapter 7, Appendix 7B. WP 02-9, Rev. 0, Westinghouse Electric Corporation.

Westinghouse Electric Corporation, Waste Isolation Division, 1994. Waste Isolation Pilot Plant, Waste Hoist Brake System Analysis (preliminary draft report). WCAP-13800, Westinghouse Electric Corporation.

## LIST OF ACRONYMS

CDF	Cumulative Distribution Function
Com	Commercial quality parts
DOE	Department of Energy
EEG	Environmental Evaluation Group
EP	Event Probability
FSAR	Final Safety Analysis Report
GF	Group fixed
IEEE	Institute of Electrical and Electronics Engineers
IRA	Integrated Risk Assessment
Mil	Parts procured in accordance with military specifications
NPRD	Nonelectronic Parts Reliability Data
QA	Quality assurance
Ref	Reference Number
TRU	Transuranic
Unk	Data from a device of unknown quality level
UOR	Unusual Occurrence Report
WEC	Westinghouse Electric Corporation
WID	Waste Isolation Division
WIPP	Waste Isolation Pilot Plant

## **APPENDICES**

## Appendix 1

We model the failure distribution as a random variable that is a grand sum of 16 lognormal random variables. To compute an approximation to the distribution of this grand sum, we use Fast Fourier Transforms to implement the calculus of characteristic functions.

Our computational methods rest on the following theorems.<sup>1</sup>

**Theorem A.1:** Let  $x$  be a continuously distributed random variable with density  $f(x)$ , and let  $y$  be a continuously distributed random variable with density  $g(y)$ . Let  $x$  and  $y$  be independently distributed. Then the random variable  $z = x+y$  is distributed with density  $h(z)$  given by the *convolution* of  $f$  and  $g$ , which is defined by

$$h(z) = \int f(u)g(z-u)du.$$

We use the discrete random variable version of the preceding theorem, namely:

**Theorem A.2:** Let  $x$  be a discrete random variable that takes values on the set  $X = [x_0, x_1, \dots, x_{T-1}]$ , with density given by  $f_i = \text{Prob}[x = x_i]$ . Let  $y$  be a discrete random variable that takes values on the *same* set  $X$ , with density given by  $g_i = \text{Prob}[y = x_i]$ . Let  $z$  be the discrete random variable  $z = x+y$ , and let  $x$  and  $y$  be distributed independently. Then  $z$  has density  $h$  determined by

$$h_i = \sum_k f_k g_{i-k},$$

where  $h_i = \text{Prob}[z = z_i]$ , and where  $z$  resides in the discrete set  $Z = [2x_0, \dots, 2x_{T-1}]$ .

---

<sup>1</sup> The mathematical theorems we quote reside in many books on operational mathematics. For example, see R.A. Gabel and R.A. Roberts, *Signals and Linear Systems*, Wiley, 1973. For statistical background, see Bernard Lindren, *Statistical Theory*, Third Edition, MacMillan Publishers, 1976; p. 454.



*Fourier transform* methods manipulate sequences defined by:

**Definition D.1** The *Fourier transform* of a sequence  $\{x_t\}_{t=0}^{T-1}$  is defined as the sequence of complex numbers  $x(\omega_j)$  determined by the following equation:

$$(1) \quad x(\omega_j) = \sum_{t=0}^{T-1} x_t e^{-i\omega_j t}$$

where  $\omega_j = 2\pi j/T$  and  $j = 0, 1, \dots, T-1$ .

**Definition D.2** The *inverse Fourier transform* is given by

$$(2) \quad x_t = T^{-1} \sum_{j=0}^{T-1} x(\omega_j) e^{i\omega_j t}$$

Equations (1) and (2) define the basic Fourier transform pair.

The utility of Fourier transforms for our purposes stems from the following 'convolution theorem':

**Theorem A.3:** The Fourier transform of the convolution of two sequences  $\{x_t\}$  and  $\{y_t\}$  is the *product* of their Fourier transforms  $x(\omega_j) y(\omega_j)$ .

### Computational methods

We put down a discrete 'grid' of points  $X = [x_0, \dots, x_{T-1}]$  on the real line, with the points spaced close enough together and over a sufficiently large set to approximate each continuous distribution well. Then we generated approximating discrete probability distributions for each of the 16 lognormal random variates in our grand sum. We used the *same* grid for each of the 16 random variables. We chose the grid carefully to make sure that each random variable as well as the

relevant sums were well approximated by the procedure. For each approximating distribution  $\hat{f}_{k_t}, k=1, \dots, 16$ , we computed the Fourier transform  $f_k(\omega_j)$ . Then we computed the Fourier transform of  $\{\hat{h}\}$ , the approximating distribution of the grand sum, as

$$h(\omega_j) = \prod_{k=1}^{16} f_k(\omega_j)$$

To compute the approximate density of the grand sum  $\hat{h}_t$ , we inverse Fourier transformed  $h(\omega_j)$ :

$$\hat{h}_t = T^{-1} \sum_{j=0}^{T-1} h(\omega_j) e^{i\omega_j t}$$

We implemented these calculations using the *Fast Fourier Transform (FFT)* and the associated inverse transform, the *IFFT*, in the computer language *MATLAB* on a *SUN Sparc 10-40 Workstation*.

### Checks on approximation

The principal computational difficulty is caused by the different locations and dispersions of our 16 lognormal distributions. Several of the distributions have such large  $(\mu, \sigma)$  that, in light of the fat-tailed character of the lognormal distribution, we want to extend our grid over a large interval. Our methods require that grid points be equispaced, so that for a grid of given dimension, the need to have a large grid forces us to accept a coarser mesh. We used the grid  $[.025 : .15 : 120000]$  (i.e., a grid with 800000 points extending from 0.25 to 120000, in steps of .15).<sup>2</sup>

---

<sup>2</sup> Each time a convolution is computed, the FFT in effect *truncates* the grid on which the relevant sum is distributed, and restricts it to the same domain on which the original two distributions are defined. Thus, the density of a sum was computed only on the *same* domain  $X = [x_0, x_1, \dots, x_{T-1}]$ , rather than on the true domain  $Z = [2x_0, \dots, 2x_{T-1}]$ . We selected the grid set  $X$  to assure that it covers the region where the pertinent sums have appreciable positive probability.

The mean and variance of a sum of independent random variables are the sums of their means and variances, respectively, which means that we can compute the mean and variance of the distribution of the grand sum analytically. We compared the true mean and variance with means and variances of our approximating distributions: for the grand total of the sixteen random variables, the approximating mean, true mean, approximating standard error, and true standard error, respectively, are: 130.0014, 137.4896, 680.0873, 970.0158. The approximate distribution has a smaller mean and lower standard deviation than the true one.

For further diagnosis of sources of approximation error, we compare the true means and variances with the means and variances of the approximating discrete distributions for each of our 16 component distributions. In the table below, we record, respectively, the approximate mean, the *true* mean, the approximate standard error, and the *true* standard error, without the factor ( $10^{-9}$ ).

<u>Approx. Mean</u>	<u>True Mean</u>	<u>Approx. Std. Error</u>	<u>True Std. Error</u>
74.1987	75.3736	559.1946	711.1104
29.1852	30.1371	246.2159	284.3278
15.7594	18.8924	282.7848	551.8288
5.3794	6.7894	119.8095	198.3113
1.4084	1.8000	37.6411	52.5749
0.6848	0.9500	7.5619	8.9632
0.6848	0.9500	7.5619	8.9632
0.5613	0.4735	28.1444	42.6164
0.5613	0.4735	28.1444	42.6164
0.5613	0.4735	28.1444	42.6164
0.5613	0.4735	28.1444	42.6164
0.2385	0.2267	6.2719	6.6216
0.2467	0.1434	12.0803	12.9053
0.2467	0.1434	12.0803	12.9053
0.0916	0.0949	0.8320	0.8951
0.0916	0.0949	0.8320	0.8951



ENVIRONMENTAL EVALUATION GROUP

AN EQUAL OPPORTUNITY / AFFIRMATIVE ACTION EMPLOYER

505 NORTH MAIN STREET  
POST OFFICE BOX 3149  
CARLSBAD, NEW MEXICO 88221-3149  
(505) 885-9675  
FAX (505) 887-0243

**MEMORANDUM**

**DATE:** August 31, 1994  
**TO:** Robert H. Neill, Director  
**FROM:** Jim W. Kenney *(Jim W. Kenney)*  
**SUBJECT:** WIPP Hoist Preoperational Check

The WIPP waste hoist log (copy enclosed) indicates that among other items, the following operational checks are performed at the beginning of each shift:

1. Hoist Brakes
2. Overwinds and Underwinds
3. Brakes Clutches and Interlocks and Depth Indicators

Dr. Greenfield's August 24, 1994 letter ask for confirmation that the emergency dump valves 52.1 and 52.2, as well as, relays MXX and MXE are tested as part of the preoperational test. I spoke with WID engineer Norm Siepel after observing the hoist log and determined that the emergency dump valves above are tested as a part of the "hoist brakes" test (#1 above). Relays MXE and MXX are tested during the "overwinds and underwinds" test (#2 above). These test are conducted at the beginning of each hoist shift, nominally 8 hours. The 12 hour frequency is actually a worst case frequency and occurs only when a hoist operator is held over and works for 12 not eight hours.

I will continue to monitor the hoist log to verify that the hoist checks are being done as described by WID. Let me know if you or Dr. Greenfield have further questions or need additional information.

JK:rb  
Enclosure

### Appendix 3

The authors of EEG-53 (Greenfield and Sargent 1993) used an exact method, though somewhat complex, to compute the probability distributions in that report. Clearly it was desirable to have some independent check on these calculations. Fortunately an opportunity arose to accomplish such a check. Professor Theodore Harris of the University of Southern California, an expert in the theory of probability, was interested in EEG-53 as an example for his students of the applications of probability to real problems in the world. For the benefit of his students Professor Harris decided to check one of the calculations using his own methods. He chose for his example, "Sensitivity Case I" (see Table 1, page 3, EEG-53), a scenario also described in an unpublished report by Chan, et al., 1987. The following has been prepared by Professor Harris:

#### "5. THE PROBABILITY OF A CATASTROPHIC NUCLEAR WASTE HOIST ACCIDENT

REFERENCE. [1] Moses A. Greenfield and Thomas J. Sargent, "A probabilistic analysis of a catastrophic transuranic waste hoist accident at the WIPP [Waste Isolation Pilot Plant]", written from the Environmental Evaluation Group, an agency of the State of New Mexico. I wish to thank Dr. Greenfield for much additional discussion about the problem.

The analysis in [1] was made for a particular machine designed to hoist nuclear waste. A "catastrophic" accident is one where all three of three possible modes of failure occur. Assuming that the three modes of failure are independent, the probability under consideration is

$$(1) P = P_1 P_2 P_3,$$

where  $P_1$  is the annual probability of an electric power failure,  $P_2$  the annual probability of component failure due to valve malfunctions and human errors, and  $P_3$  is the annual probability of failure of a different kind of valve, a "dump" valve. Prior estimates had been given for these probabilities. It is assumed, for at least part of the analysis, that  $P_1 = .0776$ . The basic

thesis of [1] is that the estimates of  $P_2$  and  $P_3$  should recognize that the values of the estimates are subject to uncertainties.

The uncertainty might be treated by using confidence intervals. A related procedure, used in [1], is to treat  $P_2$  and  $P_3$  as random variables. This would be true, for example, if the various components determining  $P_2$  and  $P_3$  were subject to chance deviations in their manufacture.

The main tool is the LOGNORMAL distribution. If  $X$  is a normal RV (random variable) with mean  $\mu$  and standard deviation  $\sigma$ , then  $e^X$ , denoted by  $Y$ , is called LOGNORMAL. We will say that  $Y$  has the PARAMETERS  $\mu$  and  $\sigma$ . Also:

$$(2) \quad E(Y) = e^{\mu + .5\sigma^2}, \text{ Var}(Y) = e^{2\mu + \sigma^2}(e^{\sigma^2} - 1), \text{ median}(Y) = e^\mu.$$

Since  $P_1$  is taken as known, the task is to study  $P_2P_3$ . A detailed analysis made in [1], based on assumptions given there, shows that  $P_2P_3$  is  $10^8$  multiplied by a SUM of 4 independent lognormal RV's, which we will call  $Y_1, Y_2, Y_3,$  and  $Y_4$ . (The factor  $10^8$  is introduced for computing convenience.) The task is to evaluate the probability distribution of the sum

$$(3) \quad Z = (Y_1 + Y_2 + Y_3 + Y_4).$$

The evaluation is carried out in [1] using techniques that are too advanced to discuss here. However, we will partly verify the calculation in [1] by the "Monte Carlo" method, which can often be applied to difficult problems. Generally speaking, it is best to use the exact methods of [1] if we can, but the Monte Carlo method (sometimes called "simulation") is often useful when exact methods are not feasible. Since the Monte Carlo estimates are based on an experiment involving random quantities, the answer is subject to chance variations, which

however will be small if we average the results of sufficiently many independent runs of our simulation.

The basic idea is this. There are computer routines for producing a standard normal RV  $W$ . Then  $\mu + \sigma W$  is normal with mean  $\mu$  and variance  $\sigma^2$ . Hence  $\exp(\mu + \sigma W)$  is lognormal with parameters,  $\mu$  and  $\sigma$ . ( $\exp(z)$  is often used to denote  $e^z$ .)

The  $Y$ 's for our application have the following parameters, taken from [1].

TABLE A3-1: VALUES OF  $\mu$  AND  $\sigma$

	$\mu$	$\sigma$
$Y_1$	3.8610	1.1917
$Y_2$	3.1705	1.1917
$Y_3$	3.5430	1.6201
$Y_4$	3.5430	1.6201

If  $X_1, X_2, X_3,$  and  $X_4$  are independent standard normal RV's we obtain a sum of 4 independent lognormal RV's with the desired parameters by writing

$$(4) \quad Z = \exp\{3.8610 + 1.1917 X_1\} + \exp\{3.1705 + 1.1917 X_2\} \\ + \exp\{3.5430 + 1.6201 X_3\} + \exp\{3.5430 + 1.6201 X_4\}.$$

Using some calculus we find that  $E(Z) = 401.95$ . However, it is much harder to find the distribution function of  $Z$ .

A fast computer can produce a large number of independent sets of 4  $X$ 's in a short time. Using GW BASIC with the random seed 9875, we get 10,000 independent values of the RV  $Z$ , say  $Z_1, Z_2, \dots$ . Let  $F(r)$  be the fraction of these values that are  $\leq r$ . ( $F$  is what is called

the EMPIRICAL DISTRIBUTION FUNCTION for this experiment.) For example, 8443 of the computer generated Z's were  $\leq 600$ , so  $F(600) = .8443$ . Here is the table:

r =	100	200	300	400	500	600	700	800	900	1000	1500	2000	2500	3000	3500
F(r)	.13	.40	.59	.71	.79	.84	.88	.90	.92	.93	.97	.98	.99		

The ESTIMATED MEAN of Z is  $\sum Z_i / 10,000 = 408.1$ , as compared with the true value 401.95.

According to the calculations in [1], the 90-percentile for Z, that is, the value of r such that  $P\{Z \leq r\} = .9$ , is 794.5. To compare with our experiment, we counted the number of values of Z that were  $\leq 794.5$ . This was 9014. In other words, our empirical value  $F(794.5)$  is .9014, which is quite close to the ideal value of .90, based on [1].

Noting that  $P = P_1 P_2 P_3 = .0776 \times 10^{-8} \times Z$ , we see that

(5) The prob that P is  $\leq 0.617 \times 10^{-6} = \text{Prob}\{Z \leq 794.5\} = .9$ .

That is, under our assumptions, we are 90% sure that the quantity P is  $\leq 0.617 \times 10^{-6}$ ."

The above concludes Professor Harris' calculations.

Note that the Harris value for P of  $0.617 \times 10^{-6}$  agrees with the value of P at the 90 percentile listed in Table 7, page 20 of EEG-53.

Now we can compare Harris' table for his F(r) and r with the values of P and Percentile listed in Table 7, and with the graph of these values in Figure 3, page 21 of EEG-53.

To make Harris' notation consistent with EEG-53 multiply his "r" by  $0.0776 (= P_1) \times 10^{-8}$ ; i.e.  $0.0776 \times 10^{-8} r = P$ . Also multiply F(r) by 100 to obtain percentiles; i.e.  $100 \times F(r) = \text{Percentile}$ .



One may rewrite the Harris table as follows:

TABLE A3-2: VALUES OF PROBABILITY (P)  
VS. PERCENTILES

100xF(r) (= Percentile)	0.0776r (= 10 <sup>6</sup> P)
13	7.8
40	15.5
59	23.3
71	31.0
79	38.8
84	46.6
88	54.3
90	62.1
92	69.8
93	77.6
97	116.4
98	155.
99	194.

The Harris values for P (Probability) and the Percentiles may now be compared with those computed in EEG-53. This was done by plotting the Harris coordinates on Figure 3, page 21, EEG-53, and the results are shown in the Figure A3-1 of this Appendix. The agreement is excellent.

