EEG-65

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

Moses A. Greenfield
Thomas J. Sargent

Environmental Evaluation Group
New Mexico

January 1998

DOE/AL/58309-65

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

January 1998

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-AC04-89AL58309. 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.

Robert H Neill

Robert H. Neill
Director

EEG STAFF

Sally C. Ballard, B.S., Radiochemist
William T. Bartlett, Ph.D., Health Physicist
Radene Bradley, Secretary III
James K. Channell, Ph.D., Environmental Engineer/Health Physicist
Lokesh Chaturvedi, Ph.D., Deputy Director & Engineering Geologist
Thomas M. Clemo, Ph.D., 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
Robert H. Neill, M.S., Director
Dale Rucker, M.S., Performance Assessment Engineer
Jill Shortencarier, Executive Assistant
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 expert typing of the manuscript. We are grateful to Betsy Kraus for careful editing which clarified the text. We thank our colleague Robert H. Neill for helpful suggestions. We also thank our colleagues Matthew K. Silva, Lokesh Chaturvedi and Ben A. Walker for helpful reviews and suggestions.

TABLE OF CONTENTS

LIST OF TABLES

SUMMARY

In its most recent report on the annual probability of failure of the waste hoist brake system at the Waste Isolation Pilot Plant (WIPP) (Westinghouse 1996) the annual failure rate is calculated to be 1.3E (-7)(1/yr), rounded off from 1.32E(-7). This report replaces a previous one (Westinghouse 1994). The new report used updated data from NPRD-95, the older one used data from the previously published NPRD-91. A calculation by the Environmental Evaluation Group (EEG) produces a result that is about 4% higher, namely 1.37E(-7)(1/yr). The difference is due to a minor error in the U.S. Department of Energy (DOE) calculations in the Westinghouse 1996 report.

Deep geologic disposal of 175,000 cubic meters of transuranic waste at a depth of 650 meters in the WIPP requires 35 year hoist operations. WIPP's hoist safety relies on a braking system consisting of a number of components including two crucial valves. The failure rate of the system needs to be recalculated periodically to accommodate new information on component failure, changes in maintenance and inspection schedules, occasional incidents such as a hoist traveling out-of-control, either up or down, and changes in the design of the brake system. This report examines DOE's last two reports on the redesigned waste hoist system. In its calculations, the DOE has accepted one EEG recommendation and is using more current information about the component failure rates, the Nonelectronic Parts Reliability Data (NPRD). However, the DOE calculations fail to include the data uncertainties which are described in detail in the NPRD reports. As previously noted by EEG, the U.S. Nuclear Regulatory Commission (NRC) recommended that a system evaluation include mean estimates of component failure rates and "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." EEG has made this suggestion previously and the DOE has indicated why it does not accept the NRC recommendation. Hence, this EEG report illustrates the importance of including data uncertainty using a simple statistical example.

I. HISTORICAL REVIEW

The Department of Energy (DOE) has continued to improve the design and operation of the waste hoist brake system at the Waste Isolation Pilot Plant (WIPP) culminating in a design fully described in a recent report: a Revised Design, WCAP-13800 (Westinghouse 1994). Component failure data for the report were taken from NPRD-91 (Denson et al. 1991). However shortly after publication of the Revised Design an updating of component failure data became available in the newly published NPRD-95 (Denson et al. 1994). DOE then made an additional analysis based on the updated component failure rates and published a new report, WIPP/WID-96-2178, Rev. 0 (Westinghouse 1996). This report is a review of the recent report by the DOE (Westinghouse 1996).

Table 1A summarizes the various reports published by DOE dealing with the safety of the waste hoist brake system at WIPP, covering the years from 1985 to 1996. EEG has published a number of reports analyzing the DOE work (listed in Table 1A), and these reports are listed in Table 1B.

TABLE 1A. 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.	3.7×10^{-7} (1/yr)
Base case	Chan et al. 1987; Section 6 in ORR, DOE/WIPP-88-022, V. 2, 1988 (Unpublished Draft)	2.7×10^{-2} (1/yr)
Sensitivity Case 1	Chan et al. Dec. 1987; (Unpublished Draft)	1.5×10^{-6} (1/yr)
Design Option B-2	FSAR, App 7B, 1990. WP02-9, Rev. 0, Westinghouse Electric Corporation	2.2×10^{-7} (1/yr)
Revised Design	WCAP-13800, February 1994 (Preliminary Draft Report)	1.3×10^{-7} (1/yr)
Revised Design	WIPP/WID-96-2178, Rev. 0, July 1996	1.3×10^{-7} (1/yr)

TABLE 1B. EEG REPORTS ON WASTE HOIST BRAKE SYSTEM AT WIPP

Report	Cases Analyzed
EEG-44 (Greenfield 1990)	Generic Case, 1985 Base Case, 1987 (Unpublished Draft) Sensitivity Case 1, 1987 (Unpublished Draft)
EEG-53 (Greenfield and Sargent 1993)	Design Option B-2, 1990
EEG-59 (Greenfield and Sargent 1995)	Revised Design, 1994 (Preliminary Draft Report)
EEG-65 (Greenfield and Sargent 1997)	Revised Design, 1996 (Rev. 0)

II. DATA SOURCES

The authors of the Westinghouse 1994 report, WCAP-13800, used the NPRD series for component failure data. They used the NPRD-91 (Denson et al. 1991) which was the latest NPRD available in February 1994. However, NPRD-95 (Denson et al. 1994) was published in July 1994. Most of the failure data in NPRD-91 (Denson et al. 1991) used in WCAP-13800, are unchanged from those listed in NPRD-95. 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, which are key components in WCAP-13800. Information about the differences between NPRD-91 and NPRD-95 (Denson et al. 1991, 1994), is contained in EEG-59 (Greenfield and Sargent 1995), and analyses were based on both sets of data for comparison purposes. It was appropriate for DOE to use the newer data in NPRD-95 (Denson et al. 1994) for their latest report, WIPP/WID-96-2178 (Westinghouse 1996).

There is an interesting and brief allusion in the Executive Summary of the Westinghouse 1996 report (page iv) to a change in data sources from the Option B-2 design (Westinghouse 1990) to that of the revised design (Westinghouse 1994). The following is a quotation from the Executive Summary:

> "The results of this reanalysis (as reported in February 1994) show the bottom line reliability of the Waste Hoist Brake System is slightly better than the earlier Option B-2 design. The annual probability of failure of the revised design is 1.3 x 10^{-7} (1/yr). By comparison, the annual probability of failure of option B-2 is 2.2 x 10^{-7} (1/yr). Our review clearly shows that the February 1994 revised design is a more robust, safer design. System failure is dominated by common cause failure due to blockage of two emergency dump valves. However, these improvements are somewhat offset by the use of much more conservative reliability data. The present analysis using NPRD-95 failure rates provides a probability of failure of 1.3 x 10^{-7} (1/yr), which is on the same order of magnitude as the February 1994 analysis."

The above quotation gives no information about the nature of the change to "much more conservative reliability data."

The need to improve the sources of failure data used in the Option B-2 design (Westinghouse 1990) was discussed in the EEG-53 (Greenfield and Sargent 1993). The recommendations in EEG-53 (Greenfield and Sargent 1993, XV) urged the DOE to obtain more current information about a certain crucial valve type. It also recommended the use of the later source, NPRD-3 (Rossi 1985), published in 1985, rather than the earlier NPRD-2 (Reliability 1981), published in 1981, which had been used by DOE in the report on Option B-2 (Westinghouse 1990).

Neither the 1994 nor the 1996 DOE (Westinghouse 1994, 1996) report reference the discussion of data sources contained in the EEG reports of 1993 and 1995.

III. ERRORS IN CALCULATIONS

A. Cutset Probability Calculations

Pages A3-4 through A3-17 in WIPP/WID-96-2178 (Westinghouse 1996) contain the detailed calculations of the cutset probabilities based on the recent NPRD-95 (Denson et al. 1994) data. Similarly pages A3-22, etc. contain the calculations for the Westinghouse 1994 case based on NPRD-91 (Denson et al. 1991). An error was made in the listings of the event probabilities (EP) for the Westinghouse 1996 case. The latter are listed inappropriately as a repetition of the values for the Westinghouse 1994 case; e.g. if one multiplies (for Number 1) 2.40 E(-3) by 2.88 E(-5) (see page A3-4), one obtains 6.91 E(-8). This is the number that is appropriate for page A3-22 (Number 1) as the cutset probability. The corresponding value of the cutset probability (Number 1) for the Westinghouse 1996 case is listed on page A3-4 as 7.20 E(-8). Is this number correct, and where does it come from? This matter was checked by preparing a detailed calculation for the Westinghouse 1996 case, using the data from the Westinghouse 1996 report. Table 2 shows this calculation, for cases Number 1 through Number 16. Comparison with the values on page A3-4 shows that there is agreement for the cutset probabilities listed there.

TABLE 2. CORRECTED CALCULATION OF CUTSET PROBABILITIES

July 1996 - Rev. 0

Number	Ref. No.	Failure Rate A3-2 (1/hr)	Mission Time (hr)	EP (corrected) A3-4	Cutset Prob. A3-4
1 a	074	2.5 E(-6)	10^3	2.5 (E-3)	7.20 E(-8)
b	087	2.4 E(-6)	12	2.88 E(-5)	
2 a	064	1.0 E(-6)	10^3	1.0 E(-3)	2.88 E(-8)
b	087	2.4 E(-6)	12	2.88 E(-5)	
3 a	071	2.5 E(-5)	10^3	2.5 E(-2)	1.80 E(-8)
b	087	2.4 E(-6)	12	2.88 E(-5)	
c	071	2.5 E(-5)	10^3	2.5 E(-2)	
4 a	056	3.0 E(-5)	10^3	3.0 E(-2)	6.57 E(-9)
b	077	7.6 E(-6)	10^3	7.6 E(-3)	
c	087	2.4 E(-6)	12	2.88 E(-5)	
5 a	059	7.9 E(-6)	10^3	7.9 E(-3)	1.73 E(-9)
b	077	7.6 E(-6)	10^3	7.6 E(-3)	
c	087	2.4 E(-6)	12	2.88 E(-5)	
6 a	067	2.6 E(-6)	12	3.12 E(-5)	9.73 E(-10)
b	067	2.6 E(-6)	12	3.12 E(-5)	
7 a	067	2.6 E(-6)	12	3.12 E(-5)	9.73 E(-10)
b	067	2.6 E(-6)	12	3.12 E(-5)	
8 a	071	2.5 E(-5)	10^3	2.5 E(-2)	4.50 E(-10)
b	087	2.4 E(-6)	12	2.88 E(-5)	
c	050	2.5 E(-5)	10^3	2.5 E(-2)	
d	071	2.5 E(-5)	10^3	2.5 E(-2)	
9 a	071	2.5 E(-5)	10^3	2.5 E(-2)	4.50 E(-10)
b	087	2.4 E(-6)	12	2.88 E(-5)	
c	050	2.5 E(-5)	10^3	2.5 E(-2)	
d	050	2.5 E(-5)	10^3	2.5 E(-2)	

TABLE 2. CORRECTED CALCULATION OF CUTSET PROBABILITIES (continued)
July 1996 - Rev. 0

Number	Ref. No.	Failure Rate A3-2 (1/hr)	Mission Time (hr)	EP (corrected) A3-4	Cutset Prob. A3-4
10 a	050	2.5 E(-5)	10^3	2.5 E(-2)	4.50 E(-10)
b	071	2.5 E(-5)	10^3	2.5 E(-2)	
c	087	2.4 E(-6)	12	2.88 E(-5)	
d	071	2.5 E(-5)	10^3	2.5 E(-2)	
11 a	050	2.5 E(-5)	10^3	2.5 E(-2)	4.50 E(-10)
b	050	2.5 E(-5)	10^3	2.5 E(-2)	
c	087	2.4 E(-6)	12	2.88 E(-5)	
d	071	2.5 E(-5)	10^3	2.5 E(-2)	
12 a	074	2.5 E(-6)	10^3	2.5 E(-3)	2.25 E(-10)
b	051	2.5 E(-5)	12	3.0 E(-4)	
c	051	2.5 E(-5)	12	3.0 E(-4)	
13 a	071	2.5 E(-5)	10^3	2.5 E(-2)	1.37 E(-10)
b	087	2.4 E(-6)	12	2.88 E(-5)	
c	050	2.5 E(-5)	10^3	2.5 E(-2)	
d	077	7.6 E(-6)	10^3	7.6 E(-3)	
14 a	050	2.5 E(-5)	10^3	2.5 E(-2)	1.37 E(-10)
b	077	7.6 E(-6)	10^3	7.6 E(-3)	
c	087	2.4 E(-6)	12	2.88 E(-5)	
d	071	2.5 E(-5)	10^3	2.5 E(-2)	
15 a	067	2.6 E(-6)	12	3.12 E(-5)	9.73 E(-11)
b	072	2.6 E(-7)	12	3.12 E(-6)	
16 a	067	2.6 E(-6)	12	3.12 E(-5)	9.73 E(-11)
b	072	2.6 E(-7)	12	3.12 E(-6)	

$$\sum_{1}^{16} \textit{Cutset Prob}\ (\text{A3-4}) = 1.315\ \text{E}(-7)$$

B. Common Cause Calculations for Emergency Dump Valves

In the calculation of the value of the failure rate due to common cause one uses the equation for the two emergency dump valves (failing to de-energize) shown on page A5-22 (Westinghouse 1996):

$$P_{cc} = \beta Q;\ \beta = 0.1$$

Q is the failure rate for the emergency dump valve. What is its value? The NPRD-91 (Denson et al. 1991) listed value is 2.4 E(-5)* (1/hr); the NPRD-95 (Denson et al. 1994) listed value is 2.5 E(-5)* (1/hr), a small increase of about 4%. DOE incorrectly used the NPRD-91 (Denson et al. 1991) value in the common cause calculation; see page A5-22, and also page A3-2 (reference no. 087). As a check, a review was made of the value for Q used to denote single failure of either of the dump valves (reference no. 051). On page A3-2 (Westinghouse 1996) the value listed for "051" is indeed the correct one of 2.5 E(-5) (1/hr), from page 2-230 of NPRD-95 (Denson et al. 1994). Also note page 3-2 of the Westinghouse 1996 report, Table 3.2-1, Updated Component and Common Cause Failure Rates. For Reference No. 051, "Dump valve fails to operate", the failure rate is listed correctly as 2.5 E(-5) (1/hr). A further check was made to note which failure rate produces the correct cutset probabilities. Reference No. "051" appears in Table 2 in Numbers 12b and 12c of this report. Note that the use of 2.5 E(-5) for Reference No. 051 produces the listed cutset probability, for Number 12, of 2.25 E(-10), in agreement with the listed cutset probability on page A3-4. The use of 2.4 E(-5) (1/hr) results in a 4% underestimate of a final failure probability value.

A final calculation is made of the cutset probabilities using the corrected failure rate for the emergency dump valves of 2.5 E(-5) in both Reference nos. "051" and "087" (see Table 3). These corrected values are then compared with the calculated values of the probabilities presented in EEG-59 (Greenfield and Sargent 1995), Table 9, pages 22 and 23, columns labeled "EP_{mean}".

*These are rounded values. The actually listed values in NPRD-91 (page 2-156) and in NPRD-95 (page 2-230) are respectively: 2.38627 and 2.50590; the change corresponds to an increase of 5%.

There is a final difference in the manner of calculation by DOE and EEG. DOE used the failure rates from NPRD-95 (Denson et al. 1994) listing only two significant figures; e.g. for Number 4a (Ref. No. 056) the listed NPRD-95 (Denson et al. 1994) value is 2.974 E(-5) (1/hr). This value is used "as is" by EEG. However DOE used 3.0 E(-5) (1/hr). This difference in usage produces "rounding-off" differences in the calculations between DOE and EEG.

Table 3 presents the comparison between the corrected DOE version and that in EEG-59 (Greenfield and Sargent 1995). The differences between the cutset probabilities are small, averaging $\pm 1\%$.

Note: only 16 terms are used above since that accounts for 99.4% of the total of 212 terms. The sum of the 16 terms in both the EEG and the corrected DOE columns is 1.37 E(-7). The sum of the first 16 terms in the DOE report (Westinghouse 1996), page A3-4, is 1.318 E(-7), about 4% less.

Further Note: In EEG-59 (Greenfield and Sargent 1995) the EP_{mean} values are then used to calculate μ_{ia}, μ_{ib} etc ($i = 1,2,......16$); also $\sigma_{ia} = \sigma_{ib} = \text{etc} = 1.5$. These values are then used to calculate

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

The μ_i and σ_i values (Table 11, page 25, Greenfield and Sargent 1995) are the parameters that appear in the lognormal distributions. They are then used to calculate the probability of failure, P, and the associated percentiles (Table 13, page 27). The methods used to compute the failure distribution functions are described in Appendix 1, pages 37-40.

TABLE 3. CORRECTED FAILURE RATE FOR DUMP VALVE OF 2.5 E(-5) (1/hr) USED IN REFERENCE NOS. 087 and 051:

Calculation of Cutset Probabilities
July 1996 - Rev. 0

Number	Ref. No.	Failure Rate A3-2 (1/hr)	EP, A3-4	Cut Prob. A3-4	EP, EEG-59	Cut Prob. EEG-59
1 a	074	2.5 E(-6)	2.5 E(-3)	7.50 E(-8)	2.506 E(-3)	7.54 E(-8)
b	087	2.5 E(-6)	3.0 E(-5)		3.007 E(-5)	
2 a	064	1.0 E(-6)	1.0 E(-3)	3.00 E(-8)	1.002 E(-3)	3.01 E(-8)
b	087	2.5 E(-6)	3.0 E(-5)		3.007 E(-5)	
3 a	071	2.5 E(-5)	2.5 E(-2)	1.875 E(-8)	2.506 E(-2)	1.89 E(-8)
b	087	2.5 E(-6)	3.0 E(-5)		3.007 E(-5)	
c	071	2.5 E (-5)	2.5 E(-2)		2.506 E(-2)	
4 a	056	3.0 E(-5)	3.0 E(-2)	6.84 E(-9)	2.974 E(-2)	6.79 E(-9)
b	077	7.6 E(-6)	7.6 E(-3)		7.588 E(-3)	
c	087	2.5 E(-6)	3.0 E(-5)		3.007 E(-5)	
5 a	059	7.9 E(-6)	7.9 E(-3)	1.801 E(-9)	7.883 E(-3)	1.80 E(-9)
b	077	7.6 E(-6)	7.6 E(-3)		7.588 E(-3)	
c	087	2.5 E(-6)	3.0 E(-5)		3.007 E(-5)	
6 a	067	2.6 E(-6)	3.12 E(-5)	9.73 E(-10)	3.082 E(-5)	9.50 E(-10)
b	067	2.6 E(-6)	3.12 E(-5)		3.082 E(-5)	
7 a	067	2.6 E(-6)	3.12 E(-5)	9.73 E(-10)	3.082 E(-5)	9.50 E(-10)
b	067	2.6 E(-6)	3.12 E(-5)		3.082 E(-5)	
8 a	071	2.5 E(-5)	2.5 E(-2)	4.69 E(-10)	2.506 E(-2)	4.73 E(-10)
b	087	2.5 E(-6)	3.0 E(-5)		3.007 E(-5)	
c	050	2.5 E(-5)	2.5 E(-2)		2.506 E(-2)	
d	071	2.5 E(-5)	2.5 E(-2)		2.506 E(-2)	
9 a	071	2.5 E(-5)	2.5 E(-2)	4.69 E(-10)	2.506 E(-2)	4.73 E(-10)
b	087	2.5 E(-6)	3.0 E(-5)		3.007 E(-5)	
c	050	2.5 E(-5)	2.5 E(-2)		2.506 E(-2)	
d	050	2.5 E(-5)	2.5 E(-2)		2.506 E(-2)	

TABLE 3 (continued). CORRECTED FAILURE RATE FOR DUMP VALVE OF <u>2.5 E(-5) (1/hr) USED IN REFERENCE NOS. 087 and 051:</u>

Calculation of Cutset Probabilities

July 1996 - Rev. 0

Number	Ref. No.	Failure Rate A3-2 (1/hr)	EP, A3-4	Cut Prob. A3-4	EP, EEG-59	Cut Prob EEG-59
10 a	050	2.5 E(-5)	2.5 E(-2)	4.69 E(-10)	2.506 E(-2)	4.73 E(-10)
b	071	2.5 E(-50	2.5 E(-2)		2.506 E(-2)	
c	087	2.5 E(-6)	3.0 E(-5)		3.007 E(-5)	
d	071	2.5 E(-5)	2.5 E(-2)		2.506 E(-2)	
11 a	050	2.5 E(-5)	2.5 E(-2)	4.69 E(-10)	2.506 E(-2)	4.73 E(-10)
b	050	2.5 E(-5)	2.5 E(-2)		2.506 E(-2)	
c	087	2.5 E(-6)	3.0 E(-5)		3.007 E(-5)	
d	071	2.5 E(-5)	2.5 E(-2)		2.506 E(-2)	
12 a	074	2.5 E(-6)	2.5 E(-3)	2.25 E(-10)	2.506 E(-3)	2.27 E(-10)
b	051	2.5 E(-5)	3.0 E(-4)		3.007 E(-4)	
c	051	2.5 E(-5)	3.0 E(-4)		3.007 E(-4)	
13 a	071	2.5 E(-5)	2.5 E(-2)	1.425 E(-10)	2.506 E(-2)	1.43 E(-10)
b	087	2.5 E(-6)	3.0 E(-5)		3.007 E(-5)	
c	050	2.5 E(-5)	2.5 E(-2)		2.506 E(-2)	
d	077	7.6 E(-6)	7.6 E(-3)		7.588 E(-3)	
14 a	050	2.5 E(-5)	2.5 E(-2)	1.425 E(-10)	2.506 E(-2)	1.43 E(-10)
b	077	7.6 E(-6)	7.6 E(-3)		7.588 E(-3)	
c	087	2.5 E(-6)	3.0 E(-5)		3.007 E(-5)	
d	071	2.5 E(-5)	2.5 E(-2)		2.506 E(-2)	
15 a	067	2.6 E(-6)	3.12 E(-5)	9.73 E(-11)	3.082 E(-5)	9.50 E(-11)
b	072	2.6 E(-7)	3.12 E(-6)		3.082 E(-6)	
16 a	067	2.6 E(-6)	3.12 E(-5)	9.73 E(-11)	3.082 E(-5)	9.50 E(-11)
b	072	2.6 E(-7)	3.12 E(-6)		3.082 E(-6)	

IV. USE OF CONFIDENCE LEVELS

EEG reports suggested following the recommendations 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." The quotation is taken from the Nuclear Regulatory Commission (NRC 1986). DOE has responded to these suggestions, and indicated why they do not accept them.

Nevertheless EEG once again makes the same recommendation. Both NPRD-91 and NPRD-95 (Denson et al. 1991, 1994) state that all the listed rates "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 (σ) = 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."

This is to state that if one wishes to include 90% of all the failure rates, one must include a range of values that somewhat exceeds two orders of magnitude $\left(\frac{11.9}{0.08} = 148+\right)$! Under these circumstances, representing the failure rate by a mean value alone disregards relevant information. It may be helpful to give a simple example that illustrates the need to include confidence bands around an observed mean value. Consider the following.

A coin is suspected to be unfair, by which we mean that the unknown probability of a heads $p \neq .5$. The ith flip of the coin yields outcome ξ_i where $\xi_i = 1$ if a head occurs, $\xi_i = 0$ if a tail occurs on the ith flip. Let n independent flips result in the fraction $\bar{\xi}_n = \frac{\sum_{i=1}^{n} \xi_i}{n}$ of heads. Because the random variable $n\bar{\xi}_n$ has a *binomial distribution*, we know that the mean and variance of $\bar{\xi}_n$ are p and $\frac{p(1-p)}{n}$, respectively. The usual estimator of p after n flips is $\hat{p}_n = \bar{\xi}_n$, with estimator of its standard error being $\frac{\hat{p}(1-\hat{p})}{n}$. For example, suppose that after n trials, we have estimated that $p = 0.7$. The standard errors around this estimate for $n = 5, 10, 20$ would be 0.205, 0.145, 0.1025. These standard errors measure our uncertainty about p after n trials. Notice that even after 20 trials, a one standard error confidence band around p shows us to remain pretty uncertain about the location of p. A beautiful property of the binomial distribution is that the central limit theorem cuts in quickly, giving us permission to use the Gaussian distribution to construct confidence intervals around our estimator.

The EEG reports worked with similar principles, but in more complex environment because the failure rates are likely to be governed by more hostile distributions than the kind binomial of the example. These distributions, especially the log normal, yield estimated failure probabilities that are distributed with fatter tails than exhibited in our little example. This observation increases the importance of handling estimated failure rates in ways that respect the uncertainty those measures revealed.

A closer examination of the present case, discussed in Westinghouse 1996 and in EEG 59 (Greenfield and Sargent 1995), will clarify the need to factor uncertainties into risk assessments.

The value for the annual probability of failure stated earlier in this report is a mean value. An omission in the DOE calculations is the lack of an estimate of the confidence level to be ascribed to the quantitative results, due to the large uncertainties that exist in the basic NPRD data (described in detail in the NPRD reports). This omission is contrary to the recommendations of the Nuclear Regulatory Commission (NRC 1986) that mean estimates "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."

The significance of this omission may be judged by noting the "uncertainty calculations" made in EEG-59 (Greenfield and Sargent 1995) for the same case. See Table 13, page 27. The mean value for the annual failure probability is 1.3E(-7). For the 90 percentile value the failure probability increases to 2.4E(-7) (i.e. the likelihood is 90 percent that the failure probability is 2.4E(-7) or less). For the 95 percentile the failure probability increases to 4.5E(-7). For the 99 percentile the failure probability exceeds E(-6), with the value increasing to 1.6E(-6)! This value exceeds the failure probability of 1.0E(-6), a desired target value.

How certain does DOE wish to be that the failure probability not exceed 1.0E(-6)? Thus it is reasonable to regard the omission in the DOE calculations of estimates of the confidence levels as a serious one.

The need to factor uncertainties into risk assessments based on a mean value has been discussed in recent scientific literature. An example is cited to illustrate some current thinking on this matter. In an article in *Science*, 1990, Leslie Roberts discusses this issue as it applies to the problem of risk assessment. He quotes from a paper by Adam Finkel (1990). The following is a quote from Roberts (1990): "The numbers are issued with startling precision: 90.3 deaths per million from exposure to, say, benzene. Partly based on these risk estimates, regulations are crafted and millions of dollars are spent. But the apparent precision in those numbers belies how fragile they really are, says Adam Finkel in a new report from Resources for the Future, Confronting Uncertainty in Risk Management. Finkel challenges federal agencies to change the way they assess chemical and other hazards. Finkel ... is simply asking the Environmental Protection Agency and other agencies to admit how squishy the numbers are and, more important, to factor this uncertainty into their risk assessments. What that would mean is that instead of providing a point estimate, the 90.3 deaths, risk analysts would provide a distribution of estimates, with some indication of the likelihood that each number is correct — for example, how confident the analyst is that the risk is greater than 20 deaths per year, and so on... . At EPA, officials were already thinking about how to incorporate uncertainty into risk analysis and are now looking closely at the report (by Finkel) and calling it 'very useful'."

In another article published in *Science* (1990) Professor George Apostolakis describes a methodology for using probability in the safety assessments of technological systems. At the conclusion of his paper he deplores the fact that a probabilistic "framework is not universally accepted". He believes that a possible reason is the "lack of a strong statistical background of most engineers." He then references an editorial published in *Science* (1989) by Nobel Laureate Arno Penzias, who does make a plea for engineers to receive more training in statistics.

V. RECOMMENDATIONS

1) After examining DOE's most recent two reports of the waste hoist brake system at WIPP (Westinghouse 1994, 1996), EEG concluded that the existing brake hoist system, recently redesigned and including all the operational caveats, is satisfactory. A redesign is not required.

2) There are a number of minor numerical errors in the most recent report (Westinghouse 1996) that are discussed in detail in this report. These errors should be corrected.

3) EEG reiterates its recommendation that DOE use probabilistic risk assessments so that account may be taken of the uncertainties in the basic data. This will permit ascribing levels of confidence to the quantitative results.

4) The approximate annual failure probability of the waste hoist brake system is 4.5×10^{-7} at a 95% confidence level; i.e. there is a 95% likelihood that the failure rate per annum is less than 4.5×10^{-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. This permits the use in calculations of a favorable 12 hours for the mission times of "standby components". The mission times of operating components are 1,000 hrs/yr, based on current operating experience of 7,000 round trips per year for the waste hoist. EEG endorses this system as predicated on the design criteria stated above. If changes are made, the calculations of the failure probabilities should be redone.

REFERENCES

Apostolakis, G. 1990. The concept of probability in safety assessments of technological systems. *Science* 250: 1360-1364.

Banz, I., S.G. Buchberger, and D.G. Rasmussen. 1985. Probability of a catastrophic hoist accident at the Waste Isolation Pilot Plant. WTSD-TME-063, Westinghouse Electric Corporation.

Chan, J.K.K., J.M. Iacovino, and S.T. Maher. 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., G. Chandler, W. Crowell, and R. Wanner. 1991. Nonelectronic Parts Reliability Data. NPRD-91, Griffis A.F.B., NY.

Denson, W., G. Chandler, W. Crowell, A. Clark, and P. Jaworski. 1994. Nonelectronic Parts Reliability Data. NPRD-95, Griffis A.F.B., NY.

Finkel, A.M. 1990. Confronting uncertainty in risk management: a guide for decision makers. Washington, D.C.: Resources for the Future.

Greenfield, M.A. 1990. Probabilities of a catastrophic waste hoist accident at the Waste Isolation Pilot Plant. EEG-44, Environmental Evaluation Group.

Greenfield, M.A. and T. J. Sargent. 1993. A probabilistic analysis of a catastrophic transuranic waste hoist accident at the Waste Isolation Pilot Plant. EEG-53, Environmental Evaluation Group.

Greenfield, M.A. and T. J. Sargent. 1995. An analysis of the annual probability of failure of the waste hoist brake system at the Waste Isolation Pilot Plant (WIPP). EEG-59, Environmental Evaluation Group.

Nuclear Regulatory Commission. 1986. 10 CFR 50. Safety Goals for the Operation of Nuclear Power Plants, Policy Statement, Correction and Republication. Federal Register (21 August) vol. 51, no. 162, p. 30028-30033.

Penzias, A. 1989. Teaching Statistics to Engineers. *Science* 244: 1025.

Reliability Analysis Center, Rome Air Development Center. 1981. Nonelectronic Parts Reliability Data. NPRD-2, Griffis A.F.B., NY.

Roberts, L. 1990. Risk Assessors Taken to Task. *Science* 247: 1173.

Rossi, M.J. 1985. Nonelectronic Parts Reliability Data. NPRD-3, Griffis A.F.B., NY.

U.S. Department of Energy, Albuquerque Operations Office. 1990. WIPP Integrated Risk Assessment, Vol. II, Section 4.3. DOE/WIPP-89-010, U. S. Department of Energy.

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.

Westinghouse Electric Corporation, Waste Isolation Division. 1996. Waste Isolation Pilot Plant, Waste Hoist Brake System Analysis. WIPP/WID-96-2178 Rev. 0, Westinghouse Pittsburgh Corporation.

LIST OF ACRONYMS

EEG	Environmental Evaluation Group
EP	Event Probabilities
NPRD	Nonelectronic Parts Reliability Data
NRC	Nuclear Regulatory Commission
DOE	United States Department of Energy
WID	Waste Isolation Division
WIPP	Waste Isolation Pilot Plant