WIPP Library

EEG-44

PROBABILITIES OF A CATASTROPHIC WASTE HOIST ACCIDENT AT THE WASTE ISOLATION PILOT PLANT

Moses A. Greenfield, Ph.D.

Environmental Evaluation Group
New Mexico

January 1990

900101

EEG-44
DOE/AL/58309-44

PROBABILITIES OF A CATASTROPHIC WASTE HOIST ACCIDENT AT THE WASTE ISOLATION PILOT PLANT

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

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

and

505 N. Main Street
Carlsbad, New Mexico 88221

January 1990

CONTENTS

TITLE	PAGE
Foreword	iii
Acknowledgments	iv
Staff	v
Summary	vi
1. INTRODUCTION	1
1.1 Waste Shaft and Hoist at WIPP	1
1.2 Probabilities of Catastrophic Failure	8
1.3 Banz et al (1985) Report: EEG Criticism, DOE Response	9
2. JULY 25, 1987 INCIDENT IN THE WIPP WASTE HOIST	13
3. SUMMARY OF THE CHAN et al (1987) REPORT	16
3.1 Hydraulic Brake System	16
3.2 Base Case Calculation	17
3.2.1 Scenarios with Component Failure, Loss of Electric Power, Human Error	17
3.2.2 Calculation of Human Error Probability	18
3.2.3 Component Failure Rates and Rate of Loss of Electric Power	19
3.2.4 Annual Probability of Brake System Failure	20
3.2.5 Annual Probability of a Catastrophic Accident	21
3.3 Sensitivity Case 1: Proposed Emergency Dump Valves	23
4. ANALYSIS OF THE CHAN et al (1987) REPORT	26
4.1 Frequency of Electric Power Failure	26
4.2 Human Error Probability (HEP)	30
4.3 Component Failure Rates	33
4.4 Summary of Correction Factors	36

5. CONCLUSIONS AND RECOMMENDATIONS..... 39
5.1 Conclusions..... 39
5.2 Recommendations..... 42

6. REFERENCES..... 43

7. APPENDICES
Appendix A: (a) December 2, 1985 Letter by R.H. Neill to W.R. Cooper; (b) Excerpts: EEG Comments on Risk of Catastrophic Hoist Accident at the Waste Isolation Pilot Plant..... 44
Appendix B: (a) December 20, 1985 Letter from W. R. Cooper to R.H. Neill; (b) Excerpts: Responses to EEG Comments on WTSD-TME-063, "Probability of a Catastrophic Hoist Accident at the Waste Isolation Pilot Plant"..... 45
Appendix C: (a) July 28, 1987 Letter from J.K. Channell to R.H. Neill, on "Unusual Occurrence with WIPP Waste Hoist"; (b) July 28, 1987 Letter from R.H. Neill to T. Bahr, et al..... 46
Appendix D: August 5, 1987 Letter from R.H. Neill to J. Tillman, DOE, "Unusual Occurrence in the WIPP Waste Hoist System"... 47
Appendix E: August 17, 1987 Letter from J. Tillman to R.H. Neill, including the UOR dated August 11, 1987 (UOR=Unusual Occurrence Report)..... 48
Appendix F: Ooctober 15, 1987 Abridged Version of Class C Investigation, "Uncontrolled Movement of Waste Hoist, July 25,1987"..... 49
Appendix G: Tables from Chan et al (1987) (a) Summary of Major Contributors to the Probability of a Catastrophic Accident-Base Case (Table 4.1-1, Chan et al, 1987); (b) Summary of Major Contributors to Brake System Failure - Base Case (Table 4.1-2, Chan et al, 1987)..... 50

FOREWORD

The purpose of the Environmental Evaluation Group (EEG) is to conduct an independent technical evaluation of the Waste Isolation Pilot Plant (WIPP) Project to ensure 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 permanent 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 provided for continued funding from DOE through Contract DE-AC04-89AL58309.

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 independent environmental monitoring of background radioactivity in air, water, and soil, both on-site and in surrounding communities.

Robert H. Neill
Director

ACKNOWLEDGEMENTS

Lokesh Chaturvedi, James K. Channell, Robert H. Neill and Marshall Little reviewed this report and made many valuable suggestions. Lynda S. Bartlett cheerfully typed and helped prepare the manuscript, and was most helpful. Carla Tafoya helped in the preparation of the illustrations. Laura Connolly edited the manuscript and insured clarity and precision in use of language. The author thanks these colleagues, and is alone responsible for any errors or oversights.

STAFF

Sally C. Ballard, B.S., Environmental Technician
Lynda S. Bartlett, B.A., Administrative Secretary
William T. Bartlett, Ph.D., Health Physicist
Radene Bradley, Secretary
James K. Channell, Ph.D., P.E., CHP, Sr. Environmental Engineer
Lokesh Chaturvedi, Ph.D., Deputy Director & Engineering Geologist
Laura H. Connolly, M.A., Librarian/Editor
Anthony F. Gallegos, Ph.D., Sr. Performance Assessment Specialist
Jim W. Kenney, M.S., Environmental Scientist
C. Robert McFarland, B.S., Sr. Quality Assurance Engineer
Robert H. Neill, M.S., Director
Kevin J. Shenk, M.S., Health Physicist
Susan Stokum, Administrative Secretary
Carla Tafoya, Secretary
Brenda J. West, B.A., Administrative Officer

SUMMARY

The United States Department of Energy (DOE) has published two reports in recent years which estimate the probability of a catastrophic accident at the Waste Isolation Pilot Plant (WIPP) waste hoist system. The earlier report, Banz et al (1985), concluded that such an accident had an annual probability of occurrence of only 1 in 60 million. Since the DOE-AL Order 5481.1A defines events having an annual probability of occurrence of less than one in one million as extremely improbable, Banz et al (1985) labelled the possibility of a catastrophic accident at the waste hoist as being extremely improbable.

The Environmental Evaluation Group (EEG) criticized that report as not being sufficiently conservative (Appendix A, 1985). Additionally, EEG stated that some important factors were not included. Factors which were not conservative or were overlooked included: nature of planned quality assurance, nature and quality of planned maintenance, human factors and operator errors. DOE rejected these criticisms (Appendix B, 1985).

Approximately two years later, on July 25, 1987, there was a serious incident at the waste hoist system at WIPP which involved two unplanned and unexpected free-wheeling upward movements of 30 ft. and 300 ft. of the waste hoist conveyance. The DOE ordered a Class C investigation and published the results on October 15, 1987 (Appendix F). The report identified a hydraulic return valve "as a single point failure common to both sets of brakes." Thus, the benefit of having two presumably independent sets of brakes was lost due to a design failure. Additionally, the report was highly critical of the Quality Assurance Program, the maintenance procedures, contractors performing warranty work at WIPP, the "Person in Charge" program to provide oversight, and much more.

Following the July 25, 1987 incident, DOE published a new study of the hoist brake system (Chan et al, 1987). This study was a distinct improvement over the 1985 analysis. The study by Chan et al (1987) was specific for the existing waste hoist system, considered the possibility of human error, and included conservative features like the possibility of common cause failures. They took into account the design defect revealed by the July 25, 1987 incident, and calculated the annual probability of a catastrophic accident as one in one thousand. This was greater than the Banz et al (1985) calculation by a factor of approximately 60,000. Chan et al (1987) proposed a number of design changes, and on that basis revised the calculation of the annual probability of a catastrophic accident at the waste hoist. The revised value is approximately one in 20 million.

An analysis of the Chan et al (1987) report shows that even the revised calculations are not sufficiently conservative, for the following reasons:

(a) the manner of calculating the frequency of loss of electric power (a common component in all risk scenarios);

(b) the use of median (or mean) values for failure rates of components, instead of upper bounds corresponding to a 90% confidence interval;

(c) the use of median values for human error probability (HEP), instead of upper bounds corresponding to a 90% confidence interval.

The calculations by DOE and EEG lead to different estimates of the annual probability of a catastrophic accident at the WIPP waste hoist system, as follows:

DOE, 1985 (Banz et al, 1985):

1 in 60 million = 1.66×10^{-8}

DOE, 1987 (Chan et al, 1987 - without design changes):

1 in 1000 = 1×10^{-3}

DOE, 1987 (Chan et al, 1987 - with suggested design changes):

1 in 20 million = 5.2×10^{-8}

Greenfield, 1989 (this report - with assumption of suggested design changes):

1 in 27 thousand = 3.7×10^{-5}

In conclusion, this report shows that the probability of a catastrophic accident involving the WIPP waste hoist system over the 25 years of expected operation is about 10^{-3}, or about 1 in 1000. EEG's estimate of the risk is about 700 times higher than the DOE estimate, and therefore DOE has erred in the Final Safety Analysis Report in concluding that such an accident is incredible (annual probability less than 10^{-6}). DOE should therefore perform consequence analyses of a catastrophic accident involving the waste hoist system. These calculations and mitigation measures to reduce the probability of an accident and to minimize the impact of such an accident should be included in the WIPP Safety Analysis Report.

1. INTRODUCTION

1.1 Waste Shaft and Hoist at WIPP

The Waste Isolation Pilot Plant (WIPP) is being constructed in southeastern New Mexico to be a repository for permanent disposal of transuranic (TRU) radioactive waste generated from the defense activities of the United States. It is planned to emplace up to 175,700 cubic meters (6.2 million cu. ft.) of contact-handed transuranic (CH-TRU) waste totalling 9 million curies of radioactivity, and 4,800 cubic meters (170,000 cu. ft.) of remote handled (RH-TRU) waste totalling 5 million curies.

One of the key facilities of the plant (WIPP) is a waste shaft and hoist that will be used to transport radioactive waste, underground mining equipment, and radiation personnel between the surface and the underground. Fig. 1 shows the surface location of the waste shaft (facility 311) in relation to other surface facilities and structures. The names of the various facilities and structures, identified by numbers in Fig. 1 are given in Fig. 1(a). The location of the waste shaft at the storage horizon, 2150 ft. below the surface, in relation to the storage and experimental areas, is shown in Fig. 2. Schematic views of the waste hoist are shown in Figures 3 and 4. A more detailed view of the waste shaft headframe is shown in Fig. 5. The waste hoist conveyance, shown in Figures 3, 4 and 5, contains an upper and lower deck. Personnel use the upper deck. The conveyance is 30 feet high, 10 feet wide and 14 feet deep. It can carry a payload of 45 tons. A counter-weight (Figures 3 and 4) of 50 tons balances the conveyance. It is expected that a total of 1820 hoist cycles per year will be required for the operations (Banz et al, 1985).

A key feature of the safety design of the waste hoist system is the presence of two independent braking systems. "The dual

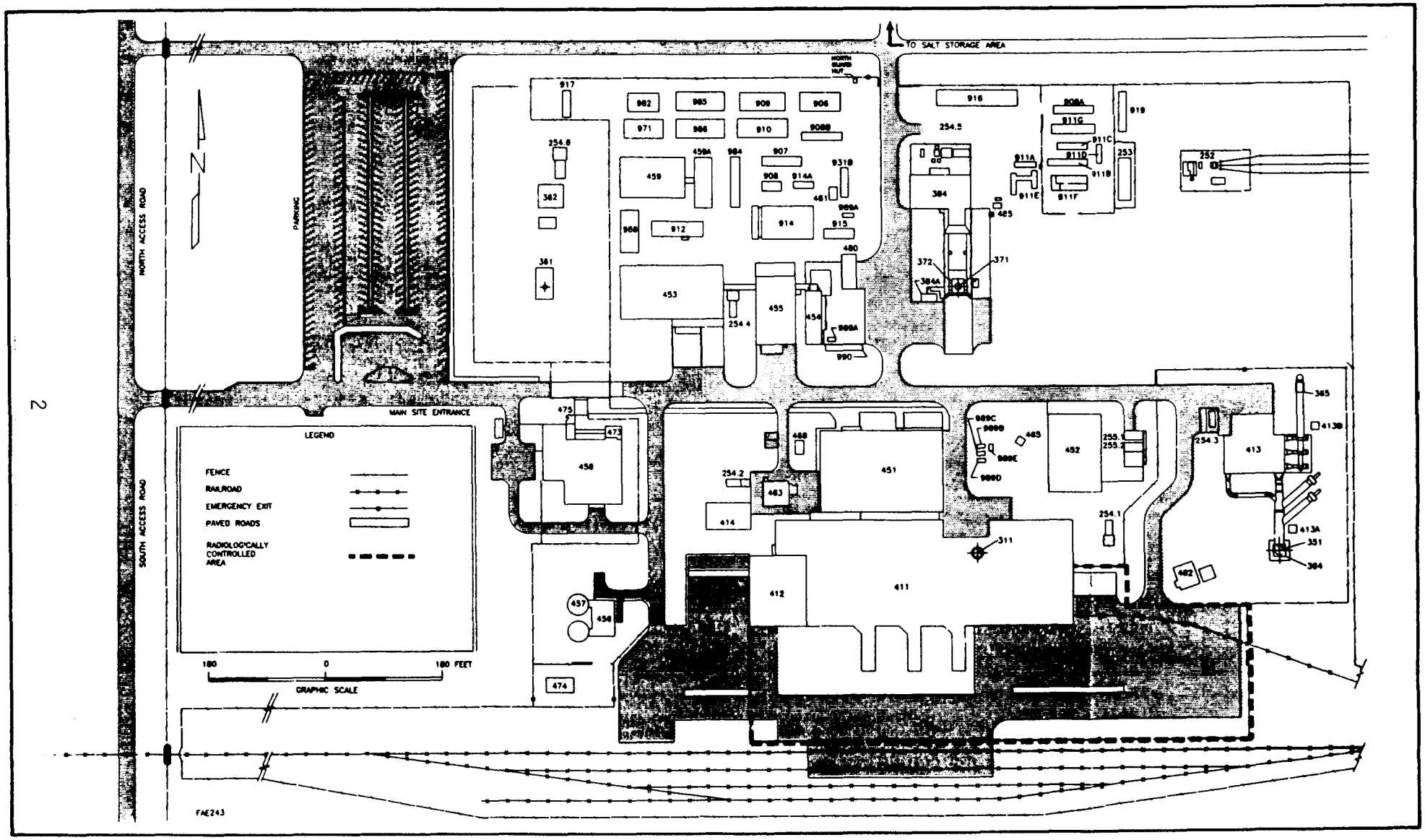


Fig. 1 Location of WIPP surface facilities (see Fig. 1(a) for legend)
From FSAR (USDOE, June 1989)

FACILITIES AND STRUCTURES NUMBERS

SPS UTILITY SUBSTATION	FAC 252
13.8 KV SWITCHGEAR 25P-SWG15/1	FAC 253
AREA SUBSTATION NO.1 25P-SW15.1	FAC 254.1
AREA SUBSTATION NO.2 25P-SW15.2	FAC 254.2
AREA SUBSTATION NO.3 25P-SW15.3	FAC 254.3
AREA SUBSTATION NO.4 25P-SW15.4	FAC 254.4
AREA SUBSTATION NO.5 25P-SW15.5	FAC 254.5
AREA SUBSTATION NO.6 25P-SW15.6	FAC 254.6
EMERGENCY GENERATOR #1 25-PE 503	FAC 255.1
EMERGENCY GENERATOR #2 25-PE 504	FAC 255.2
WASTE SHAFT	FAC 311
EXHAUST SHAFT	FAC 351
AIR INTAKE SHAFT	FAC 361
AIR INTAKE SHAFT/WINCH HOUSE	FAC 362
C&SH SHAFT	FAC 371
C&SH HEADFRAME	FAC 372
C&SH HOISTHOUSE	FAC 384
LAMPHOUSE	FAC 384A
WASTE HANDLING BUILDING	BLD 411
TRUPACT MAINTENANCE BUILDING	BLD 412
EXHAUST SHAFT FILTER BUILDING	BLD 413
MONITORING STATION A	BLD 413A
MONITORING STATION B	BLD 413B
WATER CHILLER FACILITY	FAC 414
SUPPORT BUILDING	BLD 451
SAFETY & EMERGENCY SERVICE FACILITIES (UNDER CONSTRUCTION)	BLD 452
WAREHOUSE/SHOPS BUILDING	BLD 453
VEHICLE SERVICE BUILDING	BLD 454
AUXILARY WAREHOUSE BUILDING	BLD 455
WATER PUMPHOUSE	BLD 456
WATER TANKS (2)	FAC 457
GUARD AND SECURITY BUILDING	BLD 458
CORE STORAGE BUILDING	BLD 459
SANDIA ANNEX	BLD 459A
FIRE HUT	BLD 461
COMPRESSOR BUILDING	BLD 463
AUXILARY AIR INTAKE	FAC 465
TELEPHONE HUT	BLD 468
ARMORY BUILDING	BLD 473
HAZARDOUS WASTE STORAGE BUILDING	BLD 474
GATEHOUSE	BLD 475
VEHICLE FUEL STATION	FAC 480
EXHAUST SHAFT HOIST EQUIPMENT WAREHOUSE	BLD 482
SULLAIR COMPRESSOR BUILDING	BLD 485
MIS & QA	TRL 906
EEG TRAILER	TRL 907
PP & C TRAILER	TRL 908
SNL CABLE FAB TRAILER	TRL 908A
IT CABLE FAB TRAILER	TRL 908B
SAFETY TRAILER	TRL 909
ENVIRONMENTAL SAFETY AND HEALTH	TRL 910
SANDIA CAL LAB #1	TRL 911A
SANDIA M101	TRL 911B
SANDIA ANNEX	TRL 911C
SANDIA MOBILE TRANSPORT	TRL 911D
SANDIA CAL LAB #2	TRL 911E
SANDIA B49 AND B49 ANNEX	TRL 911F
SANDIA LABORATORY TRAILER	TRL 911G
TRAINING TRAILER	TRL 912
CONSTRUCTION MGMT AND MAINTENANCE COMPLEX	TRL 914
CONSTRUCTION MGMT ANNEX	TRL 914A
CONSTRUCTION MGMT	TRL 915
SANDIA NATIONAL LAB TRAILER	TRL 916
SNL STAGING AND PREPARATION TRAILER	TRL 917
REGULATORY AND ENVIRONMENTAL STORAGE	TRL 919
MENS CHANGE TRAILER	TRL 931B
SAFETY EVALUATION PROGRAMS TRAILER	TRL 971
PP & C TRAILER	TRL 982
HUMAN RESOURCES TRAILER	TRL 984
PURCHASING TRAILER	TRL 985
PURCHASING TRAILER	TRL 986
SECURITY/EOC TRAILER	TRL 988
MOBILE STORAGE BUILDING	TRL 989A
MOBILE STORAGE BUILDING	TRL 989B
MOBILE STORAGE BUILDING	TRL 989C
MOBILE STORAGE BUILDING	TRL 989D
MOBILE STORAGE BUILDING	TRL 989E
MOBILE STORAGE BUILDING	TRL 990

Fig. 1(a) Legend for Fig. 1
From FSAR (USDOE, June 1987)

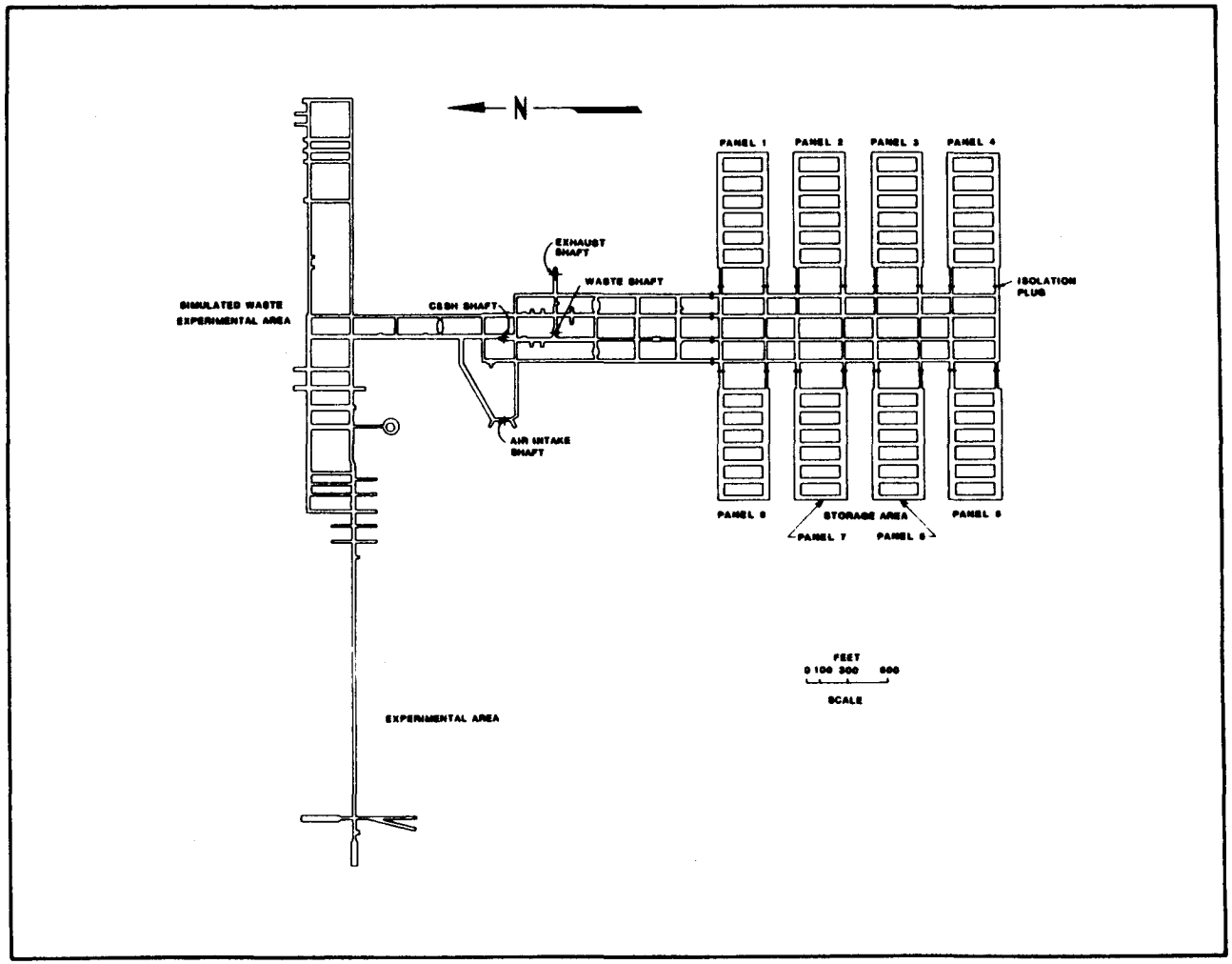


Fig. 2 Underground layout of WIPP
From FSAR (USDOE, June 1989)

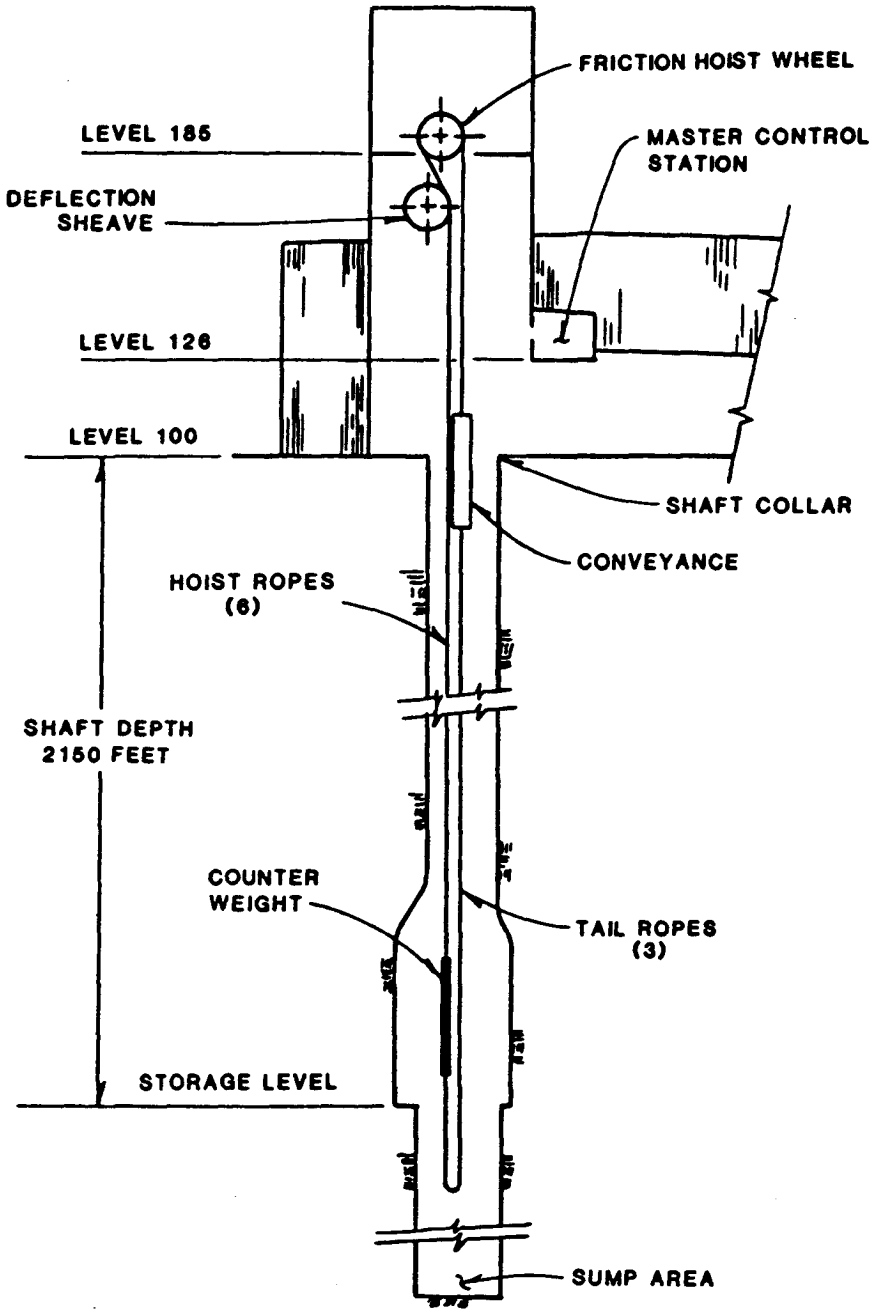


Fig. 3 WIPP Waste hoist concept
(Fig. 1-1 of Banz, 1985)

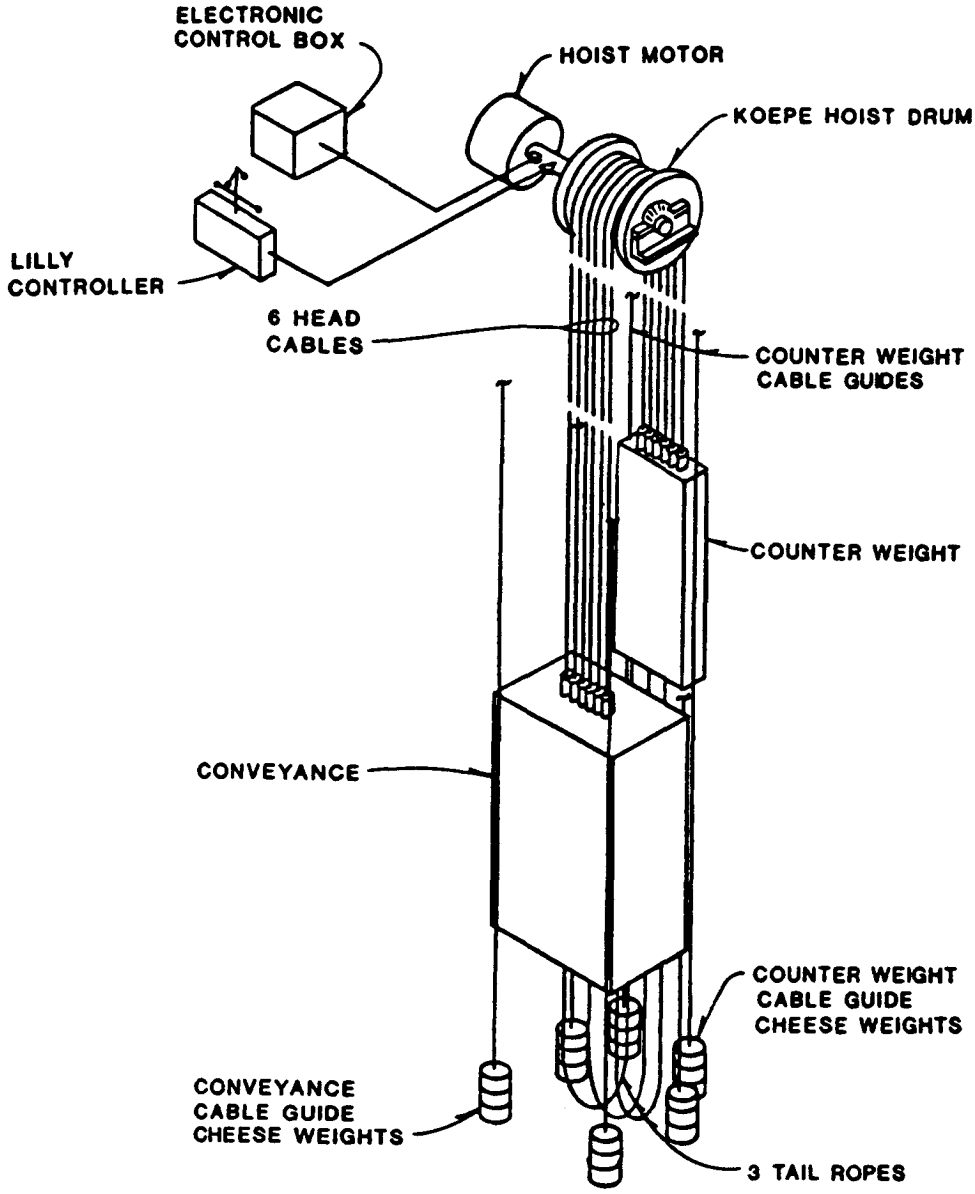


Fig. 4 Waste hoist configurations
(Fig. 1-2 of Banz, 1985)

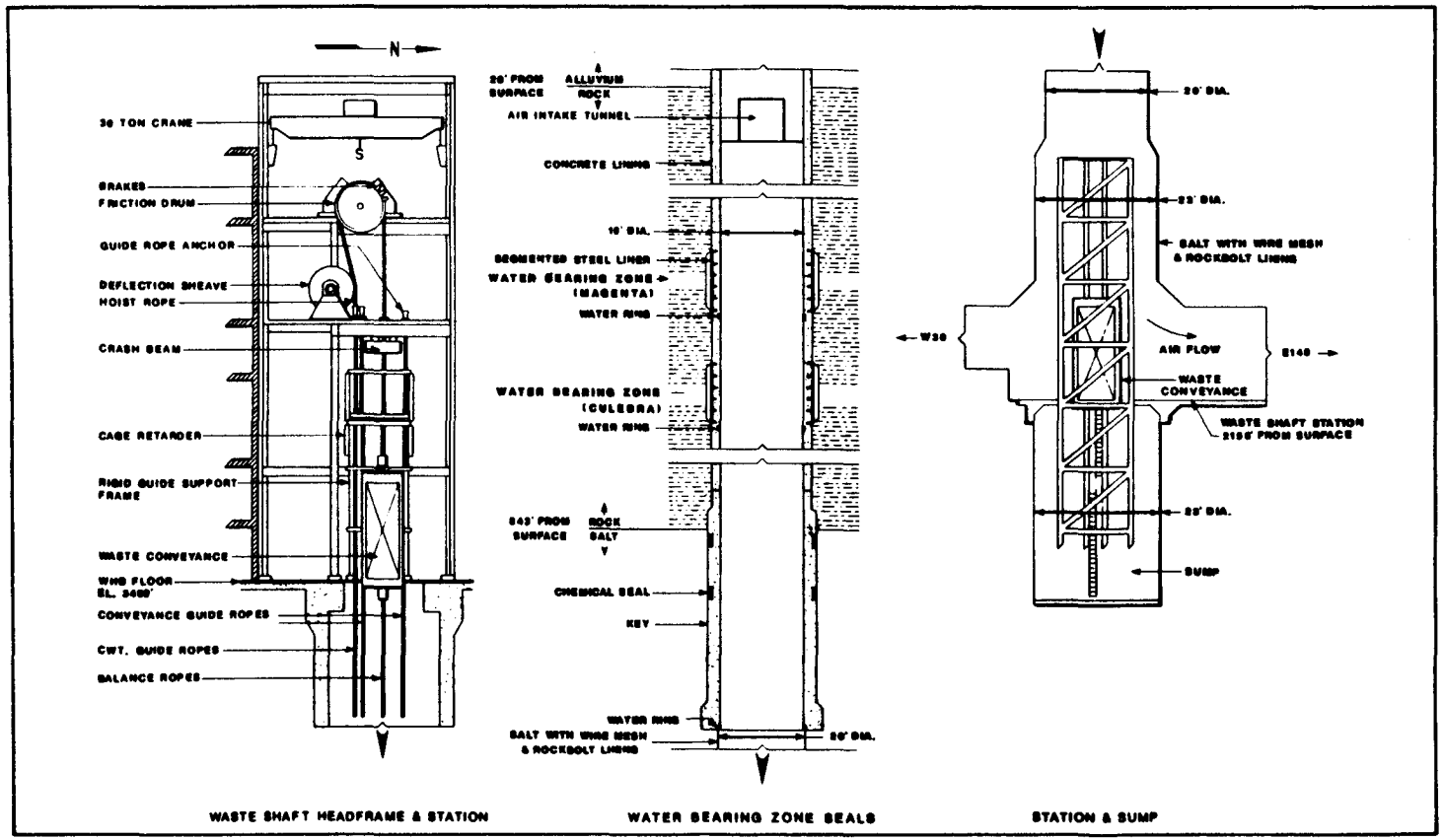


Fig. 5 Waste shaft headframe and station
From FSAR (USDOE, June 1989)

brake system is designed so that each brake is able to stop the conveyance at maximum payload within a 30 feet travel distance" (Banz et al, 1985). Another safety feature is the presence of six cables, designed to a safety factor of six (Banz et al, 1985). This is a conservative system since "five of six cables must fail in order to cause a cable break accident" (Banz et al, 1985).

1.2 Probabilities of Catastrophic Failure

The importance of the waste hoist system as a key facility at WIPP required that a study be made of the probability of a catastrophic hoist accident. Such a study was performed by the Westinghouse Electric Corporation and Dravo Engineers, Inc., for DOE (Banz et al, 1985). The report concluded that the annual probability of a catastrophic hoist accident at WIPP was quite small, with a value of 1.7×10^{-8} (1 in 58 million). Since DOE-AL Order 5481.1A states that any event with an annual probability of less than 1.0×10^{-6} (1 in 1 million) is deemed extremely improbable, the report concludes that the occurrence of a catastrophic hoist accident "may be categorized as an extremely improbable event at WIPP" (Banz et al, 1985). This result was reviewed by EEG (Appendix A) which disagreed with the conclusions of the Banz et al (1985) report. EEG stated that the possibilities of human errors and operational errors were not addressed. Some two years later, on July 25, 1987, an incident occurred which opened the entire matter, and required a fresh look at the probability of a catastrophic hoist accident at WIPP. The incident consisted of two unplanned, unexpected and uncontrolled upward movements of the waste-hoist conveyance, first 30 ft. and later 300 ft. (the incident is further discussed is Chapter 2). A new DOE study (Chan et al, 1987) calculated the annual probability of a catastrophic hoist accident at WIPP to be 1.0×10^{-3} (1 in 1 thousand), more than 4 magnitudes greater than the results of the Banz et al (1985) report. The large difference is due in part to the assumption of a design defect in

certain valves, as well as human and operational errors, which were factors in the July 25, 1987 incident. The authors of the Chan et al (1987) report suggested and recommended some design changes which could dramatically improve the situation. With the assumption of an improved design, and appropriate control of human factors, Chan et al (1987) calculated a new annual probability of a catastrophic hoist accident at WIPP to be 5.2 X 10^{-8} (1 in 20 million).

The wide fluctuations of these various calculations and the occurrence of the July 25, 1987 incident prompted EEG to undertake another review, which is the purpose of this report.

1.3 Banz et al (1985) Report, EEG criticism, DOE response

The first DOE study (Banz et al, 1985) calculated the annual probability of a catastrophic hoist accident at the Waste Isolation Pilot Plant (WIPP) to be 1.7 X 10^{-8}. This is equivalent to an annual probability of a catastrophic accident of approximately one in 58 million. After reviewing this document, EEG concluded (Appendix A) that the annual probability of a catastrophic hoist accident was probably greater than one in 1 million. EEG stated that several assumptions in the DOE study were not conservative, and that some important factors were not included. Factors which were not conservative or overlooked included:

- Number of work shifts per day
- Calculation of the number of power losses per year
- Nature of planned Quality Assurance
- Nature and quality of planned maintenance
- Human factors and operator errors (this last factor was crucial in the July 25, 1987 incident).

It is useful to review the DOE responses (Appendix B) to some of the EEG comments. Some aspects of the exchanges have a

bearing on the Chan et al (1987) report. The format below is arranged in the following manner: The item number refers to the same number in Appendix B, and gives the EEG Comment, followed by the DOE response (all in 1985). Then a comment by the author of this report is made on the given item. For clarity the author's comments are preceded by "EEG-44".

Appendix B, Item 3 (1985)

EEG Comment: The analysis should have considered the possibility that WIPP will operate with more than one waste handling shift per day, and the possibility that a fourth shaft will be added.

DOE Response: As noted on page 5.1-2 of the WIPP Safety Analysis Report (SAR), current plans are for one waste handling shift per day. The analysis was performed for the current design of WIPP; it is not feasible to consider all possible modifications which may be implemented in the future.

EEG-44. As DOE stated, it is true that not all possible modifications to be implemented in the future can be considered in terms of the possible impact on the estimation of the probability of a catastrophic accident. However, prudence and conservative design should take into account certain obvious and feasible changes. Certainly one of these is the possibility of having two waste handling shifts per day. This would introduce a factor of 2X in the calculation of the probability of a catastrophic accident. A potential need for reprocessing the drums (placed in the repository during the performance assessment and operational demonstration phase) may arise if the waste emplacement proposed by DOE (68,000 drums of CH-TRU Waste) is accomplished. In such circumstances, it may be necessary to accomplish retrieval in a short time period. This would reasonably to two shifts per day.

Appendix B, Item 7 (1985)

EEG Comment: The choice of lambda, the number of power losses per year, is not conservative since the data on which lambda is based is narrow in scope.

DOE Response: Lambda is the average rate of occurrence of an event. Therefore, in some years there may be more than one power loss and in others there may be none. This random variability does not invalidate the average rate of occurrence. However, even if an additional factor of two is applied to the value of lambda, the resulting probability of a catastrophic hoist accident would be approximately 3E-8 per year, which is not considered credible.

EEG-44. The DOE response indicates a lack of understanding of the problem of estimating the frequency of electric power loss. Since this is a vital number that the Chan et al (1987) report adopted from the Banz et al (1985) report, this matter is treated separately and in detail in Section 4.1 of this report.

Appendix B, Item 9 (1985)

EEG Comment: The nature of planned QA and maintenance should be addressed in the report.

DOE Response: Adequate maintenance and quality assurance efforts are assumed in this analysis. Specific plans regarding these efforts have not yet been finalized.

EEG-44. The nature of the July 25, 1987 incident underscores the importance of EEG's advice on the vital matter of quality assurance, maintenance, proper supervision, written instructions, etc. Clearly from 1985 to 1987 these matters were not addressed appropriately by DOE.

Appendix B, Item 10 (1985)

EEG Comment: The human factors and operator errors are not addressed in WTSD-TME-063 (Banz et al, 1985). Two additional scenarios should be considered: brake system failure plus human error, and power outage plus human error.

DOE Response: Human error is addressed in Table 3-1 of the final report. It states as follows:

> "Inattentive hoist operation is a relatively frequent cause of hoisting mishaps. The WIPP hoist procedure is designed to virtually eliminate the human element. When transporting CH-TRU or RH-TRU waste, the hoist will be in an automated mode (Bechtel, 1984). The only human interaction involves pushing a single button to activate the lowering cycle."

Therefore, human error was judged to be a negligible contributor to the total probability of a catastrophic hoist accident at WIPP.

EEG-44. Again EEG advice on the matter of human error was germane and timely. It was precisely "brake system failure plus human error" which largely accounted for the July 25, 1987 incident. The DOE response that human error "was judged to be a negligible contributor to the total probability of a catastrophic hoist accident at WIPP" turned out to be in error. The Chan et al (1987) report includes the possibility of human error, and this matter is treated separately and in detail in Section 4.2 of this report.

2. JULY 25, 1987 INCIDENT IN THE WIPP WASTE HOIST

On Saturday, July 25, 1987, during a maintenance procedure on the Waste Hoist System at WIPP, two unplanned and unexpected upward movements of the waste hoist conveyance occurred. Tom Lukow of DOE notified James Channell of EEG about the incident on late Tuesday morning, July 28, 1987, some 3 days after the accident (Appendix C). Mr. Neill of EEG promptly notified (July 28, 1987) a number of officials of the State of New Mexico (Appendix C). This was followed by a letter from Neill to Jack Tillman of DOE, dated August 5, 1987, discussing the occurrence (Appendix D). Neill made the point that EEG had expressed strong disagreement with contractors' assertions (Dravo and Westinghouse) that a catastrophic hoist accident at WIPP is "not credible" or "extremely improbable." DOE had previously denied the possibility of human error saying, "The WIPP hoist system is designed to virtually eliminate the human element, and thus human error was judged to be a negligible risk contributor." Mr. Tillman responded to Neill on August 17, 1987 and included a copy of an Unusual Occurrence Report (UOR) which described what had taken place (Appendix E). This was followed by an abridged copy of a Class C Investigation. Only the scope of the investigation and a summary was included (3 pages) (Appendix F). The balance of the report, which contained "Facts," "Analysis," "Recommendations," and "Appendices," some 17 or more pages, was not included. The report was received on December 31, 1987 by EEG, although the report is dated October 15, 1987.

In 1985, EEG (Appendix A) reviewed the DOE report (Banz et al, 1985) on the probability of a catastrophic hoist accident at the WIPP. At that time EEG emphasized some serious shortcomings in the report: lack of consideration of the possibilities of design inadequacies, improper maintenance, operator errors and possible other human factors. Unfortunately, a serious incident

did occur on July 25, 1987. While short of being a catastrophe, because the hoist was empty, the incident involved all the elements stated in the above mentioned report (Appendix A) and more.

Briefly, the incident involved a malfunctioning of one of the hydraulic 4-way valves, #45. It had excessive internal hydraulic leakage, causing depletion of the oil inventory in the primary hydraulic system. Since the system was still under warranty, the supplier decided to replace the valve with another, of different design, apparently without proper documentation and quality assurance. With some on-the-spot modification, the replacement valve was made to fit, and the system was energized. There was an unintended fall of the counterweight (weighs more than the conveyance), and a rise of the conveyance by approximately 30 ft. Fortunately, the brakes applied by themselves and the hoist came to a halt. The supplier personnel and management and operating contractor (MOC) personnel then decided to reverse the valve (180°) and try again. This time there was an unintended upward movement of the conveyance for about 300 ft! The personnel cleared the area fearing the worst (Appendix F). Fortunately, once again the hoist brakes engaged, and the hoist was brought to a halt. At this point, the system was returned to its original configuration, and notifications were sent to management and the manufacturer. Later examinations revealed that a "plugged vent port resulted in a configuration that blocked the hydraulic flow in the brake system return circuit. Blocking of the flow allowed pressurization and release of the hoist brake actuation cylinders and thus maintained the brakes in a disengaged position causing a free fall of the counterweight and lifting of the conveyance (Appendix E)." This detail is important to note since the newer report on the waste hoist (Chan et al, 1987, page 26) makes the point that the design of the hoist brake system is "safe" because the brakes are designed to set, when there is a loss of pressure; i.e. a system

is safer if the brakes set when there is a loss of pressure, rather than a design in which the brakes set as a result of a suitable increase of pressure. The facts of the July 25, 1987 incident undermine this assumption.

The Unusual Occurrence Report (UOR) (Appendix E) described the failure of three barriers which led to the occurrence: (a) the replacement valve lacked proper documentation, and in fact was not a suitable plug-in replacement; (b) the second failed barrier was the potential for the "installation contractor personnel to stop the warranty action based on the absence of appropriate documentation and the physical difference in valve configuration"; (c) a third failed barrier was the absence of a "quality assurance input for this process." The responsible operations personnel failed to properly manage the entire procedure, and especially to "stop the activity after the first inadvertent brake release."

3. SUMMARY OF THE CHAN et al, (1987) REPORT

3.1 Hydraulic Brake System

In the light of the July 25, 1987 incident and the factors that led to it, it is clear that the probability calculation in the report, "Probability of a Catastrophic Hoist Accident at the Waste Isolation Pilot Plant," WTSD-TME-063 (Banz et al, 1985), of a catastrophic hoist accident at WIPP, with a value of an annual probability of 1.7×10^{-8} was fatally flawed. In a number of ways, the report, "Quantitative Fault Tree Analysis of the Waste Isolation Pilot Plant Waste Hoist Hydraulic Brake System," (Chan et al, 1987) is considerably more satisfactory. It does include the possibilities of errors associated with maintenance and those associated with operators.

Banz et al (1985) had correctly identified the failure of the hoist braking system as the major potential contributor to a hoist accident sequence. Chan et al (1987) properly address the hydraulic brake system as the most important potential contributor to a catastrophic accident. In a distinct improvement over the 1985 study, the analysis is based on a detailed study of the engineering design and the mode of operation. Of course, Chan et al (1987) were guided by the design inadequacies revealed by the July 1987 incident.

The Chan et al (1987) study evaluates sequences of postulated failures, and identifies the "dominant contributors to risk and potential single failures which could disable the system."

The hydraulic system consists of two independent pressure supply units. Only one of these two pressure units is sufficient to release the brakes during system operation. The brakes will be set when the pressure from the brake cylinder is removed. Any single path to the hydraulic pump reservoir is

sized sufficiently to bleed the pressure from the brake units to initiate brake setting. Thus the scenarios involving releasing the brakes inadvertently involve blocking the release of oil, and maintenance of the pressure.

3.2 Base Case Calculation

3.2.1 Scenarios with Component Failure, Loss of Electric Power, Human Error

In a study which the authors of the 1987 report call the "Base Case," it was revealed that major contributors to the probability of a catastrophic accident were scenarios involving the two solenoid-operated 4-way valves, numbers 45 and 51. Valve 45 was the one involved in the July 25, 1987 incident. If either one fails, a blocking of flow results. However, there must also be a simultaneous loss of electric power in order to produce a catastrophic accident. Thus, one must multiply the probabilities of failure of either one of the valves and the loss of electric power to obtain a contributing probability of a catastrophic accident. Chan et al (1987) found two ways in which either of the valves 45 and 51 may fail. One way is termed "local fault", in which the valve stops operating and blocks flow. The other failure may occur when either valve is in maintenance during a hoist shutdown. Then the operator makes an error in resetting either valve, leaving it in a "blocked" mode. For both "local fault" failure and the operator error failure, there must be a simultaneous loss of electric power in order to have a catastrophic accident. On this basis the authors have identified 10 scenarios (termed "cutsets", a term used by writers on reliability) which are the major contributors to the probability of a catastrophic accident. These are listed in Table 4.1-1, page 36, of the Chan et al (1987) report. Table 4.1-2, page 37, lists the 10 largest contributors to brake system failure, Base Case. (These two tables are referred to frequently

in this report, and for that reason are included as Appendix G.) The values for component failure rates listed in Table 4.1-2 are mostly obtained from industry sources. Examination of valves 45 and 51, and information from the manufacturer led Chan et al (1987) to assign an annual failure rate to 45 of 9.02×10^{-3}, twice that assigned to valve 51 or 4.52×10^{-3}, due to "local faults."

3.2.2 Calculation of Human Error Probability

The failure rate assigned to operator error in maintaining either valve 45 or valve 51 is 6.56×10^{-3}. This is a composite value derived by the authors as follows.

The human error probability associated with failure to restore these valves after maintenance is composed of two elements:

(a) Failure to follow written test or calibration procedures: 8.1×10^{-2}

(b) Special short term, one-of-a-kind checking, with alerting factors: 8.1×10^{-2}

The composite human error probability (HEP) is:

$$(8.1 \times 10^{-2}) \cdot (8.1 \times 10^{-2}) = 6.56 \times 10^{-3}$$

Chan et al (1987) based these choices on methods described in a handbook of human reliability analysis (Swain, 1983).

It is important to note that this assignment of an HEP value represents the authors' method of taking into account human error factors which may contribute to brake system failure, and thus to

a catastrophic accident. This point is discussed in detail in Section 4.2 of this report.

3.2.3 Component Failure Rates and Rate of Loss of Electric Power

Chan et al (1987) list all the component failure rates used in their analysis in their Table 2-1.

Some comparisons will be made for a few items listed in Tables 2-1 and 4.1-2 (Appendix G).

From Table 2-1, for valve #51 the failure rate is: 1.45×10^{-6} per hour.

To convert to an annual rate, Chan et al (1987) assume an 8 hr day for hoisting waste and 4 hrs for maintenance, a total of 12 hrs.

Annual hours: $12\ ^{hrs}/_{d} \times 5\ ^{d}/_{wk} \times 52\ ^{wk}/_{yr} = 3{,}120\ ^{hrs}/_{yr}$

Thus for valve #51:

1.45×10^{-6} 1/hr x 3,120 hrs/yr. = 4.52×10^{-3} per year, which is the value listed in Table 4.1-2 (Appendix G).

Similarly, one obtains for valve #45, the value 9.02×10^{-3} per year.

For site specific failure rates, Chan et al (1987) have adopted the values quoted in Banz et al (1985). As Table 4.1-1 (Appendix G) indicates, a very important failure rate is that for loss of electric power at 3.4×10^{-2} per year, adopted from the previous report. This factor appears as a multiplicative element in each of the most important 10 terms of Table 4.1-1. Chan et

al (1987) recognize the importance of this value for loss of electric power in their Table 4.1-3. They establish an index for "importance," and loss of electric power has the largest value in the "importance" listing. The choice of this value (0.034) will be discussed in some detail later in this report.

3.2.4 Annual Probability of Brake System Failure

The sum of the 10 items in Table 4.1-2 (Appendix G) is 2.7×10^{-2}, and represents the annual probability of brake system failure. As Chan et al (1987) state in their report (p. 29), "The specific brake system annual probability of failure is approximately 2.7×10^{-2}. This is somewhat high, but as can be seen from the later sensitivity studies, these failures will be mitigated by some design changes which are currently in the process of being implemented." It is useful to note how the startling change occurred between this number and the comparable number developed in the July 1985 report (Banz et al, 1985). In that report, it was assumed that <u>two</u> brake failures had to occur in sequence to produce total failure in the brake system. Thus the probability for single brake failure would be multiplied by the probability of the second brake failure. The probability for a single brake failure was based on MSHA data. The Banz et al (1985) report quoted 18 brake malfunctions in 5×10^7 hoists. Since WIPP was planned to have 1820 hoist cycles per year, one computes the annual failure rate as:

$$\frac{18 \text{ malfunctions}}{5 \times 10^7 \text{ hoists}} \times \frac{1820 \text{ hoists}}{\text{yr}} = 6.6 \times 10^{-4} \text{ per year}$$

The annual failure rate for simultaneous failure of both components of the brake system would then be:

$$(6.6 \times 10^{-4})\ (6.6 \times 10^{-4}) = 4.36 \times 10^{-7} \text{ per year}$$

In contrast with this small number, the probability values in Table 4.1-2 of Chan et al (1987) are associated with failures of single components, as item (1) for failure of valve #45, local faults, with a value of 9.02×10^{-3}, followed by items (2) and (3) for valves #45 or #51 in maintenance, followed by operator error in maintenance leading to values of 6.56×10^{-3} and 6.56×10^{-3}, and so on to the other items in that table.

3.2.5 Annual Probability of a Catastrophic Accident

Table 4.1-1 (Appendix G) lists the major contributors to the probability of a catastrophic accident, base case, in decreasing order of magnitude. All the 10 items listed involve failures of valves #45 or #51, either because of local faults, or because of maintenance. The table is arranged with values of the component failure rates on the right, and the consequent contribution to the probability value on the left. Thus for item 1, three events are involved in producing failure:

1) Valve #45 fails and blocks flow due to local fault: failure rate = 9.02×10^{-3}

2) CH-TRU waste is being hoisted: 0.57, i.e. 57% of the time is allocated to hoisting CH-TRU waste.

3) There is an electric power failure, and the result is an upward hoist movement: failure rate = 0.034

Multiplying the 3 rates produces: 1.75×10^{-4}

The last number is the contribution of this scenario to the probability of a catastrophic accident.

A striking contrast exists between the items in Table 4.1-1 (Appendix G), the contributors to the probability of a catastrophic accident, and comparable numbers in the Banz et al (1985) report. The latter one computes the contribution of brake system failure plus electric power loss to the probability of a catastrophic accident as follows: Assume CH waste is being hoisted. In that report 1560 cycles are assumed to be for hoisting CH with the balance of 1820 cycles for RH. The probability for power loss is taken as 0.034. Thus for "brake system fails" and "loss of electric power to the hoist":

$$\frac{1560}{1820} \times 0.034 \times 6.6 \times 10^{-4} \times 6.6 \times 10^{-4} = 1.27 \times 10^{-8}$$

This is the number listed in the Banz et al (1985) report, Table 6-2, for CH-TRU "over travel up: Power loss, Brake System Failure."

In contrast, Table 4.1-1 (Chan et al, 1987) lists 10 contributors to the probability of a catastrophic accident, all involving failures of valve #45 or #51. The lead value for (1) is 1.75×10^{-4} for valve #45 failure ("local fault"), blocking flow, CH-TRU waste being hoisted, with loss of electric power. The 10 items can be listed on the basis of reason for failure and by valve number:

Failure Reason	Valve #45	Valve #51	Total Probability (per year)
local fault	0.307×10^{-3}	0.138×10^{-3}	0.445×10^{-3}
maintenance plus operator error	0.201×10^{-3}	0.223×10^{-3}	0.424×10^{-3}
GRAND TOTAL PROBABILITY OF A CATASTROPHIC ACCIDENT.....			0.87×10^{-3}

Chan et al (1987) state (p. iii) that Table 4.1-1 accounts for 99% of the probability for total system failure. Rounded up, this sum is approximately equal to the stated value for system failure probability of 1×10^{-3} per year listed in Table 4.1-4 (page 39).

3.3 Sensitivity Case 1: Proposed Emergency Dump Valves

Again one may understand the difference between 1×10^{-3} of the 1987 report (p. 39) and the 1.7×10^{-8} of the 1985 report (p. 32) in terms of the latter requiring the simultaneous failures of the two independent components of the brake system, plus the failure of electric power. Further the analysis in the 1987 report identified 10 significant pathways which led to flow block and subsequent catastrophic failure. It was a careful analysis of the specific design of the hydraulic brake system that revealed the larger opportunities for system failures. The July 25, 1987 incident provided the spur to seek out the possible failure modes due to operator errors in connection with valve maintenance.

By the same token, Chan et al (1987) had gained the insight needed to supply possible corrective steps in the basic design of the hydraulic system. Clearly what was needed were ways relatively certain to relieve flow blocks that might occur for the reasons detailed above. Chan et al (1987) proposed the addition of two solenoid-operated emergency dump valves, one on each of the brake disc systems. "These dump valves should open when de-energized, dumping brake fluid directly into the primary brake fluid reservoir." The authors suggest placing the dump valves upstream of manual ball valves 56.3 and 56.6. These latter valves appear to be near or adjacent to the disc brake systems. Thus even if valves 56.3 and 56.6 were blocked and other downstream valves (e.g. valves 25.2 and 25.4) were also blocked, the emergency dump valves could still provide pressure

relief. See Figure E-1, drawing 95080294, Rev. F, "Hyd. Brake System-Sheet 1" (Chan et al, 1987).

The next step is to calculate the improvement associated with the presence of the two emergency dump valves. Chan et al (1987) assume that both valves fail due to common cause; e.g. they both fail to de-energize. This is a more conservative assumption than assuming each can fail independently of the other. Chan et al (1987) use an equation for two component common cause failures as follows:

$$P_{CC} = B \cdot Q$$

P_{CC} is the probability of common cause failure.

Q is the random failure probability of the component, from Table 2-1.

B is the beta factor (statistical observation factor = 0.05).

From Table 2-1 for the proposed dump valve:

$$Q = 2.89 \times 10^{-6} \text{ per hour}$$

Thus: $P_{CC} = 0.05 \times 2.89 \times 10^{-6}$ per hour

$= 1.45 \times 10^{-7}$ per hour

Since these valves are standby, one converts the per hour failure rate to a "demand" or unavailability quantity, Q, based on the time between inspection tests:

$Q = 0.5\ d \cdot t$

Q = unavailability

d = hourly failure rate

t = time interval between tests (= 730 hrs/month for emergency dump valves)

Thus, $Q = 0.5 \times 1.45 \times 10^{-7}$ per hour x 730 hr

$= 5.27 \times 10^{-5}$

If this factor is now applied to the base values in Table 4.1-4, one obtains:

Brake system failure:

$2.7 \times 10^{-2} \times 5.27 \times 10^{-5} = 1.4 \times 10^{-6}$ per year

Total probability for catastrophic accident:

$1.0 \times 10^{-3} \times 5.27 \times 10^{-5} = 5.3 \times 10^{-8}$ per year

These results are very close to those of sensitivity case 1, Table 4.1-4, page 39 (Chan et al, 1987).

4. ANALYSIS OF THE CHAN et al (1987) REPORT

4.1 Frequency of Electric Power Failure

Chan et al (1987) admit (p. 32) the uncertainty of the failure data accuracy and "operator response/error" accuracy. They chose to use a frequency of electric power failure adopted from the Banz et al (1985) report: $\lambda = 0.034$ per year. It has already been emphasized that this is a key number, appearing in each cutset group listed in Table 4.1-1, (Chan et al, 1987). Any change in this number introduces a multiplicative factor for the total probability of a catastrophic accident.

In response to item 7 (Appendix B) DOE correctly states that lambda, λ, (Banz et al, 1985, page 27) is the average rate of occurrence of the event. What DOE did not appear to realize is that λ represents the mean value of a population, which is not known. All that can be known is the average value, $\bar{x}$, of a limited sample size, based on observation. EEG's point, quite simply, is that a larger sample size tends to be a better estimate of the true but unknown value of λ, the population mean. In fact, when one is faced with a sample mean, $\bar{x}$, based on a small number of observations, it becomes necessary to calculate the possible range of values of $\bar{x}$, based on a choice of a confidence level. This possible variation in the sample estimate of the mean is the sampling error. Assuming a normal or near normal distribution one may use the Student's t distribution to state that the true mean, λ, lies somewhere between certain values with some level of confidence; e.g. with a confidence interval of 95%, two-sided, the value for t may be selected from Student's table. One can then state that there is a 95% likelihood that the true mean, λ, lies between: $\bar{x} \pm t\ s/(n)^{1/2}$

where $\bar{x}$ is the sample mean

s is the estimate of the standard deviation of the mean

n is the number of observations.

Now the values of s, $\bar{x}$, n will be calculated from the data presented in Banz et al (1985), page 27. A frequency can only be calculated by taking the time interval between two occurrences of the event. The data presented on page 27 are:

First Power Loss:	December 1982
Second Power Loss:	October 1983
Third Power Loss:	May 1984

The report calculated the frequency incorrectly. This can be understood if one imagines there had been only a single power loss reported in December 1982. Clearly with only that information, a frequency cannot be calculated.

From the above:

Incident	Time of Occurrence	Time Difference	Rate/yr.
First P.L.	12/82		
		10 mo = 0.833yr	1.200
Second P.L.	10/83		
		7 mo = 0.583yr	1.715
Third P.L.	5/84		

Thus there are n=2 independent observations.

$$\bar{x} = 1.458 \quad 1/yr$$

$$s = 0.36 \quad 1/yr$$

$$\frac{s}{(n)^{\frac{1}{2}}} = \frac{0.36}{(2)^{\frac{1}{2}}} = \frac{0.36}{1.414} = 0.25$$

Entering the "t" table with a confidence interval of 95%, with the number of degrees of freedom n-1=1, t=12.7.
Taking the upper limit:

$$\bar{x} + t \frac{s}{(n)^{\frac{1}{2}}} = 1.458 + 12.7 \times 0.25$$

$$= 4.6 \text{ per year}$$

For example, one may now state that there is only a 2.5% chance that the true value of λ will exceed 4.6 per year.

This value is now used in the calculation of page 27, with the value for S (time at risk) = 0.035 yrs: for the annual power loss probability: $P=1-e^{-\lambda S}=1-e^{-(4.6)(0.035)}$

$$= 0.149$$

The previously computed value was 0.034. Thus, one has to introduce to all scenarios involving a loss of electric power a factor:

$$\frac{0.149}{0.034} = 4.4$$

(Technical note: One may also calculate the upper limit of a 95% confidence interval for the mean of a Poisson distribution. In the present case there are 3 observed events occurring over a span of 17 months. The upper limit value for λ in this instance is 5.72 events/yr, somewhat greater than the 4.6 calculated on the basis of the t-distribution (Sachs, 1984, p. 344).)

If one wishes to express a stronger likelihood: e.g. there is only a 1% chance (98% confidence interval) that λ is greater, then the probability becomes:

$$P = 0.281$$

This exceeds 0.034 by a factor = 8.3.

This calculation used a value of S (time at risk) = 0.035 years. A better estimate of S appears to be available.

Harris et al (1985) give a better engineering estimate of the cycle time for the waste hoist than is offered by Banz et al (1985). The cycle time combined with the planned number of hoist trips per year defines the parameter, S, the time at risk in the event of loss of electric power. Banz et al (1985) state the cycle time as follows: "With an estimated 1,820 hoist trips per year and conservatively assuming each trip takes <u>10 minutes</u>, (underlining added) an annual power loss ....". They then compute a time at risk of 0.035 years. This enters into the calculation of the probability:

$$P = 1 - e^{-\lambda S} \qquad \text{(Banz et al, 1985, p.27)}$$

In contrast, Harris et al (1985, p.2-7) describe the operation of the waste hoist in detailed, engineering terms, including "maximum speed of 500 f/min and a maximum acceleration/ retardation of 2 f/sec^2 to provide a cycle time of about <u>16 minutes</u>, (underlining added) not including loading and unloading time".

If one assumes the shaft travel distance to be 2150 feet (Banz et al, 1985, p.3), the maximum acceleration, deceleration to be 2 ft/sec^2, maximum speed 500 ft/min, then an elementary calculation reveals the absolutely <u>minimum</u> time for travel in one direction and then return, for a complete cycle, to be 8.7 minutes. However, this would require maximum acceleration, deceleration, and velocity <u>all</u> the time. On this basis, the estimation of a cycle time of about 16 minutes is more reasonable than 10 minutes.

The change from 10 minutes to 16 minutes per hoist cycle changes the annual time at risk from S=0.035 years to:

$$S = 16 \frac{\text{min}}{\text{h.t.}} \times 1820 \text{ h.t.} \times \frac{1 \text{ yr}}{365\text{d}} \times \frac{1 \text{ d}}{1440 \text{ min}}$$

$$= 0.0554 \text{ years}$$

The probability for the annual power loss is:

$$P = 1 - e^{-\lambda S}$$

With $\lambda = 4.6$ per year (95% confidence interval)

$$P = 1 - e^{-(4.6)\ (0.0554)}$$

$$= 0.225$$

This exceeds the 0.034 value used in the Chan et al (1987) report by a factor 6.6.

With $\lambda = 9.40$ per year (98% confidence interval)

$$P = 0.406$$

This exceeds the 0.034 value by a factor 11.9.

4.2 Human Error Probability (HEP)

The primary motivation for the Chan et al (1987) report on the probability of a catastrophic accident of the waste hoist was the July 25, 1987 incident. The incident also forced a re-evaluation of the design, with the proposed introduction of emergency dump valves in order to recapture the basis of a safe system. Thus, a careful analysis of the incident, with an effort to model what had occurred, was needed in order to arrive at a believable estimate of the probability of such errors in human

performance. For this key calculation, Chan et al (1987) produced a disappointing analysis, given as a brief paragraph "2.1.2 Human Error" on page 13 of their report. They used as a basis for their calculation the work of Swain and Guttman (1983) on human reliability analysis.

Swain and Guttman (1983) are very careful to point to the paucity of "hard" data, and often "judgments were the only source of error probability estimates. In such cases the judgments were based on information from tasks that most nearly resemble the task in question, and the magnitude of the uncertainty (emphasis added) bounds was adjusted in accordance with the judged similarities or differences between the tasks." (Swain and Guttman, 1983, p. 6-8.)

Swain and Guttman (1983) use the term "human error probability" (HEP) based on the idea of "error relative frequency," the ratio of the number of errors to the number of attempts. The authors caution that the nominal values for HEP presented in the book are for average plants. In fact, they state, "it is preferable that more than one analyst be employed in performing an HRA (human reliability analysis) and that expertise in human behavior technology be represented on the HRA team (p. 6-20)." The HEP values quoted in the book are single-point estimates, and are accompanied by an error factor (E.F.). The HEP value is the median of an assumed log-normal distribution. Thus, 50% of the population will have values greater than the HEP. The E.F. factor takes account of the uncertainty of the HEP value relative to the range of values that appear in the total population. Thus, associated with a HEP value is a lower bound and an upper bound. The lower bound, calculated as (HEP/E.F.), is the 5th percentile of the population. The upper bound, calculated as (HEP) (E.F.) is the 95th percentile of the population (p. 6-20). Thus, the upper bound defines the value which is exceeded by only 5% of the

population. Another way of stating this is that there is a 95% likelihood that the value of (HEP)(E.F.) will not be exceeded (p. 6-20). The upper and lower bounds define a 90% interval.

We will now examine the treatment of this matter by Chan et al (1987). It does not appear from this report that a human reliability analysis was made in order to arrive at a probabilistic risk assessment due to human error. Chan et al (1987, p. 13), "model" the occurrence of the human errors by assuming that two basic errors occurred.

(a) Failure to follow written test or calibration procedures: HEP=8.1×10^{-2}

(b) Special short term one-of-a-kind checking with alerting factors: HEP=8.1×10^{-2}

They then compute the composite human error probability as:

$$(8.1 \times 10^{-2}) \cdot (8.1 \times 10^{-2}) = 6.56 \times 10^{-3}$$

It is not clear that this simplistic treatment models what had occurred in the July 25, 1987 incident. However, let it be assumed that the modeling is adequate.

Now the relevant material from Swain and Guttman (1983) is quoted: From Table 16-1 "Failure of Administrative Control", item 6: Failure to use written test or calibration procedures:

HEP = 0.05; E.F. = 5

The upper bound (95th percentile):

$$=(HEP)\ (E.F.) = 5 \times 0.05 = 0.25$$

From Table 20-22, p. 20-38 (or Table 19-1): Item 3: Special short-term, one-of-a-kind checking with alerting factors:

HEP = 0.05; E.F. = 5

The upper bound (95th percentile) = (HEP) (E.F.) = 0.25

The composite probability is now computed as:

$$(0.25)\ (0.25) = 6.25 \times 10^{-2}$$

This exceeds the Chan et al (1987) report number (6.56×10^{-3}) by approximately a factor of 10.

If one uses the Chan et al (1987) value of HEP = 8.1×10^{-2}, then the composite probability, based on upper bounds to reach the 95th percentiles becomes:

$$(8.1 \times 10^{-2})\ (5)\ (8.1 \times 10^{-2})\ (5) = 0.164$$

This exceeds the Chan et al (1987) number by a factor of 25.

The use of the 95th percentile is prudent and conservative. Despite all the calculations, one is left with a sense of great uncertainty because of the inherent difficulty in modeling this complex situation, and almost a complete lack of hard data, except of course for the harsh fact of the July 25, 1987 incident.

4.3 Component Failure Rates: Point Estimate Mean vs. Upper Bound Value at the 95th Percentile (90% Confidence Interval).

Chan et al (1987) state, "all failure data used was recorded as a point estimate mean. An uncertainty analysis was not performed for this project, (p. 12)."

This point has been previously addressed in Sections 4.1 and 4.2 of this report. The argument in both cases has been that it is conservative to assume that the probability of exceeding the selected parameter values is less than 5%, corresponding to a 90% confidence interval, or 2 1/2%, corresponding to a 95% confidence interval, depending on the choices made. The same situation holds for the choice of a component failure rate. Chan et al (1987) turn to industry, particularly the nuclear power plant industry, for its collective experience. This is entirely appropriate. One of their references is: "Common Cause Fault Rates for Valves (Steverson et al, 1983)." This report states, "Every estimated quantity is estimated by both a point estimate and by a 90% confidence interval. Many of the intervals are rather wide, reflecting the observed plant-to-plant variability (p.iii)." On this basis it is clear that when Chan et al (1987) choose the point estimate, usually a mean or a median, they have accepted the possibility that the selected value for their case may be exceeded by approximately 50% (in the case of a median) of the plants' data bank from which they selected a value. To be conservative one may choose an upper bound value, corresponding to a 90% confidence interval, as is done in the quoted reference (Steverson et al, 1983). The key component failure rates which figure significantly in the analysis and are listed in Table 2-1 of Chan et al (1987) (reproduced in Appendix G), are as follows:

Component	Failure Mode	Failure Rate
(a) Dump Valve	Proposed dump valve for system fails	2.89×10^{-6} per hr
(b) Valve 51	Directional 4 way valve fails blocking flow	1.45×10^{-6} per hr
(c) Valve 45	Solenoid operated valve plugs	2.89×10^{-6} per hr

The source for these values is given by Chan et al (1987) as IEEE Std. 500-1984, p. 1150, which lists data for solenoid valves sizes 2-3.99 inches. This reference states that when data were available which were amenable to statistical treatment (see page 20, section 2.3), values are given as confidence bands in addition to a recommended (Rec) value. The IEEE Standard lists the values for these solenoid valves as follows:

Failure Mode	Failure/10^6 hours		
	Low	Rec	High
All modes	0.72	2.89	11.6

It is assumed that the high values correspond to a 90% confidence interval, which appears to be an industry standard. The upper bound value 11.6 is just about 4X the Rec value of 2.89. Thus, a factor of 4X is suggested as a reasonable choice.

While a 90% confidence interval is used for the component failure rates and for the maintenance/operator errors, a stricter limit of a 95% confidence interval was used in defining the upper bound value for the frequency of electric power failure. The reason for the distinction stems from the fact that the value for electric power failure appears in <u>each</u> and <u>every</u> scenario leading to a catastrophic accident. Also, each scenario contains two or three events before a catastrophe occurs. With an uncertainty factor present in the value for each component, it is clear that the entire scenario has a greater uncertainty as far as numerical

values are concerned than is the case for each individual component. This is an additional justification for the 95% confidence interval employed for electric power failure.

4.4 Summary of Correction Factors

Based on the discussion in Sections 4.1 to 4.3, the correction factors to be used can be summarized as below:

	Reason for Corrections	Correction Factor
a)	Two Waste handling Shifts per day:	2X
b)	Frequency of electric power failure With a confidence interval of 95% that true value of will not exceed 4.6 1/yr:.....	6.6X
	With a confidence interval of 98% that the true value of will not exceed 9.4 1/yr:.....	11.9X
	time at risk, S = 0.055 yrs	
c)	Human Error(Maintenance plus operator Error) With a confidence interval of 90%:	
	For HEP = 0.05, EF = 5	10X
	For HEP = 0.081, EF = 5	25X
d)	Component Failure Rates: Point Estimate Mean vs. Upper Bound Value at the 95% Percentile (90% Confidence Interval)	4X

Of these four factors the first two (a,b) are multiplicative for the total value of the probability of catastrophic failure. However, factors (c) and (d) apply to a limited number of the cases listed in Table 4.1-1 (Chan et al, 1987). This table has been analyzed earlier in this report with a partition of values contributing to the annual probability of a catastrophic accident. The partition found is repeated for convenience:

Failure Reason	Valves 45,51	Relative Percent
local fault	0.445×10^{-3}	51%
maintenance plus operator error	0.424×10^{-3}	49%

Thus factor (c) (human error, etc.) applies to only 49%, and factor (d) (component failure) applies to the remaining 51%. For convenience, these percentages will both be treated as 50%.

e) There is a fifth correction factor associated with the value chosen for the component failure rate for the proposed dump valves. Based on the arguments already set out, a factor 4X is chosen. This choice applies to the entire value of the calculated annual probability of a catastrophic accident.

CORRECTION FACTORS FOR CALCULATED
PROBABILITY OF A CATASTROPHIC WASTE HOIST ACCIDENT

ITEM	CONFIDENCE INTERVAL	CORRECTION FACTOR
a) Two waste shifts/day		2X
b) Frequency of electric power failure	98%	11.9X
time at risk, S=0.055 yrs	95%	6.6X
c) Human error(maintenance plus operator error)		
HEP=0.05, EF=5	90%	10X
HEP=0.081, EF=5	90%	25X
(Apply 50% factor)		
d) Component Failure (Valves 45, 51)		
(Apply 50% factor)	90%	4X
e) Proposed Dump Valves Failure		
Common cause failure	90%	4X

There are two alternatives for item (b), and two for item (c). That makes a total of 4 cases possible, listed below:

		Composite Factor
Case I:		
(a) :	2X	
(b) :	11.9X	
(c),(d) :	(1/2x10+1/2x4)	
(e) :	4X	666
Case II:		
(a) :	2X	
(b) :	6.6X	
(c),(d) :	(1/2x10+1/2x4)	
(e) :	4X	370
Case III:		
(a) :	2X	
(b) :	11.9X	
(c),(d) :	(1/2x25+1/2x4)	
(e) :	4X	1380
Case IV:		
(a) :	2X	
(b) :	6.6X	
(c),(d) :	(1/2x25+1/2x4)	
(e) :	4X	766

If one chooses a geometric mean of the 4 composite values, one obtains:

714

This factor applied as a correction to sensitivity Case I, Table 4.1-4, page 39, (Chan et al, 1987) produces:

$$5.2 \times 10^{-8} \times 714 = 3.7 \times 10^{-5}$$

as the estimated annual probability of a catastrophic waste hoist accident.

The probability can be restated as corresponding to an annual rate of occurrence of approximately one in 27,000.

5. CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

A few salient points emerge from this analysis of the Chan et al (1987) report on the WIPP waste hoist system. In a number of ways this report is a significant improvement in its treatment of the probability of a catastrophic accident of the waste hoist system as compared with the previous report, Banz et al (1985). The 1987 report deals specifically with the waste hoist as it exists, considers the engineering design, the components employed and, most importantly, includes the possibility of human error. The 1985 report did not consider any of these factors, and was too general and non-specific. Indeed when EEG in 1985 (Appendix A) suggested the need to consider risks arising from human error, DOE's response (Appendix B) was insubstantial, stating that human error "was judged to be a negligible contributor to the total probability of a catastrophic hoist accident at WIPP." The July 25, 1987 incident which was in part due to human error, changed the perspective on this issue. DOE is to be commended for promptly re-examining the basis for an accident analysis of the waste hoist system, and issuing the Chan et al (1987) report.

The DOE WIPP Project Office (DOE/WPO) did not recognize the Chan et al (1987) report in the WIPP draft Final Safety Analysis Report (FSAR) (U.S. DOE, June 1989). The Failure Modes, Effects and Criticality Analysis in Chapter 4 of the FSAR also failed to mention any scenario failure which was similar to the incident which occurred on July 25, 1987. The FSAR referenced only the Banz et al (1985) report as a basis for assuming an annual probability for a hoist accident of 1.7×10^{-8}. EEG objected to this assumption in their comments on the FSAR (EEG-1989), and questions also were raised concerning this low probability by the DOE Office of the Deputy Assistant Secretary for Safety, Health, and Quality Assurance. Their comments on the FSAR were detailed

in a Safety Evaluation Report (SER), (U.S. DOE, July 1989). The DOE/WPO, in responding to this comment in the SER, again referenced the Banz et al (1985) report and failed to recognize the Chan et al (1987) report. In fact, the Chan et al (1987) report made an analysis of the waste hoist system in the light of the July 25, 1987 incident and calculated an annual probability of 1×10^{-3}, a factor of approximately 60,000 greater than the 1.7×10^{-8} of Banz et al (1985).

There are two points of interest concerning the comments in the SER: The SER expressed concern because the 1.7×10^{-8} "appeared low". The second point is that the authors of this comment appear to be unaware of the waste hoist "unusual occurrence" on July 25, 1987, and the Chan et al (1987) report that followed. The DOE/WPO response failed to enlighten them concerning either.

This comment in the SER addressed 3 questions (a, b, c) concerning the waste hoist accident probability that are pertinent. The first (a) relates to safety aspects of the redundant cable system, which was responded to adequately by the DOE/WPO. However, the following two questions (b, c) had inadequate responses, as follows:

(b) The question challenged the use of past accident data from MSHA since "significant design differences may exist between the WIPP hoist and hoists in the MSHA report, or even among the hoists in the MSHA report." EEG had raised the same objection in 1985.

The DOE/WPO response ignored the fact of the July 25, 1987 incident and the existence of the Chan et al (1987) report. The response referred to redundance and the fact that "WIPP's hoist is fully automatic." Yet these features did not prevent the 1987 incident. The response referred to a "more rigorous preventive

maintenance and inspection program." However, the Class C Investigation, dated October 15, 1987, an "Uncontrolled Movement of Waste Hoist Investigation Report" (Appendix F) was highly critical of the Quality Assurance program, maintenance procedures, contractors performing warranty work at WIPP, the "Person in Charge" program to provide oversight, and much more. It appeared that the author of the DOE/WPO response was completely unaware of the existence of the Class C Investigation. In fact it was a design feature that was peculiar to the existing waste hoist system, plus human error, that was responsible for the incident.

(c) The SER also raised the question about calculating probabilities "based on a limited number of accident data." The comment continued with the advice to "provide the expected statistical error due to the small size."

The DOE/WPO response was not germane to the question. It simply referred to the "large number of operational hoists." It is exactly this matter of small sample size and uncertainties in the available data which is the core of the present analysis. As a consequence of these factors, this report has calculated an annual probability of a catastrophic accident in the waste hoist system of one in 27,000.

The analysis by Chan et al (1987) yielded the annual probability of a catastrophic accident to be 1 in 1000. With the assumption of design changes, they calculated a probability of 1 in 20 million. Even ignoring the fact that the design changes are only assumed and not actually implemented, the revised projection of Chan et al (1987) is not sufficiently conservative for the following reasons:

(a) Calculation of the probability of loss of electric power, which appears in <u>each</u> cutset of the calculation for a catastrophic accident.

(b) Calculation of human error probability in terms of a median value, instead of employing a 90% confidence interval.

(c) Calculation of failure of components in terms of a point estimate mean, instead of employing a 90% confidence interval.

Taken together, employing a more conservative approach leads to a correction factor of almost 3 orders of magnitude. This changes the estimated annual probability of a catastrophic waste hoist accident from approximately one per 20 million (Chan, 1987) to one in 27,000 (this report).

5.2 Recommendations

It is hoped that DOE will consider adopting EEG's conservative approach. DOE may also wish to consider the usefulness of some re-design in the waste hoist braking system to properly exploit the presence of the two redundant and independent pressure supply units and sets of disc brake units. A re-design should make it impossible to have a brake system failure unless there are truly <u>independent</u> and <u>simultaneous</u> failures of all the components in the braking system. Evidently the present design is not at this stage, based on the experience of the July 25, 1987 incident. Until significant changes in the hoist system design are made that will justify reducing the probability of a catastrophic accident, such an accident should be considered credible and the project should be prepared to deal with the probability of 1 in 1000 that such an accident may occur in any given year during the 25 year operational life of the WIPP project. The dose consequences of such an accident should be evaluated in the Safety Analysis Report for WIPP.

6. REFERENCES

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

Chan, J.K.K., Iacovino, J.M., and Maher, S.T., December 1987, Quantitative fault tree analysis of the Waste Isolation Pilot Plant waste hoist hydraulic brake system: Section 6 of Operational Readiness Review, v. 2, U.S. Department of Energy, July 1988, DOE/WIPP-88-022.

Environmental Evaluation Group, May 1989, Review of the final safety analysis report (draft), DOE Waste Isolation Pilot Plant, December 1988, EEG-40 (DOE/AL/10752-40).

Harris, P.A., Ligon, D.M., and Stamatelatos, M.G., July 1985, High-level waste preclosure systems safety analysis phase 1, final report, NUREG/CR-4303, SAND85-7192, GA-A17670.

Institute of Electrical and Electronics Engineers, Inc., 1983, IEEE guide to the collection and presentation of electrical, electronic, sensing component, and mechanical equipment reliability data for nuclear-power generating stations, John Wiley & Sons, IEEE Std. 500-1984.

Sachs, Lothar, 1984, Applied Statistics - A Handbook of Techniques, Second Edition, Springer-Verlag New York, Inc.

Steverson, J.A. and Atwood, C.L., February 1983, Common cause fault rates for valves, U.S. Nuclear Regulatory Commission Report, NUREG/CR-2770.

Swain, A.D. and Guttman, H.E., August 1983, Handbook of human reliability analysis with emphasis on nuclear power applications, U.S. Nuclear Regulatory Commission Report, NUREG/CR-1278.

U.S. Department of Energy, June 1989, Final safety analysis report, Waste Isolation Pilot Plant, WP-02-9, Rev. 0, 5 volumes.

U.S. Department of Energy, July 1989, Waste Isolation Pilot Plant Safety Evaluation Report. Prepared by the Safety, Health and Quality Assurance Office of U. S. Department of Energy, Washington, D.C.

7. APPENDICES

7.1 Appendix A - (a) December 2, 1985 Letter by R.H. Neill to W.R. Cooper; (b) Excerpts: EEG Comments on Risk of Catastrophic Hoist Accident at the Waste Isolation Pilot Plant.

"Equal Opportunity Employer"

HEALTH & ENVIRONMENT department

STATE OF NEW MEXICO

ENVIRONMENTAL EVALUATION GROUP
320 E. MARCY STREET
P.O. BOX 968
SANTA FE, NEW MEXICO 87503
(505) 827-8280

December 2, 1985

Mr. W. R. Cooper
WIPP Project Manager
WIPP Project Office
P. O. Box 3090
Carlsbad, New Mexico 88220

Dear Mr. Cooper:

Subject: WTSD-TME-063, "Risk of Catastrophic Hoist Accident at the Waste Isolation Pilot Plant", forwarded with letter WIPP:RAC 85:206, 9/16/85

Attached are our comments prepared by Dr. Peter Spiegler on the above referenced report. We do not believe that the analysis presented in the report is objective. There is one obvious mathematical error. Several assumptions are not conservative even though the report makes that claim. It is our belief that the annual probability of a catastrophic hoist accident at the WIPP is not less than one in 58 million as described in the subject DOE report but is probably greater than one in 1 million. Therefore, we believe that the catastrophic hoist accident scenarios should not be deleted from the Safety Analysis Report (SAR) or from the Final Environmental Impact Statement (FEIS).

Futhermore, the WTSD-TME-063 report should be withdrawn and revised taking into consideration the attached EEG comments.

Thank you for allowing us to comment on this report. If you have any further questions on our comments please contact Dr. P. Spiegler.

To: W. R. Cooper
December 2, 1985

Please let me know by December 22, 1985 what action you intend to take in response to our comments and recommendations.

Sincerely,

Robert H. Neill

Robert H. Neill
Director

RHN:to

cc: Peter Spiegler
Dennis Krenz

Excerpts from

RECEIVED
ENVIRONMENTAL EVALUATION GROUP

EEG COMMENTS

on

RISK OF CATASTROPHIC HOIST ACCIDENT AT THE

WASTE ISOLATION PILOT PLANT

WTSD-TME-063

As the report states, the dominant hoist accident sequences are associated with power and brake system failure, accounting for 90% of the total accident sequences (see Table 6-2 of WTSD-TME-063). Thus it is appropriate to consider carefully the calculation of the annual probability of a power loss, stated as 0.034 in TABLE 5-2, and based on a calculation given on page 27 of WTSD-TME-063.

The calculation of the key parameter theta =lambda*S requires estimations of both lambda, the number of power losses per year, and S, <u>the time interval at risk</u>.

To make the calculation of the time at risk truly conservative a number of factors must be added that were not considered in the report. One factor is the possibility that WIPP will operate with more than one waste handling shift per day. The original design of WIPP included four shafts, which allowed for three waste handling shifts per day. Cost saving measures reduced the number of shafts to three and the possible number of waste handling shifts to two. Actually, because of difficulty with the mining machine and some concerns with the ventillation system, there have been suggestions lately to bring back the fourth shaft. Thus a factor of 2 or 3 is indicated on a <u>conservative</u> basis, for the interval at risk. A second factor relates to the assumption of 10 min per hoist trip, the time required "for a trip from the waste handling building to the repository horizon". The <u>time at risk</u> clearly needs to include the loading time as well as travel time. Thus 20 min to 30 min is more realistic than 10 min giving another factor of 2 or 3 for a conservative estimation of the <u>time at risk</u>.

Yet another factor is the duration of the power outage, which WTSD-TME-063 ignores. Half hour outages have been common in parts of the city of Carlsbad due to electrical storms. In fact, on October 15 or 16, 1985, there were two power outages at the WIPP site with the first one lasting four hours. It is difficult to quantitate the impact on estimated <u>time at risk</u> due to the duration of a power outage. However, common sense tells us that a longer duration of a power outage increases the risk of a catastrophic occurrence, especially if a loaded hoist is about ready to travel down when the

power outage occurs. At the very least one may state that any final calculation of the annual probability of a catastrophic accident should have a good safety factor as a cushion over and above a pre-stated and required probability (e.g. the quoted factor of one in a million attributed to DOE).

Now let us turn our attention to lambda, the number of power losses per year. The choice of the report of lambda = 1 per year is based on the narrow data base of having three power outages during the year 1982, 1983, and 1984 (all three have been attributed to human error). The recent example of a large increase in number of deaths due to airplane accidents, after a number of years of markedly better experience, suggests that a lambda value based on three years experience is not a conservative choice. A safety factor of two for the value of lambda, to counteract the short period of observation, appears reasonable.

A summary of the factors which lead to a more conservative estimate of lanbda*S is as follows:

Factor for number of shifts:	2 or 3
Factor for loading time:	2 or 3
Factor for conservative choice of lambda	2
Factor for duration of power outage:	?
Combined factor	8 to 18 (plus ?)

If the reported value of lambda*S (=0.034) is multiplied by 8 or 18 then the value of

$$P = 1 - \exp^{-(lambda*S)} = 0.24 \text{ or } 0.46$$

The increases in the previous value of P (=0.034) are by factors of 7.1 or 13.6.

When applied to the estimate of one in 15 million, a probability range is obtained from approximately one in 2 million to one in 1 million (not counting the unknown factor associated with duration of a power outage).

Our attention turns now to the basic TABLE 5-1, which provides the basic accident data culled from MSHA sources. While these source materials have not been reviewed by us, the question arises wether the MSHA data are truly representative of industrial hoist accident experience in the United States. Are factors such as hoist load magnitude, length of cables similar to the situation at WIPP?

Another question relates to the lack of mention in the report of the nature of planned QA, and the nature and quality of the planned maintenance. If the calculated annual probability of a catastrophic hoist accident at WIPP is to be valid in years 2, 3, 4, etc. there is a presumption of appropriate maintenance. The report is silent on the issue.

The questions raised in our review of the draft version in April 1985 about human factors and operator errors are not addressed in WTSD-TME-063. Since power loss and brake system failures figure so importantly in the scenarios, it would be prudent to add at least two more scenarios to cover these possibilities. One scenario could be brake system failure plus human error: the second scenario could be power outage plus human error.

7.2 Appendix B - (a) December 20, 1985 Letter from W.R. Cooper to R.H. Neill; (b) Excerpts: Responses to EEG Comments on WTSD-TME-063, "Probability of a Catastrophic Hoist Accident at the Waste Isolation Pilot Plant."

Department of Energy
Albuquerque Operations Office
Waste Isolation Pilot Plant Project Office
P. O. Box 3090
Carlsbad, New Mexico 88221

DEC 20 1985

RECEIVED

DEC 23 1985

ENVIRONMENTAL
EVALUATION GROUP

Robert H. Neill, Director
ENVIRONMENTAL EVALUATION GROUP
State of New Mexico
P. O. Box 968
Santa Fe, NM 87504-0968

Dear Mr. Neill:

Enclosed are the WPO responses to your December 2, 1985, comments on WTSD-TME-063, "Probability of a Catastrophic Hoist Accident at the Waste Isolation Pilot Plant."

After careful review of the EEG comments, the WPO continues to believe that the conclusions reached in the report are valid. As indicated in the enclosed comments, there was no "mathematical error" in the report as suggested in your comments. The WPO considers assumptions made in the analysis to be conservative and the conclusion that a catastrophic hoist accident is not credible to be accurate.

We also see no evidence to support the EEG assertion that the analysis was not "objective."

Should you have any questions, please contact me or Dick Crawley of my staff.

Sincerely,

James R. Anderson
for W.R. Cooper
Project Manager

WIPP:RAC E85:282

Enclosure

cc:
C&C File
Dick Coleman, Westinghouse
Peter Speigler, EEG

Excerpts from

RESPONSES TO EEG COMMENTS ON WTSD-TME-063,

"PROBABILITY OF A CATASTROPHIC HOIST ACCIDENT

AT THE WASTE ISOLATION PILOT PLANT"

3. EEG Comment: EEG states that the analysis should have considered the possibility that WIPP will operate with more than one waste handling shift per day, and the possibility that a fourth shaft will be added.

   DOE Response As noted on page 5.1-2 of the WIPP Safety Analysis Report (SAR), current plans are for one waste handling shift per day. The analysis was performed for the current design of WIPP; it is not feasible to consider all possible modifications which may be implemented in the future.

7. EEG Comment: EEG states that the choice of lambda, the number of power losses per year, is not conservative since the data on which lambda is based is narrow in scope.

   DOE Response: Lambda is the average rate of occurrence of an event. Therefore, in some years there may be more than one power loss and in others there may be none. This random variability does not invalidate the average rate of occurrence. However, even if an additional factor of two is applied to the value of lambda, the resulting probability of a catastrophic hoist accident would be approximately 3E-8 per year, which is not considered credible.

9. EEG Comment: EEG states that the nature of planned QA and maintenance should be addressed in the report.

   DOE Response: Adequate maintenance and quality assurance efforts are assumed in this analysis. Specific plans regarding these efforts have not yet been finalized.

10. EEG Comment: EEG states that human factors and operator errors are not addressed in WTSD-TME-063, and suggests that two additional scenarios be considered: brake system failure plus human error, and power outage plus human error.

    DOE Response: Human error is addressed in Table 3-1 of the final report. It states as follows:

> "Inattentive hoist operation is a relatively frequent cause of hoisting mishaps. The WIPP hoist procedure is designed to virtually eliminate the human element. When transporting CH-TRU or RH-TRU waste, the hoist will be in an automated mode (Bechtel, 1984). The only human interaction involves pushing a single button to activate the lowering cycle."

Therefore, human error was judged to be a negligible contributor to the total probability of a catastrophic hoist accident at WIPP.

7.3 Appendix C - (a) July 28, 1987 Letter from J.K. Channell to R.H. Neill, on "Unusual Occurrence with WIPP Waste Hoist."
(b) July 28, 1987 Letter from R.H. Neill to T. Bahr et al.

HEALTH & ENVIRONMENT department

"Equal Opportunity Employer"

STATE OF NEW MEXICO

ENVIRONMENTAL EVALUATION GROUP

P.O. BOX 968
SANTA FE, NEW MEXICO 87504
(505) 827-0556

MEMORANDUM

TO: R. H. Neill

FROM: J. K. Channell

DATE: July 28, 1987

SUBJECT: "Unusual Occurrence" With WIPP Waste Hoist

On Saturday, July 25, 1987, during a "maintenance exercise" on the waste hoist system at WIPP, two unexpected upward movements of the waste hoist cage occurred. This happened when a leaky valve in the hydraulic system was replaced by a new valve. For unexplained reasons, this new valve in conjunction with other manual valves in the system caused a hydraulic overpressure. The waste hoist hydraulic system is designed to be "fail safe" in that loss of pressure causes the cage to stop whereas overpressure causes it to move. The first movement was 30 feet. While a worker was going to report this occurrence, the cage moved another 200 feet (no information was given about the speeds of these movements). The old valve was put back in the system and it works normally. The shaft is being used on a limited basis, "very carefully".

Tom Lukow, who reported the incident to me, said DOE considered the present design unacceptable and that it would have to be changed. They don't want a system that can have unexpected movement even during a maintenance exercise. There will be a report on the incident which we will get. No public announcement of the occurrence is planned. I did not ask, nor did Lukow mention, why EEG was not called until late Tuesday morning (July 28, 1987).

It is interesting to note that the WPO and EEG have been engaged in a disagreement for over a year about their contention that a hoist drop accident was an incredible event (probability of less than 10^{-6}/year) and need not be considered in accident scenarios.

JKC:mh

DCOF 7-3

"Equal Opportunity Employer"

HEALTH & ENVIRONMENT department

STATE OF NEW MEXICO

ENVIRONMENTAL EVALUATION GROUP

P.O BOX 968
SANTA FE, NEW MEXICO 87504
(505) 827-0556

M E M O R A N D U M

TO: Thomas Bahr, Secretary, Energy, Minerals & Natural Resources Dept.
Larry Gordon, Secretary, Health and Environment Dept.
Michael Burkhart, Director, Environmental Improvement Division
Vickie Fisher, Secretary, Taxation & Revenue Department
Dewey Lonsberry, Administrator, Highway Department

FROM: Robert H. Neill, Director, EEG, EID

DATE: July 28, 1987

The attached letter from Dr. James K. Channell summarizes a July 25th unusual occurrence event in the WIPP waste hoist system and is intended to keep you informed.

cc: Mr. Hal Stratton, Attorney General

7.4 Appendix D - August 5, 1987 Letter from R.H. Neill to J. Tillman, DOE, "Unusual Occurrence in the WIPP Waste Hoist System."

"Equal Opportunity Employer"

HEALTH & ENVIRONMENT department

STATE OF NEW MEXICO

ENVIRONMENTAL EVALUATION GROUP

P.O. BOX 968
SANTA FE, NEW MEXICO 87504
(505) 827-0556

August 5, 1987

Mr. Jack Tillman
WIPP Project Manager
P. O. Box 3090
Carlsbad, NM 88220

Dear Mr. Tillman:

You may find the attached correspondence between our offices interesting and helpful in light of the hoist incident in the WIPP Waste Shaft that occurred last week. The correspondence relates to your report "Probability of a Catastrophic Hoist Accident at the Waste Isolation Pilot Plant" WTSD-TME-063 and clearly documents our strong disagreement with your contractors' (Dravo and Westinghouse) assertion that a catastrophic hoist accident at WIPP is "not credible" or "extremely improbable". With respect to the possibility of human error, the DOE position was, "The WIPP hoist system is designed to virtually eliminate the human element, and thus human error was judged to be a negligible risk contributor." And your position on the cage failures, cage testing errors and equipment failures was that "these events are negligible risk contributors relative to other failure mechanisms."

This incident emphasizes the need for your office to be skeptical when your contractors are extremely optimistic about their design or analysis in the face of strong criticism from independent reviewers. We are looking forward to receiving a complete report of the incident from you and will be happy to discuss with you the proposed steps to make the hoist system as safe as it should be. We would like to receive from you an analysis of the changes in estimates of the probability of catastrophic hoist accidents at WIPP based on the new data from this incident. Also, while we appreciate Mr. Lukow informing us of the Saturday, August 1, 1987 incident on August 4, 1987, it should have been more timely.

Sincerely,

Robert H. Neill
Director

LC:cs

cc: Mr. James E. Bickel, Asst. Manager
Project & Energy Programs, ALO

Enclosure

DCOF 7-3

7.5 Appendix E - August 17, 1989 Letter from J. Tillman to R.H. Neill, including the UOR dated August 11, 1987 (UOR=Unusual Occurrence Report).

Department of Energy
Albuquerque Operations Office
Waste Isolation Pilot Plant Project Office
P. O. Box 3090
Carlsbad, New Mexico 88221

RECEIVED
AUG 19 1987
ENVIRONMENTAL EVALUATION GROUP

AUG 17 1987

RHN

Mr. Robert H. Neill, Director
Environmental Evaluation Group
State of New Mexico
P.O. Box 968
Santa Fe, NM 87503

Dear Mr. Neill:

In response to your letter, dated August 5, 1987, enclosed is the Unusual Occurrence Report that was prepared following the incident that occurred on July 25, 1987, while the Waste Hoist was out of service for maintenance. The incident is under further investigation and you will be provided with a copy of the published report. Please note that Mr. Lukow contacted you about the incident on July 28, 1987 and not August 4, 1987 as noted in your letter.

Following the implementation of the recommendations contained in the report, you will be informed of alterations to the estimates used by the Project to evaluate the probabilities of a catastrophic Waste Hoist accident when transporting wastes.

Sincerely,

Jack B. Tillman
Project Manager

Enclosure

cc w/Enclosure:
C&C File
J. Kenney/R. McFarland, EEG

cc w/o Enclosure:
R. Coleman, WID

WIPP:TEL E87-0110

RECEIVED
AUG 19 1987
ENVIRONMENTAL EVALUATION GROUP

8.3 UNUSUAL OCCURRENCE REPORT FORMAT

FORMAT (Spacing of items in following example may be altered as necessary to provide adequate space for full exposition of items).

NAME OF SITE AND/OR CONTRACTOR

Page 1 of 5

1. UOR Number UOR:87:003

2. Status and Date: Initial 7/27/87
Interim 8/11/87
Final

3. Site:

Waste Isolation Division - WIPP

4. Facility, System, or Equipment: Waste Handling Hoist

5. Date of Occurrence: 7/25/87

6. Time of Occurrence: 11:00am

7. Subject of Occurrence: Unplanned release of hoist brakes causing uncontrolled motion of conveyance.

8. Apparent Cause: Design xx Material xx Personnel xx Procedure ..
Other ____ (Explain in Item 9)
NOTE: This incident resulted from a combination of the identified causes.

9. Description of Occurrence: Two unplanned releases of the Waste Hoist disc brakes occurred during warranty work on the hoist brake hydraulic system. Because neither the conveyance nor the counterweight was blocked, nor the brakes isolated, the brakes released resulting in the uncontrolled upward movement of the conveyance due to the unbalanced condition (CONTINUED)

10. Operating Conditions of Facility at Time of Occurrence:
waste hoist turned over and operational, project in a startup phase.

11. Immediate Evaluation:
Improper installation or function of replacement valve allowed counterweight to descend and conveyance to ascend without braking or motor controls. Insufficient work preparation and control. The system design needs additional failsafe features.

12. Immediate Action Taken and Results: Stopped all warranty repair work. Removed replacement valve and reinstalled original valve. Inspected braking components and fluid power system for visual damage or anomalies. Physically tested hydraulic power unit performance while isolated from brakes, tested each brake pedestal independently to provide a secured hoist while (CONTINUED)

13. Is Further Evaluation Required? Yes x No ____

If Yes, Before Further Operations? Yes ____ No x

If Yes, By Whom? Mine Eng., Safety, Maintenance, QA, Mining Ops., Manufacturer

When? Preliminary by 7/28/87, Final by 9/-/87.

Interim

14. **Evaluation and Lessons Learned:** There were several causative factors involving personnel, procedures, processes and hardware, and these factors contributed to inadvertant release of the Waste Handling Hoist brakes and two congruent unplanned, uncontrolled movements of the conveyance. The process involved the poorly executed replacement of a misapplied 2 position. (CON

15. **Corrective Action:**

Taken: X Recommended: _____ To Be Supplied: _____

SEE CONTINUATION SHEET.

16. **Programmatic Impact:**

None.

17. **Impact Codes and Standards:**

None.

18. **Similar Unusual Occurrence Report Numbers:**

None.

19. **Signatures (as a minimum):**

Originator H. L. Lucus [signature] A. Varga Date 8-12-87

Approved by:

MOC Manager, Operations [signature] Date 8-12-87

Manager, Safety/Security [signature] Date 8/13/87

Manager, Quality Assurance [signature] Date 8/12/87

WPO Manager, Safety/Security [signature] Date 8/13/87

20. **Distribution:**

MOC Operations Manager
MOC Quality Assurance Manager
MOC Safety and Security Manager
MOC Applicable Managers

WPO Safety and Security Manager
WPO Quality Assurance Manager
WPO Applicable Branch Managers
WPO Applicable Contractors
WPO EG&G CAIRS program if applicable
WPO ES&H Division, ALO if applicable

UNUSUAL OCCURRENCE REPORT CONTINUATION SHEET

CONTINUED:

9. Description of Occurance:

(i.e. 66,000 lb. conveyance vs. 104,000 lb. counterweight). The estimated distance of upward travel was 30 feet for the first event and 300 feet for the second incident. The conveyance was at the underground station at the time of the first incident. These incidents were associated with the installation and checkout of a replacement hydraulic 4 way valve (flow return directional valve). This valve was supplied by the Rexnord Company to WIPP to satisfy a warranty action involving excessive internal hydraulic leakage causing liquid transfer between the primary pressure unit and the stand-by system.

12. Immediate Action Taken and Results:

verifying brake valve performance. The hoist power was activated for limited travel and brake testing, which confirmed proper brake operations. The Hoist Operator then performed all operating safety tests of hoisting systems. Maintenance Department representatives performed a physical inspection of all hoist ropes, conducted a collar test and a rope "kick test". All systems and components were found to be in good operating order. The system was then tested in the various operating modes, no immediate problems or areas of concern were detected.

14. Interim Evaluation and Lessons Learned:

4 way, solenoid operated, directed control valve, which functions to direct hydraulic fluid in the low pressure return system to either the primary fluid storage system or to the standby fluid storage system. The replacement was being accomplished as part of a warranty action. During the process of waste hoist system turnover to the Management and Operating Contractor (MOC), the valve was identified for repair or replacement under warranty due to excessive bypassing leakage causing depletion of the oil inventory in the primary hydraulic system. The replacement valve was provided by the hoist hydraulic system supplier/designer and subsequent evaluation evidenced that the valve was not a suitable plug-in replacement. The presence of a plugged vent port and other factors resulted in configuration that blocked the hydraulic flow in the brake system return circuit. Blocking of the flow allowed pressurization and release of the hoist brake actuation cylinders and thus maintain the brakes in a disengaged position causing a [illegible]

NOTE: Please use this form when there is insufficient space for providing complete information on pages 1 and 2. Indicate the appropriate page number, UOR number, and UOR date. when entering information on this form, use the appropriate item number and title for each item carried over from pages 1 and 2.

UNUSUAL OCCURRENCE REPORT CONTINUATION SHEET

CONTINUED:

14. free fall of the counterweight and lifting of the conveyance. The initial valve receipt lacked proper documentation, such as drawings, installation procedures, safe checkout procedures and specifications. The second barrier, which failed, was the potential for the original construction/installation contractor personnel to stop the warranty action based on the absence of appropriate documentation and the physical difference in valve configuration. A third absent barrier was the lack of Quality Assurance input for this process. Installation procedures, drawings, hazards and/or failure mode analysis were not provided and the replacement/checkout was performed on a real-time, on the spot basis.

The primary deterrent missed was the accountability, responsibility, and operational control assigned to the responsible Operations group. The control is related to operations by qualified personnel and management using proven procedures issued to preclude inadvertant energy releases. The primary procedure is a lockout/tagout procedure, which specifically addresses electrical lockout as well as lockout of potential energy releases. The criteria translates to providing for physical retention of the hoist either through system balancing, chairing of the counterweight or very positive lockout of the brakes to prevent disengagement. The Operations personnel failed to exercise management control and stop the activity after the first inadvertant brake release. Up-front involvement by the Quality Assurance and Safety organizations would have resulted in a higher success potential.

In summary, the incident was characterized by a breakdown of barriers established in the WIPP modus-operandi to prevent unplanned events. Lack of good operational control is considered to be the most significant causation factor.

The lessons learned to date are summarized as follows:

1. Operational control over operational processes must be improved and specific accountability, ownership and responsibility must be established and maintained.
2. Processes which involve non-MOC personnel, must be better managed, controlled, and overviewed to ensure full compliance with WIPP work procedures.
3. Adequate documentation and data such as drawings, certifications, specifications, installation and checkout procedures must accompany critical replacement hardware. (CONTINUED)

NOTE: Please use this form when there is insufficient space for providing complete information on pages 1 and 2. Indicate the appropriate page number, UOR number, and UOR date. when entering information on this form, use the appropriate item number and title for each item carried over from pages 1 and 2.

UNUSUAL OCCURRENCE REPORT CONTINUATION SHEET

CONTINUED:

14. 4. The technical guidance and directions associated with work must be of sufficiently high quality to minimize incidences.
    5. The analysis of critical systems should include methods such as Failure Modes and Effects analysis to uncover any single point failure mechanisms.
    6. Procedures, such as the lockout/tagout procedure, must be understood and thoroughly implemented.
    7. The Quality Assurance and Safety functions must be involved in critical work processes to extract value from their expertise and overview.

15. Corrective Action:

    As of August 10, 1987, the following corrective actions have been taken:

    1. A task team, which was comprised of multi-disciplined (i.e. Safety, Training, Quality Assurance) investigators, interviewed the personnel, gathered data and is currently preparing a Class "C" investigation report.
    2. With appropriate consideration and forethought, disciplinary actions, which included time off without pay, were imposed on personnel who clearly performed poorly relative to this incident.
    3. A strongly worded letter was transmitted to the subsystem designer/hardware supplier to clearly identify the potential consequence of this incident and WIPP MOC expectations for critical component and system suppliers.
    4. Appropriate safety bulletins, internal MOC correspondence and department level meetings were used to disseminate accurate information and maximize the learning value derived from this incident.
    5. Critical valves have been locked out using physical locks and a comprehensive Failure Modes and Effects Analysis (FMEA) will be expeditiously completed to ensure identification of any single point failures and implement remedial actions quickly.

NOTE: Please use this form when there is insufficient space for providing complete information on pages 1 and 2. Indicate the appropriate page number, UOR number, and UOR date. When entering information on this form, use the appropriate item number and title for each item carried over from pages 1 and 2.

8.4 DISTRIBUTION LIST

The following is the minimum UOR distribution list:

8.4.1 Managing Operating Contractor

- o Operations Manager
- o Quality Assurance Manager
- o Safety and Security Manager
- o Applicable Managers

8.4.2 WIPP Project Office

- o Safety and Security Manager
- o Quality Assurance Manager
- o Applicable Branch Managers
- o Applicable Contractors
- o EG&G CAIRS program if applicable
- o ES&H Di sion, ALO if applicable

7.6 Appendix F - October 15, 1987 Abridged Version of Class C Investigation, "Uncontrolled Movement of Waste Hoist July 25, 1987."

CLASS C INVESTIGATION

INADVERTANT HOIST MOVEMENT

FINAL REPORT

WASTE ISOLATION PILOT PLANT
CARLSBAD, NEW MEXICO

UNCONTROLLED MOVEMENT OF WASTE HOIST

INVESTIGATION REPORT

JULY 25, 1987

CLASS "C" INVESTIGATION

FINAL

INVESTIGATION REPORT SUBMITTED: OCTOBER 15, 1987

WASTE ISOLATION PILOT PLANT

CARLSBAD, NEW MEXICO

TABLE OF CONTENTS

SECTION	TITLE	PAGE
	LIST OF FIGURES	ii
	LIST OF APPENDICES	iii
	LIST OF PHOTOGRAPHS	iv
I.	SCOPE	1
II.	SUMMARY	2
III.	FACTS	4
	A. Site Description	4
	B. Organization and Responsibilities	4
	C. Incident Details	5
IV.	ANALYSIS	9
	A. Background	9
	B. Evaluation	12
V.	RECOMMENDATIONS	17
	A. Design	17
	B. Administrative	17
VI.	SIGNATURES	19
VII.	APPENDICES	20

LIST OF FIGURES

Figure 1 - Project Participants

Figure 2 - WIPP Project Office Organization

Figure 3 - Managing Operating Contractor Organization

Figure 4 - Hydraulics System One Line Diagram

Figure 5 - Simplified Waste Hoist Hydraulic Schematic

Figure 6 - Simplified Waste Hoist Hydraulic Schematic

Figure 7 - Events and Causal Factors Sequence Chart

LIST OF APPENDICES

Appendix 1. - Waste Hoist Operations and Maintenance Manual

A. Hydraulic System Description

B. Disc Brake System Operation

Appendix 2. - Transmittal of Deficiencies: Waste Hoist

Appendix 3. - Unusual Occurrence Reports

A. Initial

B. Interim

Appendix 4. - Engineering Design Data - Racine Valve

Appendix 5. - Engineering Design Data - Oil Gear Valve

Appendix 6. - Waste Hoist Brake Release Sequence

Appendix 7. - Waste Hoist Brake System Analysis

Appendix 8. - New Mexico Hydraulics Test Reports

LIST OF PHOTOGRAPHS

Photograph 1. -Waste Hoist Hydraulics

Photograph 2. -Racine Valve in Operation

Photograph 3. -Valve Comparison

Photograph 4.- Valve Comparison

Photograph 5.- Racine Valve No.45

Photograph 6.- Racine Valve Baseplate

Photograph 7. - Oil Gear Valve No. 45

Photograph 8. - Oil Gear Valve Baseplate

UNCONTROLLED MOVEMENT OF WASTE HOIST

INVESTIGATION REPORT

I. SCOPE

As a result of the July 25, 1987 incident of two related uncontrolled movements of the Waste Isolation Pilot Plant Waste Handling Hoist and conveyance, an investigation board was formed and convened on July 27, 1987. The investigation board was tasked to investigate, to determine the cause or causes of the uncontrolled movements, and to make appropriate recommendations to prevent a recurrence.

The investigation included an analysis of the events that led to the "freewheel" of the Waste Hoist drum and the attached conveyance. Included in the analysis was a review of the procedures that were followed, the manufacturer's recommendations and directions for the use and repair of the hoist, the warranty repair process, the quality assurance process, the work control process, the design of the hoist system hydraulics, testing of the manufacturer-provided replacement parts, the operations and maintenance manual for the hoist system, and interviews with the cognizant engineer for the hoist repairs and the installation contractor employees who were performing the warranty work. Event and Causal Factors sequencing was used to determine the failure mode with a Change Analysis providing the key investigative direction.

II. SUMMARY

On July 25, 1987, at approximately 11:00 A.M. the first of two uncontrolled movements of the Waste Handling Hoist occurred. Representatives of Brinderson Construction Corporation were in the process of replacing, under warranty, a suspect malfunctioning valve in the hydraulics system of the Waste Hoist. The valve had been identified as a deficiency during pre-turnover testing. The valve malfunctioning was considered a nuisance factor in that excessive hydraulic fluid was being pumped to a (the) standby tank during the operation of the hoist. Approximately five percent (5%) of the fluid was being vented to the opposite tank during operation. During the operation of the primary pump, the fluid vented to the secondary (standby) pump tank. Also, during the operation of the secondary pump, the fluid was being vented to the primary tank. A level switch in the primary tank automatically switches to the secondary system when a low hydraulic fluid level is detected in the primary tank. A level switch in the secondary tank activates the Emergency Stop (E-Stop) function of the hoist when a low hydraulic fluid level is detected. Proper design of the system and function of the shunting valve should vent the hydraulic fluid only to the appropriate tank preventing a low level condition developing during normal operation of the hoist. Undesired activation of the E-Stop function of the waste hoist is less than adequate system performance. Administrative controls were being utilized to manually switch the pumps to prevent inadvertent activation of the E-stop function.

The manufacturer of the hoist system, Rexnord Inc., had agreed, under warranty, to supply a valve that would provide the desired function. A replacement valve was provided to be installed, and on July 25, this work was being done. The valve provided was of a different design and manufacturer and minor modifications were necessary to make the valve fit. However, to the persons doing the work, all appeared to be in order with normal field fit activities required. The replacement valve was installed, electrical connections made and the pump system was energized. At this time, the fluid from the secondary tank was transferred directly to the primary tank. The system was deenergized and the electrical connections were reversed and the system reenergized. At this time the brakes were hydraulically released resulting in the first uncontrolled movement or freewheel. The distance travelled by the conveyance was approximately thirty (30) feet. The system came to a halt on its own with the brakes resetting. The system is designed to require 1200 pounds per square inch to release the brakes to allow movement.

The brakes had apparently been released due to the impeded flow of fluid through the valve which created back pressure in the system. The pump system was deenergized and the valve was removed from the system. The valve was reexamined and the employees discovered that the valve could be reversed and the alignment dowels in the base of the valve would still fit.

At this time the valve was installed oriented one hundred eighty (180) degrees from the first installation. As a precaution, manual dump valves to the brakes were opened and the normally open hydraulic valves that provide hydraulic activation of the brakes were closed. The pump system was reenergized and the second freewheel of approximately three hundred (300) feet occurred. The Brinderson employees and the engineer made every effort to open or close valves that might have halted the freewheel to no apparent effect. The personnel cleared the area fearing the worst. Again, the hoist brakes set. At this time the system was returned to the original configuration, onsite QA was notified and callout notifications were made to management and the manufacturer.

An evaluation of the event was made, and on recommendation of the manufacturer, the system was returned to operation with the original valve reinstalled. Every effort was made to return the hoist to the conditions existing before the repair was undertaken. Preoperational tests of the hoist were made with checks of systems affected. The system was energized and run through operational tests before it was released to service. These actions were completed by approximately 9:00 P.M., on July 25, 1987. See Figure 7 for Events and Causal Factors Chart.

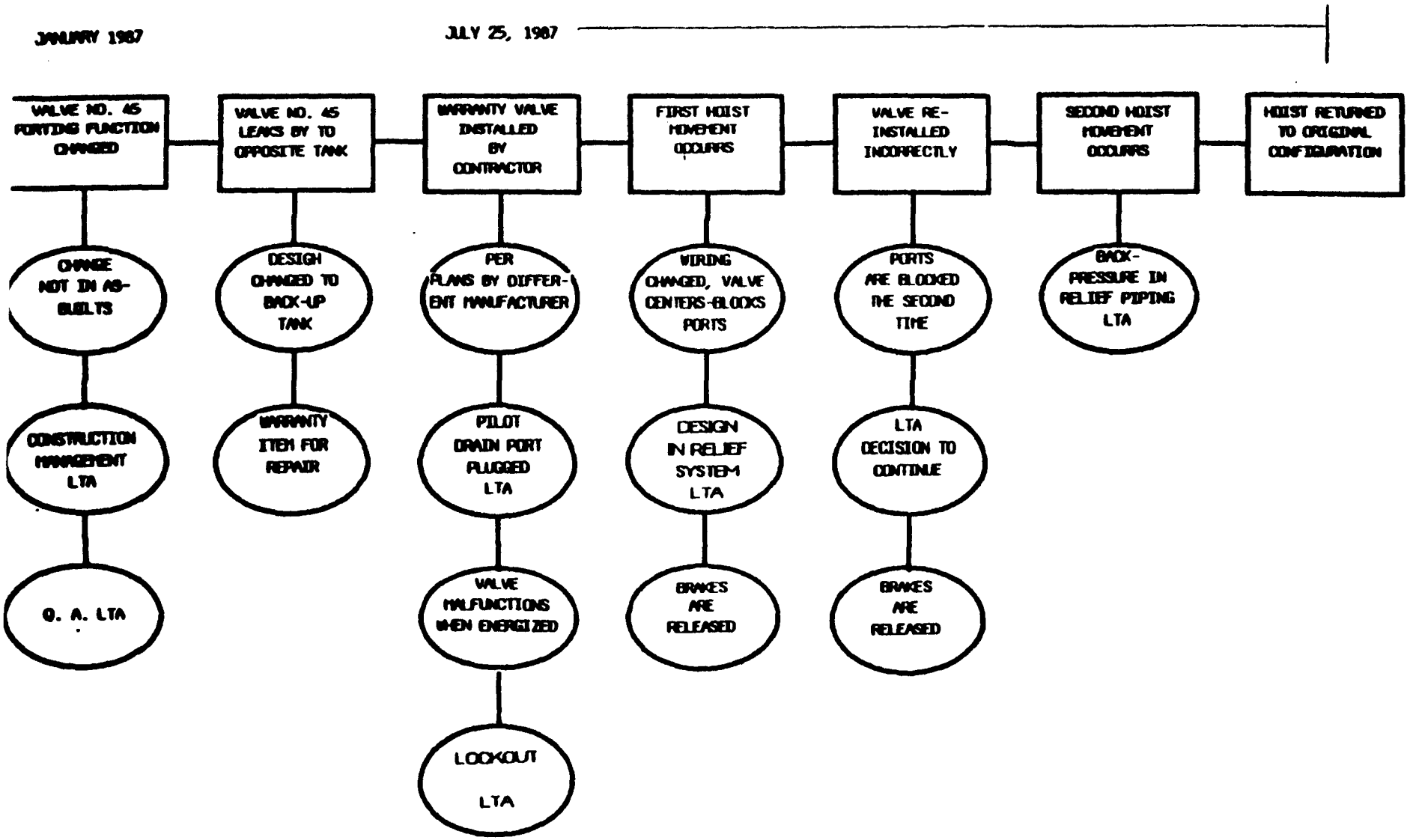


FIGURE 7 EVENTS AND CAUSAL FACTORS

III. FACTS

A. SITE DESCRIPTION

The Department of Energy (DOE) is constructing the Waste Isolation Pilot Plant (WIPP) in Southeastern New Mexico to perform Research and Development on the disposal of transuranic waste resulting from United States defense activities. This project has been authorized by Public Law 96-164. Certain radioactive wastes (called transuranic waste) are proposed to be permanently emplaced at WIPP.

The WIPP site is located approximately 30 miles southeast of Carlsbad, New Mexico, over the Permian Salt Basin. This 3,000 foot thick salt formation extends laterally for hundreds of miles in all directions from the site. The main storage area for the waste is at a depth of 2150 feet below ground level.

The project is nearing completion of the construction phase and is scheduled to begin receiving waste in October 1988.

B. Organization and Responsibilities

1. Organization

The DOE's Albuquerque Operations Office manages the WIPP Project. The DOE WIPP Project Office (WPO) is responsible for project integration, organization, and operational activities. Under WPO direction, the following organizations provide(d) scientific, engineering, and construction support to the Project:

Sandia National Laboratories - provides overall scientific support with emphasis on environmental issues, site characterization, and experimental programs.

Bechtel - provided architect/engineer services for facility design and inspection for the waste hoist system.

U.S. Army Corps of Engineers - provided facility construction and construction management services for the waste hoist system

The WIPP facility is managed and operated by the Waste Isolation Division of the Westinghouse Electric Corporation. The Waste Isolation

Division will hereafter be referred to as Westinghouse. See Figure 1. for the Project Participant Organizational Chart.

2. Responsibilities

a. DOE WIPP Project Office.
The DOE WIPP Project Manager has the overall responsibility and authority for WIPP activities. The WPO is staffed to provide managerial direction and overview of all site activities. See Figure 2 for WPO Organization.

b. Waste Isolation Division, Westinghouse Electric Corporation.
Westinghouse is the Managing Operating Contractor for the WIPP Project. Westinghouse has the responsibility for operating and maintaining facilities as directed by the WPO., including the surface and underground facilities at the WIPP Site and the Trupact facilities and office spaces maintained in the City of Carlsbad. Westinghouse also acts as Construction Manager for newly contracted construction as may be directed by the WPO. See Figure 3 for MOC Organization.

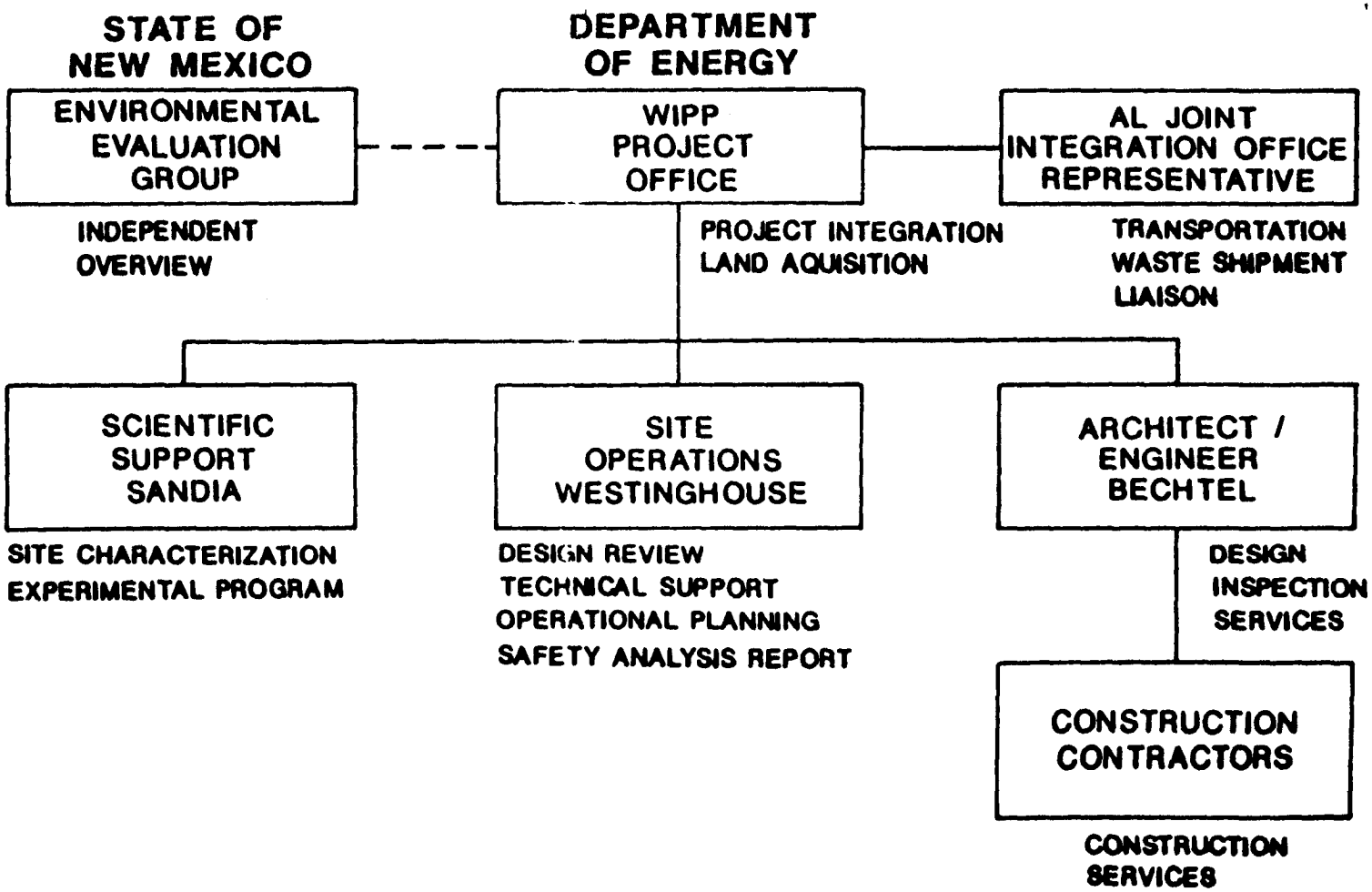
c. Bechtel, as the architect for the WIPP facilities constructed to date provided the facility design and inspection services. The waste hoist design specifications were provided by Bechtel.

d. The U.S Army Corps of Engineers provided construction management services for the Waste hoist and continues to be the intermediary concerning items of warranty. Brinderson Corporation contracted to the U.S.A.C.E. for construction of the Waste Hoist system. Rexnord Inc. subcontracted to Brinderson for the design and manufacture of the Waste Hoist System. Oil Gear subcontracted to Rexnord to supply the Brake hydraulic system parts to Rexnord specifications.

C. Incident Details

Valve 45 (solenoid control valve #7 manufactured by Racine),

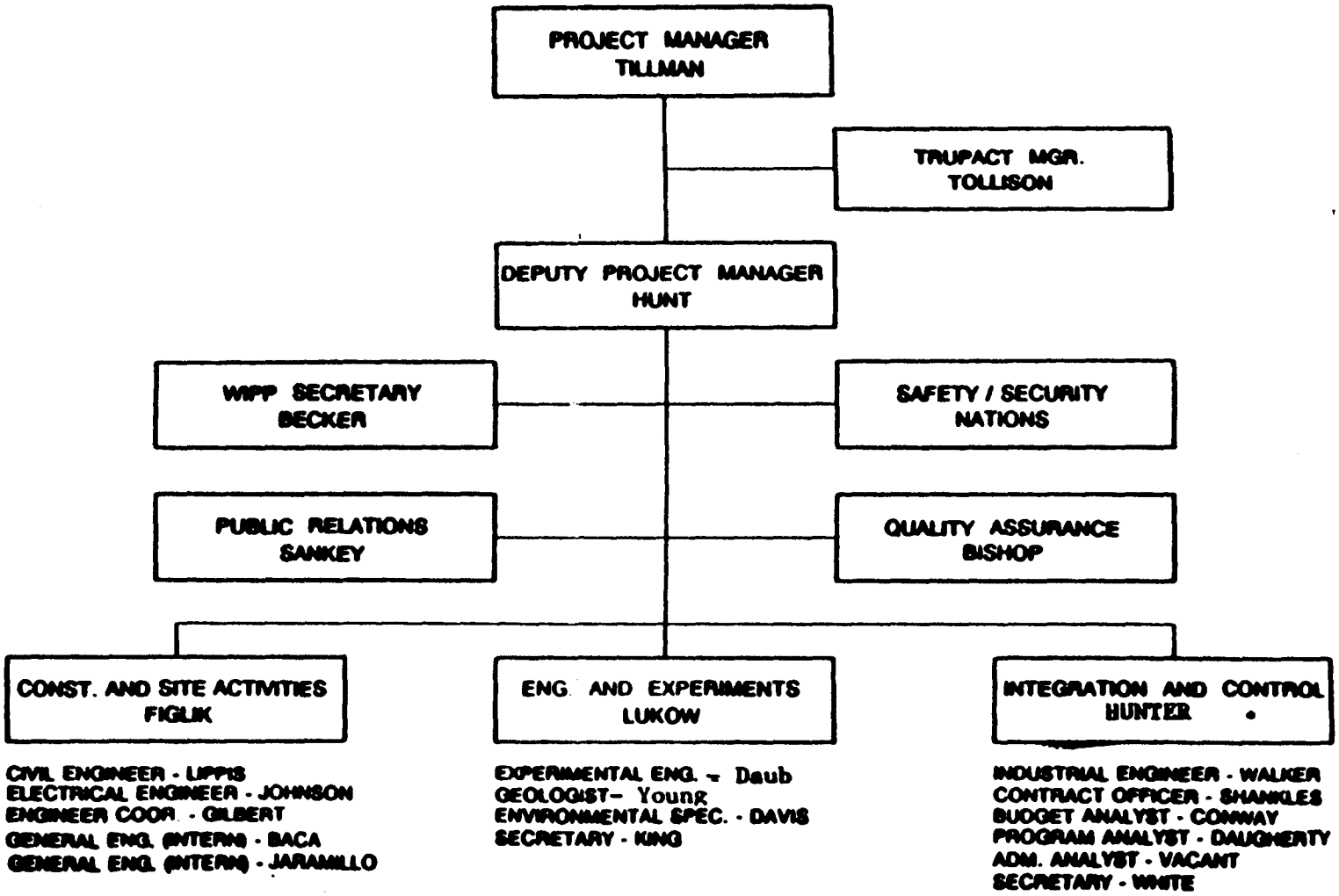
PROJECT PARTICIPANTS



887:1722

FIGURE 1

WIPP PROJECT OFFICE



FUNCTIONS

CONSTRUCTION
FACILITIES
MAINTENANCE
FACILITIES ENGINEERING

IN SITU TESTING
SITE CHARACTERIZATION
INSTITUTIONAL
RW COORDINATION
ENVIRONMENTAL

OPERATIONS
WASTE MANAGEMENT
PROJECT CONTROL
ADMINISTRATION
FINANCIAL MANAGEMENT
CONTRACTS

• ACTING

FIGURE 2

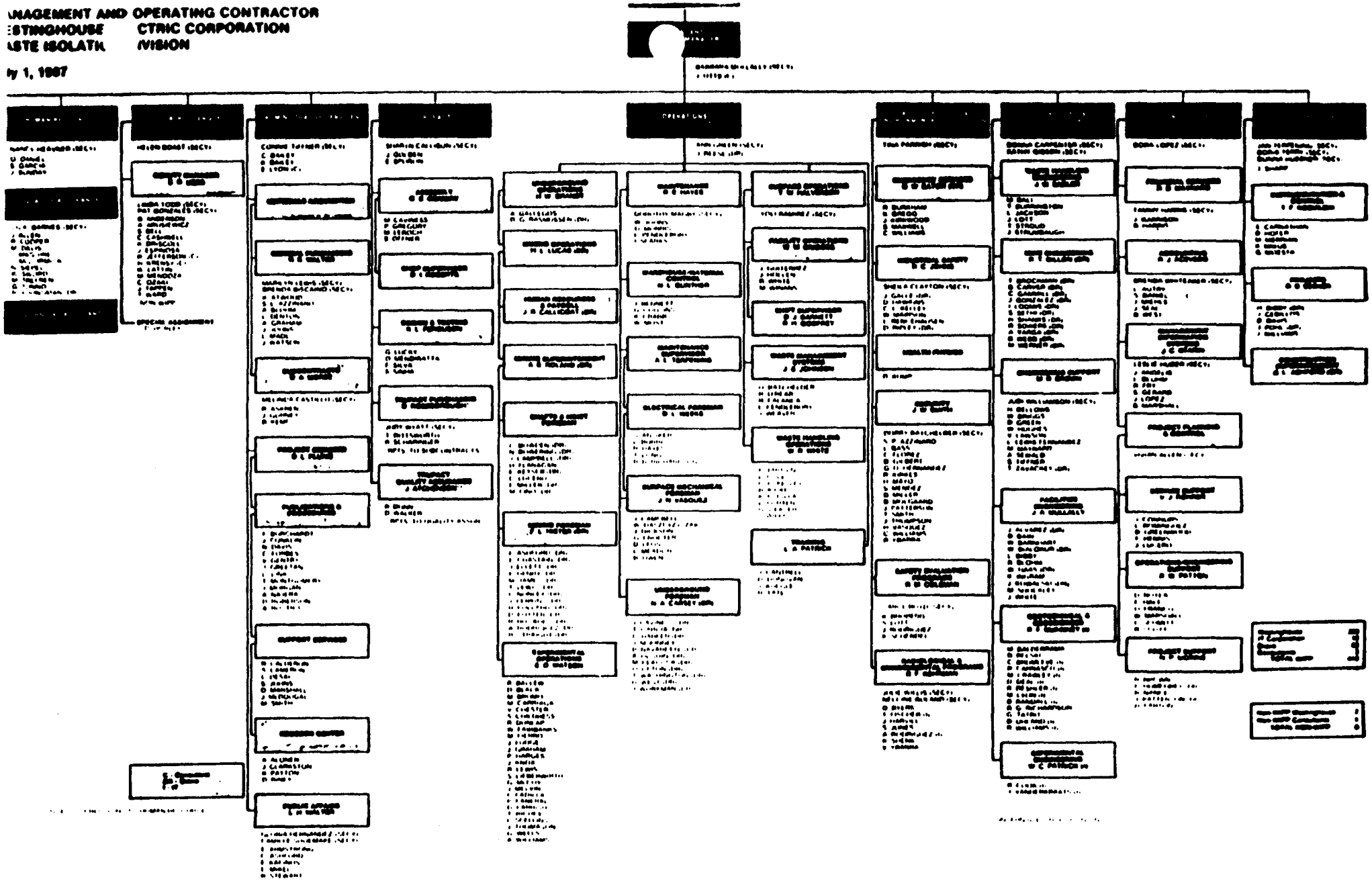

\NAGEMENT AND OPERATING CONTRACTOR
:STINGHOUSE CTRIC CORPORATION
\STE ISOLATI /IVISION
ly 1, 1987

FIGURE 3

provided by the manufacturer Rexnord, was identified as a deficiency in the pre-operational turnover testing.

Approximately five percent of the hydraulic fluid vents/seeps into the wrong tank. The valve was targeted by Rexnord as the source of this seepage.

After the valve had been determined during pre-turnover testing to be malfunctioning, the spare parts inventory valve was installed to determine if the installed valve was defective. The replacement valve, also manufactured by Racine, was determined to function the same as the valve originally installed.

Rexnord provided, under warranty, a replacement valve manufactured by Oil Gear to correct the venting problem.

The Oil Gear replacement valve provided by Rexnord was not accompanied with design engineering data, installation instructions, or changes to parts list and the Operations and Maintenance instructions to WIPP Operations.

Blockage of the valve 45 with the hydraulic pump(s) running provides, by design, a flow path for hydraulic fluid to provide pressure to release (all) of the hoist brakes.

The Hoistman's Emergency Stop button does not function unless there is control power. Without control power, all electrically operated valves move to the "failsafe" position.

With control power to the Hoistman's console, the Emergency Stop button activates valve numbers 25.1, 25.2, 25.3, and 25.4 which vent hydraulic fluid pressure through valve 45 to the reservoir.

Blockage of the valve 45, with or without control power, has the potential to release the brakes and inactivate the electrically operated limit switches and overspeed safeties designed into the system.

Valve 25.3 (and 25.1*) requires the Hoistman to operate the controls to release the brakes for the valve to provide a flowpath for the hydraulic fluid-pressure in normal operation. (*corresponding valve)

Valve 25.4 (and 25.2*) requires the motor to generate approximately 500 amps in the motor (torque proving) to provide a normal flowpath for the hydraulic fluid-pressure. Conversely, if the torque proving is not provided, the return line from the brake system is open.(*corresponding valve)

The current (as of July 1987) Operations and Maintenance Instruction Manual provided by Rexnord Inc. indicates the valve installed with the valve spool oriented in a 180 degree position to the actual operation position.

Tests performed on the Oil Gear replacement valve resulted in the valve spool being centered, blocking the ports.

The Oil Gear valve was specified and provided by the manufacturer with the pilot drain port plugged.

The porting arrangement on the Oil Gear valve, with the exception of the blocked pilot port, provides flow per the Operations and Maintenance Manual diagrams.

The counterweights weigh 104,000 pounds.

The conveyance weighs 66,000 pounds, plus the weight of the workdeck that has been installed which is 10,000 lbs.

The brakes were released and the hoist did move.

The conveyance was located at the mine level 2,150 feet below ground level, the position with the most potential energy.

The brakes are designed to automatically apply under the following circumstances:

1. Power failure

2. Loss of pressure in the brake operating system

3. Excessive brake lining wear

4. Overspeed

5. Overwinding (overtravel)

By design, retardation is controlled when the brake is applied under emergency conditions.

The brake furnished is a high pressure hydraulic disc brake, spring applied and pressure released.

Two sets of brakes are supplied; each set consist of three brake calipers with six disc brake pads. Each set of brakes is designed to stop and hold the design load.

The hydraulic fluid return for both sets of brakes flows through valve 45.

New Mexico Hydraulics performed functional tests of the Racine and Oil Gear Valves. These tests were observed by Westinghouse personnel. Functional tests of the Racine valve determined the flow path of "P" to "A" when deenergized, and "P" to "B" when energized. This is opposite of what is shown in the current Revision F of the hydraulic schematic in the Rexnord Inc. O & M Manual. The Racine valve tested was in service at the time of turnover of the Waste Hoist.

The Racine valve tested and the valve currently in use have been in service during the test periods and training conducted by Rexnord Inc. representatives.

The test of the Oil Gear valve when deenergized was from port "P" to "B" and when energized from port "P" to port "A" as indicated correct in the O & M Manual. However when the solenoid was again deenergized, the valve became centered and blocked all flow paths.

Removing the plug in the Oil Gear pilot port allowed the valve to operate and changed ports when energized/deenergized, however the flow was opposite to the Racine valve that is currently functioning in the Waste Hoist Hydraulic system.

Valve 45 has no normal on/off role. Regardless of the power situation, flow through 45 is assumed.

IV. ANALYSIS

A. Background

On July 25, 1987, repairs to the Waste Isolation Pilot Plant Waste Handling Hoist were being effected. Brinderson employees Bud Barnes and Curtis Kessler were working on a warranty repair under the oversight of Cognizant Engineer Al Varga representing the Managing Operating Contractor, Westinghouse. The Warranty item being replaced was the malfunctioning hydraulic return Valve 45. The problem with the valve is that during operation approximately five (5) percent of the hydraulic fluid leaks by the internal parts to the vent line to a hydraulic fluid storage tank. This venting or leaking is to the second of two tanks, either the primary tank or the secondary tank.

The brake system is hydraulically operated with essentially two complete braking systems, either of which is designed to support the design load of the system. Redundancy in the braking system is intended to provide a single failure "failsafe" braking system. The one-line diagrams provided in this report show mirror images in the braking system. There are two sets of brakes, each consisting of three disc brake calipers with six disc brake pads. There are also two pumps with each capable of providing the hydraulic pressure/flow necessary to operate both sets of brakes. There are two hydraulic fluid tanks that provide the volume to the two pumps, a primary tank and a secondary tank. The primary tank has a safety function installed that will switch to the secondary system, both the secondary pump and the secondary tank, should the primary tank sensors determine that the fluid level is low. The secondary tank also has a low fluid level sensor, however, when the fluid is detected to be low, the sensor activates the emergency stop (E-Stop) function.

The events on July 25 resulted from the combination of conditions outlined above. Brinderson employees and the Cognizant Engineer were in the process of replacing the No. 45 valve. Although work authorization 87-1763 had been written, maintenance had elected not to support the valve changeout, reportedly a management decision based on employee overtime. As a result, the Cognizant Engineer elected to "make do" with the available manpower. Jim Ellet, the Mining Operations Supervisor was contacted and completed the lockout provisions that were required to deenergize the hoist and the Construction group electrician, Tom Hackler was utilized to make electrical connections. The Hoistman on duty at the time was Jim Campbell. Thus the

technical requirements and paperwork for lockout and deenergizing the hoist were accomplished.
The replacement valve was received on site during the week of July 13. Al Varga visually examined the valve in the warehouse receiving area on the 22nd and subsequently showed the valve to Brinderson employees on the 23rd. The tools and equipment were gathered and on the morning of the 25th the replacement was begun. Rexnord Inc. had provided the Oil Gear valve to correct the Racine valve leakage problem. The Brinderson employees and the Cognizant Engineer were accomplishing the task on Saturday the 25th because it was the only convenient "window" in the work schedule to minimize impacts in other work and Project Participant schedules of activities.

The morning of the replacement, the underground employees were lowered on the Waste Handling Hoist and the hoist was left positioned at the underground station, 2150 feet below ground level. The hoist was deenergized, locked out and replacement was begun. There was no control power to the hoistman's console. Everything appeared to be in order. The Oil Gear replacement valve was "supposed to be" a direct changeout with no modifications required. At least, this was the belief of the employees doing the work. However, a shim was required to be removed and different length of bolts required to remake the connections. The valve was examined and put into place with the ports on the bottom of the valve lining up in the configuration most common to the valve being replaced. See Photographs 6 and 8. The only manufacturers instructions available were those in the O & M Manual. See Appendix 1. The personnel present noted that the Oil Gear valve did have a plug in one of the pilot ports. See Photograph 8. No additional instructions, directions, or Engineering Design Data were provided. Revisions to the O & M Manual were not indicated to be necessary by the manufacturer.

Installation and electrical connections were made and personnel were directed to remove the lockout and energize the system. The system was energized, the hoistman was instructed to start the standby hydraulic pump motor from the hoist motor control panel (not to be confused with the control power). The effect was that the hydraulic fluid was "jettisoned" to the opposite (primary) tank. The system was deenergized and again locked out. Al Varga left the hoist house for some reference material while the electrician changed the wires to the solenoid valve. The system was reenergized and again the pump was turned on with the Cognizant Engineer absent. See Figure 5 for the control valve configuration for incident one. At this

time the first of two incidents occurred; The thirty (30) foot uncontrolled movement or freewheel of the hoist. At this time, only two changes from normal operations had been made; Valve 45 had been changed and the electrical connections to solenoid SV-7 had been changed.

The Cognizant Engineer was made aware of the occurrence. With the Cognizant Engineer present, the sequence of events was evaluated and the Oil Gear Valve was removed and examined. The O & M Manual was rechecked and the piping was examined. The base plate was checked and it was discovered that the alignment dowels would fit if the valve was turned 180 degrees. The flow chart of the manual was compared and it appeared that indeed the valve had been installed backwards. The decision was made at this time to reinstall the valve in what appeared to be the correct configuration. This was accomplished, however, as a safety precaution the manual dump valve was opened before the system was energized. Also valve 56.4 was opened. See Figure 6 for valve configuration for incident two. The system was reenergized and the hoistman was instructed to start the hydraulic pump. When the pump was started, event number two occurred, the hoist freewheeled for approximately 300 feet. During the event, employees made the attempt to stop the freewheel by opening or closing various valves to no apparent effect. Fearing the worst, personnel departed the immediate area. The brakes again set relatively slowly since a loud squealing noise was heard prior to the final stop. The hoistman observing the winding of the hoist had also hit the E-Stop button, to no apparent effect.

The onsite QA engineer was notified and on his recommendation the Cognizant Engineer then made notification calls to Management, Safety and the hoist manufacturer. Management officials reported to the site to determine the cause and to effect repairs. On recommendation of the hoist manufacturer, the hoist was placed back in service with the original valve reinstalled. Every effort made to reestablish conditions existing prior to the attempted repair. Actions were evaluated and changes made were considered for the effects to the hoisting system. Hoist systems were checked and tested as possible. Hoist operational safety checks were made and test runs up and down the shaft were made prior to release of the hoist to service. During this time, the underground personnel were stopped from working and were removed from the mine via the exhaust shaft hoist.

Data has been collected on the hoist hydraulic, electrical and emergency operations functions of the

hoist. Hydraulic Return valve 45 has been identified as a single point failure common to both sets of brakes. Valve 45 is common in the pressure relief function. See Figure 4. Blockage of this valve has the potential to provide full hydraulic pressure of 1900 pounds per square inch (psi) in the pressure relief piping. There are two valves controlled by the hoistman that normally operate the hoist and also activate the pressure relief safety function designed to set the brakes. The brakes are spring activated and pressure released. These two valves are 1) The brake release lever controlled valve 25.3 and 2) The torque proving controlled valve 25.4 which requires approximately 500 amps on the hoist motor to release.

The torque proving valve vents to the pressure relief system when it is in the "off" position. In normal operation the torque proving valve 25.4 and the brake release valve 25.3 BOTH have to be in the "on" position to allow hydraulic fluid/pressure to the brakes for release.

During both incidents, the control power to the hoistman's console was "off" with valves 25.3 and 25.4 in the "off" position. This description is based on one side of the brake system only and is shown in Figures 5 and 6. The other side of the brake system is a mirror image as determined by Figure 4. All comments affecting one side apply to the other side with minor differences. One side has the Primary Pump vs. the Secondary Pump on the other. Therefore when pressure is experienced on one set of brakes, it is assumed unless manual valves isolate the system that pressure is also experienced on the other set of brakes.

Both of the freewheel events assume a blocked hydraulic return valve 45 since the valve is the only change that has been made.

B. EVALUATION

At a point in time during the construction and testing of the Waste Hoist a change was made to the operation of Racine Valve 45, changing the function of the porting of the valve. This orientation of the porting arrangement versus power input was not properly recorded in the as built diagrams and Operations and Maintenance Manual provided to WIPP Operations.

The Operations and Maintenance manual hydraulic system description on page 08-01-01 of section 4 states that "each pump is mounted with its motor on a common reservoir and is complete with pipe connections arranged for flooded suction". In fact, the pumps are

mounted on separate reservoirs. If the pumps were mounted on a common reservoir, the leakage through the return line(s) would be returned to the common tank, there would not be a low fluid level sensed and there would not be a problem. Although the literature does not specifically state that some leakage is expected and desired for internal lubrication, similarly designed valves are known to function in this manner. The use of Valve 45 in the current design is apparently a misapplication of the valve. The Operations and Maintenance manual is not correct for the as built conditions concerning the hydraulic fluid reservoirs.

The spare Racine Valve provided by the Manufacturer Rexnord Inc. had been installed during pre-turnover testing to correct the identified problem of the fluid leakage. The spare valve functioned the same as the original valve. The spare valve also leaked fluid to the tank opposite that which was being used. The spare valve was left in service with the first valve returned to the warehouse spare parts inventory. A third Racine valve from warehouse invetory was also tested and functioned the same as valves that have been in service.

Rexnord Inc. had been notified through the Construction Manager, the U. S. Army Corps of Engineers, and the Contractor, Brinderson Corporation, that the valve was not providing the desired function. Rexnord had agreed to repair/replace the valve under Warranty. Rexnord provided the Oil Gear valve to the Brinderson contractor to correct the leakage problem. The Oil Gear valve provided, with the exception of a plugged pilot port, was configured to provide functions as represented in the O & M Manual. Since the O & M Manual is incorrect in reference to current operation, the Oil Gear valve could not possibly operate in the Waste Hoist hydraulic system. With the plugged pilot port, testing has determined that the Oil Gear valve spool will center, blocking porting functions.

Contractor Quality Assurance controls applied to the receipt and installation of the Oil Gear valve no. 45 are less than adequate. Although the identification of the complex problem by Q.A. was not probable, the Q.A. of items received under warranty are not being addressed. Items received through the purchasing system receive Q. A checks and appear to be entirely adequate. However, the receipts of warranty goods are perhaps inadequately presumed to be correctly provided by the manufacturer.

The lockout and tagout procedures were accomplished by persons not intimately familiar with the systems involved. Although the paperwork and procedures were technically followed, the lockout and tagout was accomplished without a complete understanding of potential consequences. Personnel accomplishing the electrical connections did not demonstrate an understanding of the system when the wiring on the solenoid valve was changed.

The contractor personnel responsible to accomplish the work did not demonstrate an understanding of the hydraulic system. The plugged pilot port, as was demonstrated by test, had to be opened for the system to function. Energizing and deenergizing the system to change the wires with a plugged pilot port effectively centered the valve spool on the Oil Gear valve, blocking the ports and setting the system in a failure mode for the first freewheel event.

The Cognizant Engineer was representing Westinghouse during the warranty repair work. Warranty repairs have not historically required a Person in Charge (P.I.C.) per procedure. However, in effect the Cognizant Engineer was the overview authority. Brinderson employes did not utilize good judgement by directing the Hoistman to energize the system without the Cognizant Engineer's presence. The Hoistman also accepted direction from the contractor in energizing the hydraulic pumps to the hoist system.

The O & M Manual provided information required to effect the change in valves, however the manufacturer had not updated the information to the correct format. The valves were properly installed according to the information provided. However when the valve did not function properly, further actions taken were less than adequate. The Oil Gear valve vented hydraulic fluid to the opposite tank, which was not per the manual. Changing the electrical connections on the solenoid valve should not change the function of the valve and only served to center the valve and block the ports. Reenergizing the system with the valve ports blocked and control power "off" provided a flow path to pressurize the return hydraulic lines and release the hoist brakes. The brakes were released and the first freewheel of thirty feet occurred. See Figure 5 for the valve configuration and flow path for event one. The physical fact that the counterweights weigh more than the cage and attachments assured that the direction of movement of the cage would be upward.

The occurrence of the first freewheel certainly should have made all persons involved with the hoist system repair aware of the significance of the event. Notification of management and the manufacturer should have occurred at this time, if not before. The participants did not exercise good judgement in electing to continue.

The Cognizant Engineer and Brinderson employees studied the O & M Manual and determined that the valve could and should be reversed. Since the O & M Manual was incorrect, further efforts were doomed to failure. The safety of the system was considered and dump valves were opened in belief that the return hydraulic lines would be vented and the hoist brakes would not be released. The porting arrangement for the venting of the relief lines also route through valve 45 providing a single point of failure mode. Instead of providing the desired dump of hydraulic fluid/pressure, the opening of the dump valves provided a more direct flow of fluid to the brake release mechanism. See Figure 6 for event two. When the system was energized and the pump started, the hydraulic pressure released the brakes and the second event, the three hundred foot freewheel, occurred.

Personnel in the hoist tower attempted to stop the freewheel by opening and or closing various valves to no apparent effect. The sequence and identification of valve positions changed cannot be established. The personnel believed at this time that a disaster was in the making. The hoistman observed the hoist freewheeling and hit the Emergency Stop button to no apparent effect. The Emergency Stop button does not presently serve any safety function if there is no control power.

The sequence of conditions or events that eventually caused the hoist brakes to reset has not definitely been determined. A failure mode and effects analysis is currently underway by Westinghouse.

Subsequent to the second freewheel event, QA was notified, the hoist was secured and Management, Safety and the Manufacturer were notified. Notifications were made to the following: Jack Gilbert, Engineering Coordinator, Construction and Site Activities Branch, DOE, Vince Likar, Manager Engineering, Westinghouse, Henry Brandt, Underground Operations Manager, Westinghouse, Jere R. Galle, Safety Engineer, Westinghouse, Bud Lucus, Mining Operations Manager, Westinghouse, Bill Rude, Field Service Superintendent,

Rexnord Inc. Brandt and Lucus reported to the site and provided overview for the mitigation of the event. Bill Rude approved the reinstallation of the Racinevalve that had been removed. Precautions were taken to assure that the valve and hoist system were returned to the conditions existing prior to attempted repairs. Hoist systems were checked and tested as possible. Preoperational Safety checks were made on the hoist system per procedures. Several trips up and down the shaft were completed without difficulties and the hoist was returned to service. Meanwhile the underground employees had been stopped from working and removed from the underground via the Exhaust Shaft Hoist.

The root cause of the freewheel events is that undocumented changes to the hoist system have been made.

V. RECOMMENDATIONS

A. DESIGN:

The Accident Investigation Board believes there are several significant deficiencies to the design of the WIPP Waste Hoist Brake System. There are many ways to change the system to achieve a "failsafe" hoist, but high priority should be given to achieving the following:

Provide a check valve in each of the return hydraulic lines to prevent back pressure to the brake release mechanism.

Provide a pressure release valve in the return line(s) with limits set well below the pressure that will release the brakes.

Interlock the Emergency stop button with the hydraulic pump motors to eliminate a continuing pressure source in the hydraulic system and simplify pressure release and subsequent brake engagement.

Vent the return line of any Emergency Stop Button controlled valves directly to the hydraulic tank(s). Currently the vent or return line passes through the single point of failure valve no. 45.

The Operations and Maintenance Manual Provided by Rexnord Inc. is incorrect in at least two instances. The manual does not correctly describe the function of valve No. 45, and it still makes references to the "common" hydraulic fluid tank. Every effort should be made to verify the as built diagrams and instructions for operating the Waste Hoist.

Establish the desired function of Valve No. 45. If the valve is desired by the manufacturer to have internal lubrication that will have leakage, an overflow connection between the two tanks could provide a solution to the low tank sensor problem. It is possible that valve No. 45 can be eliminated.

B. ADMINISTRATIVE

Contractors performing warranty work at WIPP should be required to follow WIPP procedures. The Person In Charge (P.I.C.) program is intended to fulfill this requirement. A P.I.C. should be assigned to all warranty work on critical WIPP systems. The P.I.C. should be familiar with the WIPP system being repaired.

The Quality Assurance program should assure that the function is covering warranty repairs on critical WIPP systems.

The Operations program should assure that Lockout/Tagout Procedures are accomplished by persons that are assigned and have responsibilities to be intimately familiar with critical WIPP systems.

A Maintenance procedure should be established to assure that during work on the hoist hydraulic systems the brakes are isolated by closing all incoming and return line manually controlled valves. A direct drain line between the isolation valves would assure that leakage through the valves could not release the brakes.

A procedure should be in place to locate or "chair" the cage at the mine level and provide adequate weight on the cage to assure counterweights cannot move the cage in an upward direction. A scenario can be developed to change all of the disc brake pads without danger of the hoist moving.

INVESTIGATION TEAM SIGNATURES

Bob Johns, Industrial Safety Manager, Westinghouse

R.C. Johns

Richard Boyer, Manager, Radiation Safety, Westinghouse

Richard Boyer

Tom Kocialski, Manager, Instrumentation and Control, Westinghouse

Tom Kocialski

Karl Schendel, Senior Engineer, Safety Evaluation Program, Westinghouse

Karl R. Schendel

Larry Patrick, Manager, Training, Westinghouse

Larry Patrick

Norm Seipel, Quality Assurance Engineer, Westinghouse

Norm Seipel

Jere R. Galle, Safety Engineer, Westinghouse

Jere R. Galle

7.7 Appendix G: Tables from Chan et al (1987)
(a) Table 2-1 - Component Failure Rates
(b) Summary of Major Contributors to the Probability of a Catastrophic Accident-
(c) Summary of Major Contributors to Brake System Failure - Base Case (Table 4.1-2, Chan et al, 1987)

(a)

TABLE 2-1. Component Failure Rates

Component #(1)	Failure Mode	Failure Rate	Variance	Unit (HR-Hour) (D-Demand)
25.1, 25.2, 25.3, 25.4	Solenoid operated valve fails to de-energize	2.89E-06	.00E ± 0	HR
None	Proposed dump valve for system fails	2.89E-06	.00E ± 0	HR
26.1, 26.2, 56.3, 56.6	Ball valve fails closed	3.60E-09	.00E ± 0	HR
27.1, 27.2	Relief valve fails to open	3.00E-04	.00E ± 0	D
28.1, 28.2, 29.1, 29.2, 48	Flow control valve fails closed	1.36E-06	.00E ± 0	HR
43	Electro-hydraulic relief valve fails	6.49E-06	.00E ± 0	HR
15.1, 15.2	Filter plugged	2.98E-06	.00E ± 0	HR
15.1, 15.2	Filter check valve fails to open	2.08E-06	.00E ± 0	D
13.1, 13.2	Heat exchanger tube side plugs	8.50E-09	.00E ± 0	HR
13.1, 13.2	Heat exchanger fan fails	3.12E-06	.00E ± 0	HR
None	Displacement overtravel sensor fails	2.83E-06	.00E ± 0	HR
None	Disc brake unit fails	2.53E-06	.00E ± 0	HR
25.1, 25.2, 25.3, 25.4	All 4 solenoid operated valves fail to operate due to common cause	1.45E-08	.00E ± 0	HR
26.1, 26.2, 56.6, 56.3	Two manual valves closed due to common cause	1.80E-10	.00E ± 0	HR
None	Protective relay fails to open	1.36E-06	.00E ± 0	D
None	4 displacement overtravel sensors fail	6.41E-23	.00E ± 0	HR
None	3 displacement overtravel sensors fail	2.27E-17	.00E ± 0	HR
None	Control timer failure	1.64E-06	.00E ± 0	HR
25.1, 25.2, 25.3, 25.4, 45	Solenoid operated valve plugs	2.89E-06	.00E ± 0	HR
45, 51	Directional 4 way valves in maintenance	1.0 +00	.00E ± 0	D
45, 51	Human error in maintaining directional 4 way valves	6.56E-03	.00E ± 0	D
51	Directional 4 way valve fails blocking flow	1.45E-06	.00E ± 0	HR
25.2, 25.4	2 hydraulic valves fail blocking flow due to common cause	1.45E-07	.00E ± 0	HR
None	Relay coil shorts to power	1.00E-08	.00E ± 0	HR
37.1, 37.2	Check valve fails closed	6.00E-05	.00E ± 0	HR
(2)	Fraction of time hoisting CH-TRU waste	5.70E-01	.00E ± 0	D
(2)	Fraction of time hoisting human	3.30E-01	.00E ± 0	D
(2)	Fraction of time hoisting RH waste	1.00E-01	.00E ± 0	D
(2)	Annual frequency of loss of electric power	3.40E-02	.00E ± 0	D
(2)	Annual frequency of hoist malfunction	1.00E-03	.00E ± 0	D

TABLE 2-1. Component Failure Rates (Continued)

Component #(1)	Failure Mode	Failure Rate	Variance	Unit (HR-Hour) (D-Demand)
(2)	Annual frequency of controller or electric malfunction	1.00E-03	.00E ± 0	D
(2)	Annual frequency of other causes for unplanned scenarios	6.90E-04	.00E ± 0	D
(2)	Annual frequency of all three pairs of cable breaking	2.40E-10	.00E ± 0	D
S1	Directional 4 way valve fails, blocking flow proposed	1.45E-06	.00E ± 0	HR
Proposed	Both emergency dump valves fail to de-energize due to common cause	1.45E-07	.00E ± 0	HR
Proposed	Both proposed emergency relief valves fails to open due to common cause	1.51E-05	.00E ± 0	HR

Specific References:

Reactor Safety Study, Appendix III, Failure Data, WASH1400, October 1975.

IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations.

"Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications" (NUREG/CR-1278), prepared for the Nuclear Regulatory Commission by Swain, A.D. and Guttman, H.E., August 1983.

"Nonelectric Reliability Notebook", Rome Air Development Center, Griffiss Air Force Base, NY, RADC-TR-75-22, January 1985.

NUREG/CR-2728, "Interim Reliability Evaluation Program (IREP) Procedures Guide"

"Common Cause Fault Rates for Valves", (NUREG/CR-2770) Nuclear Regulatory Commission, February 1983.

"Probability of a Catastrophic Hoist Accident at the Waste Isolation Pilot Plant," TME-063, July 1985.

(1) P&ID Hydraulic Brake System, Sheet 1 of 2, 95080 294F

(2) Probability of a Catastrophic Hoist Accident at the Waste Isolation Pilot Plant, TME-063, July 1985.

WIPP Waste Hoist Hydraulic Brake System FTA

(From Chan, 1987)

TABLE 4.1-1

SUMMARY OF MAJOR CONTRIBUTORS TO THE PROBABILITY OF A CATASTROPHIC ACCIDENT BASE CASE

No.	Cutset Rate	Cutset Description	Component Rate
1.	1.75E-04	DIRECTIONAL VLV 45 FAILS DUE TO LOCAL FAULTS, BLOCKING FLOW	9.02E-03
		CH-TRU WASTE HOISTING	5.70E-01
		LOSS OF ELECTRIC POWER	3.40E-02
2.	1.27E-04	VALVE 45 OR 51 IN MAINTENANCE DURING TOTAL HOIST SHUTDOWN	5.00E+00
		OPERATOR ERROR IN MAINTAINING DIRECTIONAL VLV 51	6.56E-03
		CH-TRU WASTE HOISTING	5.70E-01
		LOSS OF ELECTRIC POWER	3.40E-02
3.	1.27E-04	VALVE 45 OR 51 IN MAINTENANCE DURING TOTAL HOIST SHUTDOWN	5.00E+00
		OPERATOR ERROR IN MAINTAINING DIRECTIONAL VLV 45	6.56E-03
		CH-TRU WASTE HOISTING	5.70E-01
		LOSS OF ELECTRIC POWER	3.40E-02
4.	1.01E-04	DIRECTIONAL VLV 45 FAILS DUE TO LOCAL FAULTS, BLOCKING FLOW	9.02E-03
		PERSONNEL ON HOIST	3.30E-01
		LOSS OF ELECTRIC POWER	3.40E-02
5.	8.76E-05	DIRECTIONAL VLV 51 FAILS DUE TO LOCAL FAULTS, BLOCKING FLOW	4.52E-03
		CH-TRU WASTE HOISTING	5.70E-01
		LOSS OF ELECTRIC POWER	3.40E-02
6.	7.36E-05	VALVE 45 OR 51 IN MAINTENANCE DURING TOTAL HOIST SHUTDOWN	5.00E+00
		OPERATOR ERROR IN MAINTAINING DIRECTIONAL VLV 51	6.56E-03
		PERSONNEL ON HOIST	3.30E-01
		LOSS OF ELECTRIC POWER	3.40E-02
7.	7.36E-05	VALVE 45 OR 51 IN MAINTENANCE DURING TOTAL HOIST SHUTDOWN	5.00E+00
		OPERATOR ERROR IN MAINTAINING DIRECTIONAL VLV 45	6.56E-03
		PERSONNEL ON HOIST	3.30E-01
		LOSS OF ELECTRIC POWER	3.40E-02
8.	5.07E-05	DIRECTIONAL VLV 51 FAILS DUE TO LOCAL FAULTS, BLOCKING FLOW	4.52E-03
		PERSONNEL ON HOIST	3.30E-01
		LOSS OF ELECTRIC POWER	3.40E-02
9.	3.07E-05	DIRECTIONAL VLV 45 FAILS DUE TO LOCAL FAULTS, BLOCKING FLOW	9.02E-03
		LOSS OF ELECTRIC POWER	3.40E-02
		RH-TRU WASTE ON HOIST	1.00E-01
10.	2.23E-05	VALVE 45 OR 51 IN MAINTENANCE DURING TOTAL HOIST SHUTDOWN	5.00E+00
		OPERATOR ERROR IN MAINTAINING DIRECTIONAL VLV 51	6.56E-03
		LOSS OF ELECTRIC POWER	3.40E-02
		RH-TRU WASTE ON HOIST	1.00E-01

(c)

WIPP Waste Hoist Hydraulic Brake System FTA

(From Chan, 1987)

TABLE 4.1-2

SUMMARY OF MAJOR CONTRIBUTORS TO BRAKE SYSTEM FAILURE BASE CASE

No.	Cutset Rate	Cutset Description	Component Rate
CUT SETS FOR GATE G0003 WITH CUTOFF PROBABILITY OF 5.00E-07			
1.	9.02E-03	DIRECTIONAL VLV 45 FAILS DUE TO LOCAL FAULTS, BLOCKING FLOW	9.02E-03
2.	6.56E-03	VALVE 45 OR 51 IN MAINTENANCE DURING TOTAL HOIST SHUTDOWN	5.00E+00
		OPERATOR ERROR IN MAINTAINING DIRECTIONAL VLV 51	6.56E-03
3.	6.56E-03	VALVE 45 OR 51 IN MAINTENANCE DURING TOTAL HOIST SHUTDOWN	5.00E+00
		OPERATOR ERROR IN MAINTAINING DIRECTIONAL VLV 45	6.56E-03
4.	4.52E-03	DIRECTIONAL VLV 51 FAILS DUE TO LOCAL FAULTS, BLOCKING FLOW	4.52E-03
5.	4.52E-04	HYDRAULIC VALVES 25.2 & 25.4 FAIL TOTAL BLOCKAGE BY COMMON CAUSE	4.52E-04
6.	8.14E-05	SOLENOID OPERATD HV 25.4 FAILS, RESULTING IN TOTAL BLOCKAGE	9.02E-03
		SOLENOID OPERATD HV 25.2 FAILS, RESULTING IN TOTAL BLOCKAGE	9.02E-03
7.	4.52E-05	SOLENOID OPERATD HV 25.1.2.3 & .4 FAIL TO DE-ENERG DUE TO C.C	4.52E-05
8.	7.34E-07	SOLENOID OPERATD HV 25.4 FAILS, RESULTING IN TOTAL BLOCKAGE	9.02E-03
		SOLENOID OPERATD HV 25.1 FAILS, RESULTING IN TOTAL BLOCKAGE	9.02E-03
		HV 25.2 FAILS TO DE-ENERGIZE DUE TO LOCAL FAULT	9.02E-03
9.	7.34E-07	SOLENOID OPERATD HV 25.4 FAILS, RESULTING IN TOTAL BLOCKAGE	9.02E-03
		SOLENOID OPERATD HV 25.1 FAILS TO DE-ENERGIZ DUE TO LOCAL FAULTS	9.02E-03
		HV 25.2 FAILS TO DE-ENERGIZE DUE TO LOCAL FAULT	9.02E-03
10.	7.34E-07	SOLENOID OPERATD HV 25.3 FAILS, RESULTING IN TOTAL BLOCKAGE	9.02E-03
		SOLENOID OPERATD HV 25.4 FAILS TO DE-ENERGIZE DUE TO LOCAL FAULT	9.02E-03
		SOLENOID OPERATD HV 25.2 FAILS, RESULTING IN TOTAL BLOCKAGE	9.02E-03

EEG-15 Bard, Stephen T., Estimated Radiation Doses Resulting if an Exploratory Borehole Penetrates a Pressurized Brine Reservoir Assumed to Exist Below the WIPP Repository Horizon, March 1982.

EEG-16 Radionuclide Release, Transport and Consequence Modeling for WIPP. A Report of a Workshop Held on September 16-17, 1981, February 1982.

EEG-17 Spiegler, Peter, Hydrologic Analyses of Two Brine Encounters in the Vicinity of the Waste Isolation Pilot Plant (WIPP) Site, December 1982.

EEG-18 Spiegler, Peter, Origin of the Brines Near WIPP from the Drill Holes ERDA-6 and WIPP-12 Based on Stable Isotope Concentration of Hydrogen and Oxygen, March 1983.

EEG-19 Channell, James K., Review Comments on Environmental Analysis Cost Reduction Proposals (WIPP/DOE-136) July 1982, November 1982.

EEG-20 Baca, Thomas E., An Evaluation of the Non-radiological Environmental Problems Relating to the WIPP, February 1983.

EEG-21 Faith, Stuart, et al., The Geochemistry of Two Pressurized Brines From the Castile Formation in the Vicinity of the Waste Isolation Pilot Plant (WIPP) Site, April 1983.

EEG-22 EEG Review Comments on the Geotechnical Reports Provided by DOE to EEG Under the Stipulated Agreement Through March 1, 1983, April 1983.

EEG-23 Neill, Robert H., et al., Evaluation of the Suitability of the WIPP Site, May 1983.

EEG-24 Neill, Robert H. and James K. Channell Potential Problems From Shipment of High-Curie Content Contact-Handled Transuranic (CH-TRU) Waste to WIPP, August 1983.

EEG-25 Chaturvedi, Lokesh, Occurrence of Gases in the Salado Formation, March 1984.

EEG-26 Spiegler, Peter, Environmental Evaluation Group's Environmental Monitoring Program for WIPP, October 1984.

EEG-27 Rehfeldt, Kenneth, Sensitivity Analysis of Solute Transport in Fractures and Determination of Anisotropy Within the Culebra Dolomite, September 1984.

EEG-28 Knowles, H. B., Radiation Shielding in the Hot Cell Facility at the Waste Isolation Pilot Plant: A Review, November 1984.

EEG-29 Little, Marshall S., Evaluation of the Safety Analysis Report for the Waste Isolation Pilot Plant Project, May 1985.

EEG-30 Dougherty, Frank, Tenera Corporation, Evaluation of the Waste Isolation Pilot Plant Classification of Systems, Structures and Components, July 1985.