WIPP/WID--96-2196

WASTE ISOLATION PILOT PLANT TRUDOCK CRANE SYSTEM ANALYSIS

October 1996

RECEIVED
APR 03 1997
OST 1

Prepared for:

Westinghouse Waste Isolation Division
P.O. Box 2078
Carlsbad, New Mexico 88221

Prepared By:

Westinghouse Pittsburgh, PA.
and
WID Carlsbad, N.M.

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

MASTER

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, make any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

**Portions of this document may be illegible
in electronic image products. Images are
produced from the best available original
document.**

This document has been reproduced directly from the best possible copy.
It is available to DOE and DOE contractors at the following addresses:

Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Prices available from (615) 576-8401

Available to the public from the
National Technical Information Services
U. S. Department of Commerce
5285 Port Royal Road
Springfield, VA 22161

RECEIVED
APR 03 1997
OSTI

Processing and final preparation of this report was performed by the Waste Isolation Pilot Plant Management and Operating Contractor for the U.S. Department of Energy under Contract No. DE-ACO4-86AL31950.

WASTE ISOLATION PILOT PLANT

TRUDOCK CRANE SYSTEM ANALYSIS

Prepared by:

Bert C. Morris
Westinghouse Pittsburgh, PA
WID Purchase Order 71538, March 1996

Mike Carter
WID Environmental and Radiological Control

Independent Reviewer:

Carl Ortiz
WID Environmental and Radiological Control

Approved by:

10/25/96
Chuan-Fu Wu, Manager
WID Environmental and Radiological Control

Processing and final preparation of this report was performed by the Waste Isolation Pilot Plant Management and Operating Contractor for the U.S. Department of Energy under Contract No. DE-AC04-86AL31950.

TABLE OF CONTENTS

<u>SECTION</u>	<u>TITLE</u>	<u>PAGE</u>
EXECUTIVE SUMMARY		1-1
1.0 INTRODUCTION		1-1
1.1 Background		1-1
1.2 Scope of the Analysis		1-1
1.3 Method of Analysis		1-2
1.4 Guidelines and Assumptions		1-2
1.5 Results		1-2
1.6 System Clarification and Component Identification		1-3
2.0 TRUDOCK CRANE SYSTEM ANALYSIS		2-1
2.1 System Description		2-1
2.1.1 TRUDOCK Crane System Overview		2-1
2.1.2 TRUDOCK Crane Brake System		2-2
2.1.3 Analysis Focus, Objectives and System Boundaries		2-2
2.2 System Interfaces		2-3
2.3 Test and Maintenance		2-3
2.4 Failure Scenarios		2-3
2.5 Success Criteria		2-5
2.6 System Modeling Assumptions		2-5

3.0 RESULTS	3-1
3.1 System Analysis	3-1
3.1.1 Fault Tree Construction	3-1
3.1.2 Failure Rate Data Base Development	3-1
3.2 Presentation of Results	3-3
3.2.1 Nomenclature	3-3
3.2.2 Quantitative Results	3-4
3.3 Conclusions	3-6
Appendix A1	
TRUDOCK Crane System Analysis	A1-1
Appendix A2	
Fault Tree Analysis Data	A2-1
Appendix A3	
Method of Analysis: Fault Tree Modeling, Guidelines and Assumptions	A3-1
Appendix A4	
PLG Human Reliability Analysis	A4-1
Appendix A5	
PLG Waste Isolation Pilot Plant Trupact Crane System Analysis	A5-1
Appendix A6	
WIPP Power Outages	A6-1
Table 3.1-1 Data and Sources Used in Failure Rate Analysis	3-2

EXECUTIVE SUMMARY

The WIPP TRUDOCK crane system located in the Waste Handling Building was identified in the WIPP Safety Analysis Report (SAR), November 1995, as a potential accident concern due to failures which could result in a dropped load. The objective of this analysis is to evaluate the frequency of failure of the TRUDOCK crane system resulting in a dropped load and subsequent loss of primary containment, i.e. drum failure.

The frequency of dropped loads was estimated to be $9.81\text{E-}03/\text{year}$ or approximately one every 102 years (or, for the 25 percent contingency, $7.36\text{E-}03/\text{year}$ or approximately one every 136 years). The dominant accident contributor was the failure of the cable/hook assemblies, based on failure data obtained from NUREG-0612, as analyzed by PLG, Inc. (Appendix 5 PLG letter WEC-3140-PLG-05). The WIPP crane system undergoes a rigorous test and maintenance program, crane operation is discontinued following any abnormality, and the crane operator and load spotter are required to be trained in safe crane operation, therefore it is felt that the WIPP crane performance will exceed the data presented in NUREG-0612 and the estimated failure frequency is felt to be conservative.

1.0 INTRODUCTION

1.1 Background

A quantitative Fault Tree Analysis (FTA) of the reliability of the WIPP TRUDOCK crane system has been undertaken as part of the safety analysis effort for the WIPP Safety Analysis Report (SAR). The crane system consists of two, 5 ton overhead bridge cranes located in the Waste Handling Building (WHB). The cranes are utilized to lift the TRUPACT payload, two-seven drum arrays, two Standard Waste Boxes (SWB), or one Ten-Drum Overpack (TDOP) from the TRUPACTS and place them on the facility pallets for transport to the underground. The TRUDOCK cranes had not been previously analyzed for failure and were identified in the SAR, November 1995, as potential accident concerns due to failures which could result in a dropped load. The objective of this analysis is to evaluate the annual frequency of failure of the TRUDOCK crane system resulting in a dropped load with subsequent loss of primary containment, i.e. drum failure.

1.2 Scope of the Analysis

The crane system analysis encompasses the two bridge cranes and their operation to lift and transport the TRUPACT contents to the facility pallets. The analysis focuses on those events which could result in a dropped load and does not consider failures which might disable crane operation and prevent the normal processing of waste but result in a safe condition for the waste.

For example, the cranes are designed to hold their load during a design basis earthquake. Therefore the analysis focuses on those mechanical and human failures which would compromise the payload. A detailed analysis of the control system is beyond the scope of this study.

1.3 Method of Analysis

The WIPP TRUDOCK crane system is evaluated using the Fault Tree Analysis methodology. Rather than focusing on the design performance of a system, Fault Tree Analysis emphasizes how the system can fail. Fault Tree Analysis provides a systematic and logical approach for determining the events or combinations of events that could lead to potential safety and reliability concerns in a system. In the case of this analysis, the primary concerns are: failure of the brakes to set during power or motor driver failures; mechanical failures and human errors which result in dropped loads. A description of Fault Tree Analysis and how it is applied to this evaluation is provided in Section 2 of this report.

1.4 Guidelines and Assumptions

The design is modeled in accordance with fault tree guidelines provided in Appendix A3 and the system specific assumptions provided in section 2.6.

1.5 Results

Results of the present analysis are presented and discussed in Section 3 of this report. The annual frequency of failure of the design, as well as components or events that dominate failure of the TRUDOCK crane system are discussed. The results of the analysis indicate that the dominant source of crane failures which could result in dropped payloads are crane hook/cable failures. The analysis indicates that such failures are likely to occur approximately once every one hundred and two years. This is based on crane/hook failure rates from NUREG-0612, July 1980, "Control of Heavy Loads at Nuclear Power Plants", see Appendix A5. The WIPP facility has a very aggressive test, maintenance and inspection program for the crane including: pre-operational checks and inspection of the hook, cables, lifting and balancing assembly; test operation of the crane (no load) once per shift; monthly inspection of the hook and cable, yearly magna-flux (non-destructive testing) of the hook and inspection of the cable. Additionally, the cranes are rated at 5 tons (with an over-design factor of 5) and the TRUPACT waste contents have an individual weight limit of 7,265 pounds (or slightly over 3.5 ton). Finally, the operators and load spotters are required to undergo extensive training in crane operation and radiation safety and are required to stop crane operation in the event of any abnormality. Therefore, it is highly likely that the performance of the WIPP crane system will exceed the cranes analyzed in NUREG-0612 so that this analysis is felt to represent an extremely conservative value. There are no recommendations or suggestions for design or procedural changes. Revised analysis based on additional, more

relevant crane operational performance data or on actual WIPP crane performance might be performed to achieve a more realistic failure frequency.

1.6 System Clarification and Component Identification

The TRUDOCK cranes are located in the WHB. There are two cranes which are referred to as the A and B crane in this analysis. Each crane is located at its own TRUDOCK docking bay. Each docking bay has two stations where TRUPACTS can be located for unloading. Each crane is equipped with its own TRUPACT adjustable center-of-gravity lift fixture, SWB lift fixture adaptor, and short and long lifting leg sets. There is one TDOP lift fixture adaptor to be shared by both cranes. This analysis assumes that both cranes are normally operating, therefore a dropped load is possible from either crane.

This Page Intentially Blank

2.0 TRUDOCK CRANE SYSTEM ANALYSIS

2.1 System Description

2.1.1 TRUDOCK Crane System Overview

After the forklift places the TRUPACT container at an unloading station in the WHB, a TRUDOCK crane is utilized to remove the outer and inner TRUPACT container lids and remove the CH waste. The CH waste may be packaged in seven drum arrays, SWBs, or a TDOP. Each TRUPACT can contain either two SWBs, two-seven drum arrays, or one TDOP. The two SWBs or two-seven drum arrays are lifted and handled as a single unit.

There are two TRUDOCK cranes within the WHB which are capable of operating alone or in parallel. These two cranes are five-ton, overhead bridge cranes with specially designed lifting and load balancing fixtures. In addition, there are two transfer bays, one for each crane, and each area has two unloading stations. Therefore, waste processing may continue if one of the cranes is being serviced or repaired.

Following radiological surveys (additional surveys are conducted throughout the process), a crane is used to remove the outer and inner TRUPACT lids and place them on their respective stands. The crane then is used to lift the the payload from the TRUPACT and place it on the facility pallet. This is accomplished by the use of either a set of specially designed lifting legs which attach, via locking pins, to an adjustable center-of-gravity lift fixture and then to the SWB lift fixture adaptor (this then attaches to the lifting lugs on the SWBs) or a longer set that attaches to the adjustable center-of-gravity lift fixture and then extends down through the two seven drum arrays. The adjustable center-of-gravity lift fixture also includes three actuator motors and hydraulic arms to rotate the lifting legs into their locking, lift positions for seven drum arrays. The control system has limit switches with lights to indicate that each lifting leg has rotated to attach to the lifting pins. The operator and spotter are also able to verify the leg rotation by observing the motion of the actuating arm. The operator and spotter can also verify that the lifting legs are at the proper elevation (i.e. completely inserted into the waste assembly) to attach to the lifting pins by observing: the disappearance of a red indicator line painted on each leg, the loss of load indicated on the crane load cells and the freeing of the hook as the load is removed from it. The cranes also have a load locking mechanism such that once the waste assemblies are locked onto the crane, they cannot be unlocked until the load is removed, (i.e. until the load is set down) and the operator must simultaneously turn two switches on the control panel to unlock the lifting legs.

The cranes have been designed for the design basis earthquake and are equipped with brakes which will lock the load in place on loss of power.

The crane control system allows the operator to lift and transfer the payload by manual control or by use of an automatic, programmed control system which first lifts the waste assemblies, then transfers them, horizontally with the ground, to the location of the pallet. The automatic control stops with the waste assemblies located above the pallet and does not lower them. The lowering of the assemblies and any final horizontal adjustments are done by the crane operator with the help of the spotter. The cranes have a maximum horizontal speed of 50 feet per minute and a maximum vertical speed of 20 feet per minute.

Once the payload is placed on the pallet, the lifting legs are rotated to disengage the lifting pins and the legs are raised out of the payload by the crane. Again, the operator and the spotter can visually observe the movement of the actuator arms and there are indicator lights to inform the operator that each leg has rotated to the unlock position. In addition, if the operator would inadvertently begin to remove the lifting legs with one or more legs still attached, the crane load cell would indicate the load was still attached and the spotter and operator would immediately observe the waste assembly move. The operator and spotter have been trained to immediately stop the operation for such an abnormal condition.

2.1.2 TRUDOCK Crane Brake System

The cranes are equipped with two braking systems: a load holding helix brake and a disc brake system on the drum. The helix brake uses the weight of the load to set the brake and requires motive force from the motor to release it, therefore the brake should set itself on loss of power or motor function. The disc brake system is a mechanical system which consists of a multiple disc assembly to prevent the cable spool from turning. The disc brakes are spring-loaded and engage automatically on loss of power.

2.1.3 Analysis Focus, Objectives and System Boundaries

The purpose of this study is to review the operation of the TRUDOCK transfer cranes and assess the likelihood of a failure which would result in damage to the CH waste container and subsequent loss of primary containment, i.e. release of hazardous waste material within the WHB. The information developed may then be used to evaluate the design, operating procedures and maintenance schedules to determine possible improvements.

The analysis performed is specifically focussed on the design and operation of the TRUDOCK transfer cranes. The focus of this analysis is to determine the reliability of the crane system and quantify the frequency of crane failures which would result in a release of hazardous waste materials.

2.2 System Interfaces

The TRUDOCK transfer cranes are self-contained with the exception that electrical power is required for crane movement and control system operation. The cranes are powered from Bus A or B from Area Substation #2.

2.3 Test and Maintenance

The WIPP facility test, maintenance and inspection program for the cranes includes: pre-operational checks and inspection of the hook, cables, lifting and balancing assembly; test operation of the crane (no load) once per shift; monthly maintenance inspection of the hook and cable, yearly magna-flux (non-destructive testing) of the hook and inspection of the cable. During the test operation, the cranes are run through their full range of movement to verify limit switch operation. All maintenance is assumed to occur during the non-operating time periods.

2.4 Failure Scenarios

The WIPP SAR, November 1995, identified the following four accident scenarios of concern for the transfer cranes:

- failure of the lifting equipment,
- failure to secure load,
- failure to remove payload,
- moving accident with inner containment vessel (ICV) lid.

Note that the last incident involves dropping or swinging an ICV lid such that it hits some of the drums in the open TRUPACT. Such an accident would likely involve less material than a crane drop incident, therefore the crane drop analysis should bound this incident. In addition, the loss of power to the cranes could result in a potential release accident, if the brakes fail to engage. These accidents scenarios are discussed below.

Loss of Electrical Power

If power is lost to the crane motor, the crane hook is free to move. The expected movement direction would be to accelerate to the ground due to the weight of the load. It would be expected that the disc brakes would de-energize and the brake would engage the spool to stop the crane. Additionally, the helix brake should actuate on loss of motive force.

Failure of the Lifting Equipment

This scenario would include those equipment failures which would cause the crane to drop its load. Typical failures would include: crane hook/cable failure, and lifting mechanism failure to engage. There are three lifting legs which are utilized during a lift however two are capable of bearing the load, if necessary. Therefore, if one failed during a transfer, the center of gravity would shift and a swinging motion could occur. Since the two-seven drum arrays are wrapped in plastic, it is not anticipated that the drums will separate. Therefore, it is assumed that should one leg attachment fail during a transfer, the load will not be dropped and the operator will be able to recover control and place the load safely down.

Failure to Secure Load

This scenario relates to the operator failure to properly connect or disconnect the load which could then result in a failure of the connections during transfer and resultant drop. The trained and certified operator and spotter will be responsible for connecting the load per existing procedures. As described previously, Section 2.1.1, there are lights to indicate proper rotation of the lifting legs, load cell indication on the crane and numerous other visual verifications that the lift assembly is properly attached to the load. In addition, crane transfer operations are typical of standard industrial practice with low stress levels and it is expected that there will be no more than 2 to 3 TRUPACTS transferred per shift per crane. Since there are two trained personnel involved in attaching the lift mechanism to the load, and there are numerous feedbacks and verifications, a human failure to properly attach the lifting fixture is felt to be incredible.

A more probable human error exists for attaching the lifting legs to the lifting fixture using the locking pins. The lifting legs must be switched for each transfer involving a two-seven drum waste array (i.e. the short legs are used to remove the outer and inner TRUPACT lids and the long legs are used to lift the two-seven drum waste array). The operator or the spotter must manually remove and insert the locking pins for each leg. The legs are designed such that they cannot be incorrectly aligned, i.e. rotation of the leg by 180 degrees will not mis-align the lifting hook, however it is possible that the operator or spotter might not insert the pin fully. The pins are attached to the lifting assembly by wire cables to prevent loss and reduce the likelihood of forgetting the pin. Complete failure to insert the pin would be immediately detected when the operator raises the legs to insert them in the waste assembly; the leg(s) without the locking pin(s) would not raise. Pin insertion is verified by a spring-loaded locking ball, and can be visually verified by the operator or spotter prior to lifting the legs for insertion into the waste assembly and again when the legs are lowered to attach to the waste assembly. During this period, the location and condition of the lifting legs are continuously observed, (i.e. this is the primary function of the spotter). As mentioned above, it will be assumed that the load can be lowered without damage if only one of the three connections is not correctly made.

Appendix A4 presents a human reliability analysis performed by PLG, Inc. of Newport Beach, CA, to estimate the likelihood of a drum drop accident due to human errors. The likelihood was estimated to be $8.7\text{E-}07$ per TRUPACT II container unloaded.

Failure to Remove Payload

This scenario involves the failure of the operator/spotter to disconnect all of the lifting connections following a transfer. This was also discussed in Section 2.1.1. Once the waste assemblies are placed on the pallet, the lifting legs are rotated to disengage the lifting pins and the legs are raised out of the waste assembly by the crane. Again, the operator and the spotter can visually observe the movement of the actuator arms and there are indicator lights to inform the operator that each leg has rotated to the unlock position. In addition, if the operator would inadvertently begin to remove the lifting legs with one or more legs still attached, the crane load cell would indicate the load was still attached and the spotter and operator would immediately observe the waste assembly move. The operator and spotter have been trained to stop the operation for such an abnormal condition. Therefore, the waste assembly would not reach an elevation where a drop would compromise its integrity. Again, since there are two trained personnel involved in detaching the lift mechanism from the load, and there are numerous feedbacks and verifications, a human failure to properly detach the lifting fixture is felt to be incredible.

Moving Accident with ICV Lid

During the initial opening of the TRUPACT, the ICV lid must be removed and placed on its holding stand. If the lid were not properly connected to the lifting legs, the lid might drop on one side and swing. The weight and momentum of that swing could damage the drums if they were within the swing radius. This incident will be bounded by the crane drop incident and is not analyzed further.

2.5 Success Criteria

The crane operation is successful if the dropping of the load and damage to the waste assemblies with subsequent hazardous waste material release is prevented.

2.6 System Modeling Assumptions

1. The waste assemblies are capable of withstanding the impact of the assemblies on the pallet (or floor) if they are lowered at the maximum crane speed (20 feet/minute).

2. Two of three connections can prevent the load from dropping and allow safe lowering of the waste assembly to the ground.
3. Throughput for CH waste is 784 drums per week (7 pallets per day, 4 days per week, 28 drums per pallet), or 2912 TRUPACTS per year. Allowing a 25 percent contingency for maintenance delays and time to transition from room to room, 2184 TRUPACTS will be processed per year.
4. There are two cranes in service, therefore each crane will transfer 1456 (or, considering the 25 percent contingency, 1092) TRUPACTS per year.
5. Dropping a TRUPACT ICV lid or lift assembly on the drum array should be bounded by the crane drop accident.
6. Structural failures of the TRUPACT lifting assembly were not considered. The lifting assemblies and legs are visually inspected prior to each transfer and inspected yearly.
7. Dropping the drums due to a failure of the center-of-gravity assembly or other unbalanced load scenarios was not considered since the two-seven drum arrays are wrapped in plastic and the load is balanced as soon as it is out of the TRUPACT. Therefore it is not anticipated that individual drums will separate.
8. Dropping the TRUPACT outer containment vessel (OCV) lid will not result in damage to the waste assemblies since the OCV will be secured on its stand prior to removing the ICV lid.

3.0 RESULTS

3.1 System Analysis

3.1.1 Fault Tree Construction

A fault tree for the TRUDOCK crane system was constructed to determine the failure frequency of the system as described in Section 2. The fault tree for the design is presented in Appendix A1.

3.1.2 Failure Rate Data Base Development

Failure rate data for the TRUDOCK crane system was obtained from a similar analysis performed on cranes used to transfer TRUPACT contents at Rocky Flats, (FSAR, Building 664, October 1992) and NUREG-0612. Table 3.1-1 summarizes the data used for this analysis, along with their sources. Failure rate data calculations for common cause failures are presented in Appendix A3.

In the application of the fault tree analysis of failure probability of nuclear power plants, the mission time is based on the premise that the nuclear power reactor is required to remain at power continuously, or the plant to remain continuously operational, for some time interval. For the operation of the TRUDOCK crane system, there is no such a constraint. At the start of each eight hour shift, the system is subjected to a series of thorough "pre-operational check" tests. The tests verify that the TRUDOCK crane system is operational. Operation of the crane system does not begin until the tests are successfully completed. Further, during the crane system operation, the system can be shutdown at any point in time for any reason, for example, any indication that the system is not performing its function as required. The system is not returned to service, until the malfunction is corrected and the same "pre-operational check" tests have been successfully completed.

Therefore, use of the mission time in the fault tree analysis of the crane system annual failure probability, on the premise that the system is required to remain continuously operational over a certain time interval, is extremely conservative. To enable the application of the fault tree analysis technique, however, the mission time is estimated on the basis of such a conservative assumption.

Table 3.1-1 Data and Sources Used in Failure Rate Analysis

Basic Event	Event Frequency	Data References	Component ID	Description
1	8.00E-5/d	6	AC	Brake Coil Contacts Fail
2	8.00E-5/d	1	BC	Brake Spring Failure
3	8.00E-5/d	1	HX	Helix Brake Failure
4	4.63E-2/yr	2	MO	Crane Motor Fails
5	4.34E-01/yr	3	E2	Loss of Electric Power to TRUDOCK Crane
6	2.47E-5/d	2	AC*	Actuator (Electric Motor) Fails
7	3.00E-4/d	4	DI*	Limit Switch Indicator Fails
8	2.50E-6/d	1	CE	Crane Cable/Hook Fails
9	8.7E-7/d	5	CP	Operator Makes Improper Pin Connection

d = demand

References -

- 1 US Nuclear Regulatory Commission "Control of Heavy Loads at Nuclear Power Plants," NUREG-0612, July 1980
- 2 IEEE-500, 1984
- 3 Failure Rates to Support WIPP TRUDOCK Crane and Waste Hoist Safety Analysis. W-SMPD Reliability Engineering, June 1996, Appendix A6
- 4 US Nuclear Regulatory Commission "Reactor Safety Study, WASH-1400," NUREG-75/014, Appendix III, Failure Rate Data
- 5 PLG, Inc., Appendix A4
- 6 PLG, Inc., Waste Isolation Pilot Plant Trupact Crane System Analysis, WEC-3140-PLG-05, Appendix A5

* - These values used for multiple components of the same type.

With the understanding of the conservatism described above, the TRUDOCK CRANE mission time for the crane suspending waste is calculated based upon WIPP/WIDD-96-2178, p. 3-3, (on a per crane basis) as follows:

$$0.2 \text{ hours per lift} \times 1456 \text{ lifts per crane} / 8760 \text{ hours per year} = 3.32\text{E-}2 \text{ hours/yr}$$

3.2 Presentation of Results

3.2.1 Nomenclature

The following paragraphs describe the nomenclature and organization of data for Fault Tree Analysis. Three data sets are particularly important to note. These are the data (.SIM), cutset (.DES) and importance ranking (.IMP) files. Their significance is described below.

Mapping the Fault Tree to the Master Data File

The design has three tables derived from the quantification of the fault trees. The first table (.SIM file) links the basic and system events from the fault tree to the master data file and lists the mission times for time-dependent events.

Fault Tree Cutsets

The second table (.DES file) shows the cutsets, both single and multiple order, listed from most to least likely to occur. A single order cutset consists of one event, while a multiple order cutset consists of two events or more. The number to the left of the cutset description is the frequency that the event may occur. If the cutset is single order, the frequency of failure is repeated at the right. If the cutset is multiple order, the failure probability of each component of the cutset is presented at the right, with the product of the individual failures offered at the left. For example, if the cutset would be composed of three individual failures, X, Y, and Z, with failure rates of 0.1, 0.02, and 0.003, respectively, the cutset would read as follows:

6.00E-06	X	1.00E-01
	Y	2.00E-02
	Z	3.00E-03

Thus, the cutset would require a failure of all three components, X, Y, and Z, with a combined probability of 6.00E-06/yr.

Dominant Cutsets

The dominant contributors to the TRUDOCK crane system failure frequency are derived through quantification of the fault tree. These dominant contributors, or cutsets, determine what single failures or combination of failures may lead to crane system failure. Identification and discussion of the dominant contributors to the annual frequency of crane failure is offered in the following section.

Importance Calculation

It is possible that single components, although not solely in the dominant cutsets, may contribute significantly to the annual probability of system failure by being a part of several cutsets. To determine if an individual component which is not identified as a single order cutset has significant impact on the failure probability, all individual component contributions are evaluated and assigned an importance weighting.

The individual component contribution to the accident sequences are listed in the third table (.IMP file). Only the component identifier as found on the fault tree is used to identify each event. Each identifier represents an individual component of failure, and is normally an abbreviation of the actual failure.

The second column "Importance Ranking," represents a general ranking based on the overall contribution of the event to system failure. The column labeled "# CS" represents the number of cutsets in which the basic event appears. The "CONT. TO Q" column represents the contribution to overall failure based on the number of cutsets in which the event appears and the value of each cutset. The final heading, "FAILURE PROBABILITY" represents the failure rate assigned to the individual component failure or event.

If an individual component failure or event is not listed in the component importance tables, it did not contribute significantly to the system failure probability because of the cutoff probability assigned during fault tree quantification.

3.2.2 Quantitative Results

The annual frequency of crane system failure resulting in a dropped load is $9.81\text{E-}03/\text{year}$ (or, for the 25 percent contingency, $7.36\text{E-}03/\text{year}$). The system failure is dominated by the following combinations of events, or cutsets, and corresponding failure probabilities. Complete results from this analysis is provided in Appendix A2.

<u>Cutset - Crane System Design</u>		<u>Annual Frequency of Failure</u>	<u>Percentage Contribution To Total</u>
1	Number of Crane B Transfers per Year (25 percent contingency) Crane B Cable/Hook Breaks	3.65E-03 2.74E-03	37.2%
2	Number of Crane A Transfers per Year (25 percent contingency) Crane A Cable/Hook Breaks	3.65E-03 2.74E-03	37.2%
3	Number of Crane B Transfers per Year (25 percent contingency) Improper Connections Due to Operator Error	1.27E-03 9.57E-04	12.8%
4	Number of Crane A Transfers per Year (25 percent contingency) Improper Connections Due to Operator Error	1.27E-03 9.57E-04	12.8%
5	Crane B Helix Brake Fails Crane Motor Failure Disk Brake Actuator Failure	2.96 E-10	0.0%
6	Crane B Disk Brake Fails due to Broken Spring Crane B Helix Brake Fails Crane Motor Failure	2.96 E-10	0.0%
7	Crane A Helix Brake Fails Crane Motor Failure Disk Brake Actuator Failure	2.96E-10	0.0%
8	Crane A Disk Brake Fails due to Broken Spring Crane A Helix Brake Fails Crane Motor Failure	2.96E-10	0.0%
9	Loss of Power to Bridge Cranes Crane B Disk Brake Fails due to Broken Spring Crane B Helix Brake Fails	9.22E-11	0.0%
10	Loss of Power to Bridge Cranes Crane A Disk Brake Fails due to Broken Spring Crane A Helix Brake Fails	9.22E-11	0.0%
11	Loss of power to Bridge Cranes Crane A Helix Brake Failure Crane Motor Failure	9.22E-11	0.0%
12	Loss of power to Bridge Cranes Crane B Helix Brake Failure Crane Motor Failure	9.22E-11	0.0%
13	Loss of Power to Bridge Cranes Common Cause Failure of Disk Brakes on Both Cranes (Spring) Common Cause Failure of Helix Brakes on Both Cranes (Spring)	9.22E-13	0.0%

3.3 Conclusions

The frequency of dropped loads was estimated to be $9.81\text{E-}3/\text{year}$ or approximately one every 102 years (or, for the 25 percent contingency, $7.36\text{E-}3/\text{year}$ or approximately one every 136 years). The dominant accident contributor was the failure of the cable/hook assembly, based on data from NUREG-0612. The WIPP crane system undergoes a rigorous test and maintenance program, crane operation is discontinued following any abnormality, and the crane operator and spotter are required to be trained in safe crane operation and radiological safety, therefore it is felt that the WIPP crane performance will exceed the data presented in NUREG-0612.

Appendix A1
TRUDOCK Crane System Analysis

This Page Intentionally Blank

Figure A-1 TDock Crane System Fault Tree, continued

Figure A-1 TRUDOCK Crane System Fault Tree, continued

This Page Intentionally Blank

Appendix A2
Fault Tree Analysis Data

This Page Intentionally Blank

FILES CONTAINING COMPUTER MODELS AND RESULTS**TRUDOCK Crane Design****MASTER DATA FILE****SIMON INPUT FILE****CUTSET DESCRIPTION FILE****COMPONENT IMPORTANCE FILE****MASTER DATA FILE FOR THE CRANE DESIGN**

<u>REFERENCE NO.</u>	<u>IDENTIFIER</u>	<u>FAILURE RATE</u>	<u>REFERENCE</u>	<u>COMMENT</u>
600	BC	8.00E-05	NUREG-0612	FAILURE OF WHB TRUPACT CRANE DISK BRAKE ¹
601	HX	8.00E-05	NUREG-0612	FAILURE OF WHB TRUPACT CRANE HELIX BRAKE ¹
602	AC	8.00E-05	NUREG-0612	FAILURE OF WHB TRUPACT DISK COIL ACTUATOR ¹
605	LOADINGS-A	1.456E+03	CALC	NUMBER OF CRANE A TRANSFERS/YEAR
	(25% contin.)	1.092E+03		
606	AC*	2.47E-05	IEEE-500	FAILURE OF TRUPACT ACTUATOR
607	DI*	3.00E-04	IEEE-500	FAILURE OF CRANE CONTROLLER LIMIT SWITCHES
608	CE	3.40E-06	NUREG-0612	CRANE CABLE/HOOK FAILS ²
612	LOADINGS-B	1.456E+03	CALC	NUMBER OF CRANE B TRANSFERS/YEAR
	(25% contin.)	1.092E+03		
613	BC	8.00E-06	CALC	FAILURE OF WHB TRUPACT CRANE DISK BRAKE DUE TO CC
614	HE	8.00E-06	CALC	FAILURE OF WHB TRUPACT CRANE HELIX BRAKE DUE TO CC
615	SUB-E2	4.34E-1	App. A6	LOSS OF POWER TO WHB CRANE
616	MO	4.63E-02	IEEE-500	CRANE MOTOR FAILURE
617	HE	8.70E-07	PLG, INC.	OPERATOR MAKES IMPROPER PIN CONNECTION

See Table 3.1-1 for complete description of reference sources

1) NUREG-0612, Page B-10, Failure of redundant component

2) NUREG-0612, Page B-10, Failure of non-redundant component

SIMON INPUT FILE FOR THE CRANE DESIGN

VER 1.6

'SIMON Case file for Tree: STONCRAN; Created: 05/06/96 14:18'

29

'Sub-E2 '	01	615	0.0332420.0
'T-BC-CRANEFA-FA '	01	600	0.0000000.0
'T-HX-CRANEFA-FA '	01	601	0.0000000.0
'T-MO-CRANEFA-FR '	01	616	0.0000000.0
'T-AC-CRANEFA-FA '	01	602	0.0000000.0
'T-AC1-CRANEFA-FA '	01	606	0.0000000.0
'T-DI1-CRANEFA-FA '	01	607	0.0000000.0
'T-AC2-CRANEFA-FA '	01	606	0.0000000.0
'T-DI2-CRANEFA-FA '	01	607	0.0000000.0
'T-AC3-CRANEFA-FA '	01	606	0.0000000.0
'T-DI3-CRANEFA-FA '	01	607	0.0000000.0
'T-LOADINGS-A '	01	605	0.0000000.0
'T-CE-CRANEFA-FA '	01	608	0.0000000.0
'T-CPCRANEFA-HE '	01	617	0.0000000.0
'T-BC-CRANEFA-FA '	01	600	0.0000000.0
'T-HX-CRANEFA-FA '	01	601	0.0000000.0
'T-MO-CRANEFA-FR '	01	616	0.0000000.0
'T-AC-CRANEFA-FA '	01	602	0.0000000.0
'T-AC1-CRANEFA-FA '	01	606	0.0000000.0
'T-DI1-CRANEFA-FA '	01	607	0.0000000.0
'T-AC2-CRANEFA-FA '	01	606	0.0000000.0
'T-DI2-CRANEFA-FA '	01	607	0.0000000.0
'T-AC3-CRANEFA-FA '	01	606	0.0000000.0
'T-DI3-CRANEFA-FA '	01	607	0.0000000.0
'T-LOADINGS-B '	01	612	0.0000000.0
'T-CE-CRANEFA-FA '	01	608	0.0000000.0
'T-CPCRANEFA-HE '	01	617	0.0000000.0
'T-BC-CRANEAB-CC '	01	613	0.0000000.0
'T-HE-CRANEAB-CC '	01	614	0.0000000.0

CRANE SYSTEM CUTSET DESCRIPTIONS

TREE NAME: Sonmod
 CUTDES VER. 1.70 11-17-89
 INPUT FILE: Sonmod.cds

CUTSETS FOR GATE (00001) WITH CUTOFF PROBABILITY OF 1.00E-15
 GATE (00001) IS: Tower Crane Falls Causing a Material Release

NUMBER CUTSET PROB. BASIC EVENT NAME EVENT PROB. IDENTIFIER

1	1.65E-03 2.74E-03	Number of Crane B Transfers per Year (25 percent contingency) Crane B Cable Hook Breaks	1.46E-03 1.10E-03 2.50E-06	T-LOADINGS-B T-CE-CRANEB-FA
2	1.65E-03 2.74E-03	Number of Crane A Transfers per Year (25 percent contingency) Crane A Cable Hook Breaks	1.46E-03 1.10E-03 2.50E-06	T-LOADINGS-A T-CE-CRANE-A-FA
3	1.27E-03 9.53E-04	Number of Crane B Transfers per Year (25 percent contingency) Improper Connections Due to Operator Error	1.46E-03 1.10E-03 8.70E-07	T-LOADINGS-B T-CPCRANEB-HE
4	1.27E-03 9.53E-04	Number of Crane A Transfers per Year (25 percent contingency) Improper Connections Due to Operator Error	1.46E-03 1.10E-03 8.70E-07	T-LOADINGS-A T-CPCRANE-A-HE
5	2.96E-10	Crane B Helix Brake Fails Crane Motor Failure Disk Brake Actuator Failure	8.00E-05 4.63E-02 8.00E-05	T-HX-CRANEB-FA T-MO-CRANEB-FR T-AC-CRANEB-FA
6	2.96E-10	Crane B Disk Brake Fails due to Broken Spring Crane B Helix Brake Fails Crane Motor Failure	8.00E-05 8.00E-05 4.63E-02	T-BC-CRANEB-FA T-HX-CRANEB-FA T-MO-CRANEB-FR
7	2.96E-10	Crane A Helix Brake Fails Crane Motor Failure Disk Brake Actuator Failure	8.00E-05 4.63E-02 8.00E-05	T-HX-CRANE-A-FA T-MO-CRANE-A-FR T-AC-CRANE-A-FA
8	2.96E-10	Crane A Disk Brake Fails due to Broken Spring Crane A Helix Brake Fails Crane Motor Failure	8.00E-05 8.00E-05 4.63E-02	T-BC-CRANE-A-FA T-HX-CRANE-A-FA T-MO-CRANE-A-FR
9	9.21E-11	Loss of Power to Bridge Cranes Crane B Disk Brake Fails due to Broken Spring Crane B Helix Brake Fails	1.44E-02 8.00E-05 8.00E-05	Sub-E2 T-BC-CRANEB-FA T-HX-CRANEB-FA
10	9.21E-11	Loss of Power to Bridge Cranes Crane A Disk Brake Fails due to Broken Spring Crane A Helix Brake Fails	1.44E-02 8.00E-05 8.00E-05	Sub-E2 T-BC-CRANE-A-FA T-HX-CRANE-A-FA
11	1.22E-11	Loss of Power to Bridge Cranes Disk Brake Actuator Failure Crane B Helix Brake Fails	1.44E-02 8.00E-05 8.00E-05	Sub-E2 T-AC-CRANEB-FA T-HX-CRANEB-FA
12	1.22E-11	Loss of Power to Bridge Cranes Disk Brake Actuator Failure Crane A Helix Brake Fails	1.44E-02 8.00E-05 8.00E-05	Sub-E2 T-AC-CRANE-A-FA T-HX-CRANE-A-FA
13	1.22E-11	Loss of Power to Bridge Cranes Common Cause Failure of Disk Brakes on Both Cranes (Spring) Common Cause Failure of Helix Brakes on Both Cranes (Spring)	1.44E-02 8.00E-06 8.00E-06	Sub-E2 T-BC-CRANEAB-CC T-HE-CRANEAB-CC

REDUCED SUM OF PROBABILITY OF FAILURE = 9.807E-03

 CONFIGURATION CONTROL

CODE NAME: CUTDES
 VERSION NO: 1.70
 DATE OF CONFIGURATION: NOVEMBER 21, 1989
 DATE OF ISSUANCE: NOVEMBER 21, 1989
 DATE: JUNE 11, 1996
 TIME: 11:15:59.7
 CONFIGURATION NO.: 5201670291133

Component Importance File for Crane Design

COMPLNK Version 2.20 9 16 1996 23:17:48

5ton2.cut

SYSTEM UNAVAILABILITY (Q) = 9.81E-03

NUMBER OF BASIC EVENTS = 29

NUMBER OF CUTSETS = 13

<u>BASIC EVENT</u>	<u>IMPORTANCE (%DECREASE)</u>	<u>NUMBER OF CUTSETS</u>	<u>DECREASE IN SYSTEM UNAVAILABILITY</u>	<u>BASIC EVENT PROBABILITY</u>
1 <u>T-LOADINGS-A</u> (25% contingency)	<u>50.12</u>	<u>2</u>	<u>4.915E-03</u>	<u>1.4600E-03</u> <u>1.1000E-03</u>
2 <u>T-LOADINGS-B</u> (25% contingency)	<u>50.12</u>	<u>2</u>	<u>4.915E-03</u>	<u>1.4600E-03</u> <u>1.1000E-03</u>
3 <u>T-CE-CRANE-A-FA</u>	<u>37.22</u>	<u>1</u>	<u>3.650E-03</u>	<u>2.500E-06</u>
4 <u>T-CE-CRANE-B-FA</u>	<u>37.22</u>	<u>1</u>	<u>3.650E-03</u>	<u>2.500E-06</u>
5 <u>T-CPCRANE-A-HE</u>	<u>12.95</u>	<u>1</u>	<u>1.2700E-03</u>	<u>8.7000E-07</u>
6 <u>T-CPCRANE-B-HE</u>	<u>12.95</u>	<u>1</u>	<u>1.2700E-03</u>	<u>8.7000E-07</u>
7 <u>T-HX-CRANE-A-FA</u>	<u>.00</u>	<u>3</u>	<u>7.764E-10</u>	<u>8.0000E-05</u>
8 <u>T-HX-CRANE-B-FA</u>	<u>.00</u>	<u>3</u>	<u>7.764E-10</u>	<u>8.0000E-05</u>
9 <u>T-MO-CRANE-A-FR</u>	<u>.00</u>	<u>2</u>	<u>5.9200E-10</u>	<u>4.6300E-02</u>
10 <u>T-MO-CRANE-B-FR</u>	<u>.00</u>	<u>2</u>	<u>5.9200E-10</u>	<u>4.6300E-02</u>
11 <u>T-BC-CRANE-A-FA</u>	<u>.00</u>	<u>2</u>	<u>3.882E-10</u>	<u>8.0000E-05</u>
12 <u>T-BC-CRANE-B-FA</u>	<u>.00</u>	<u>2</u>	<u>3.882E-10</u>	<u>8.0000E-05</u>
13 <u>T-AC-CRANE-A-FA</u>	<u>.00</u>	<u>1</u>	<u>3.882E-10</u>	<u>8.0000E-05</u>
14 <u>T-AC-CRANE-B-FA</u>	<u>.00</u>	<u>1</u>	<u>3.882E-10</u>	<u>8.0000E-05</u>
15 <u>Sub-E2</u>	<u>.00</u>	<u>3</u>	<u>3.697E-10</u>	<u>1.44E-02</u>
16 <u>T-BC-CRANEAB-CC</u>	<u>.00</u>	<u>1</u>	<u>9.22E-13</u>	<u>8.0000E-06</u>
17 <u>T-HE-CRANEAB-CC</u>	<u>.00</u>	<u>1</u>	<u>9.22E-13</u>	<u>8.0000E-06</u>
18 <u>T-AC1-CRANE-A-FA</u>	<u>.00</u>	<u>0</u>	<u>0.0000E+00</u>	<u>2.4700E-05</u>
19 <u>T-D11-CRANE-A-FA</u>	<u>.00</u>	<u>0</u>	<u>0.0000E-00</u>	<u>3.0000E-04</u>
20 <u>T-AC2-CRANE-A-FA</u>	<u>.00</u>	<u>0</u>	<u>0.0000E+00</u>	<u>2.4700E-05</u>
21 <u>T-D12-CRANE-A-FA</u>	<u>.00</u>	<u>0</u>	<u>0.0000E+00</u>	<u>3.0000E-04</u>
22 <u>T-AC3-CRANE-A-FA</u>	<u>.00</u>	<u>0</u>	<u>0.0000E-00</u>	<u>2.4700E-05</u>
23 <u>T-D13-CRANE-A-FA</u>	<u>.00</u>	<u>0</u>	<u>0.0000E-00</u>	<u>3.0000E-04</u>
24 <u>T-AC1-CRANE-B-FA</u>	<u>.00</u>	<u>0</u>	<u>0.0000E-00</u>	<u>2.4700E-05</u>
25 <u>T-D11-CRANE-B-FA</u>	<u>.00</u>	<u>0</u>	<u>0.0000E+00</u>	<u>3.0000E-04</u>
26 <u>T-AC2-CRANE-B-FA</u>	<u>.00</u>	<u>0</u>	<u>0.0000E+00</u>	<u>2.4700E-05</u>
27 <u>T-D12-CRANE-B-FA</u>	<u>.00</u>	<u>0</u>	<u>0.0000E+00</u>	<u>3.0000E-04</u>
28 <u>T-AC3-CRANE-B-FA</u>	<u>.00</u>	<u>0</u>	<u>0.0000E+00</u>	<u>2.4700E-05</u>
29 <u>T-D13-CRANE-B-FA</u>	<u>.00</u>	<u>0</u>	<u>0.0000E+00</u>	<u>3.0000E-04</u>

CONFIGURATION CONTROL

CODE NAME : COMPLNK

VERSION NO. : 2.20

DATE OF CONFIGURATION : NOVEMBER 22, 1989

DATE OF ISSUANCE : NOVEMBER 22, 1989

DATE : SEPTEMBER 16, 1996

TIME : 23:17:48:48

CONFIGURATION NO. : 5646185161963

Appendix A3
Method of Analysis: Fault Tree Modeling,
Guidelines and Assumptions

This Page Intentionally Blank

SECTION	TITLE	PAGE
A3.1	Fault Tree Guidelines for WIPP TRUDOCK Crane System Analysis	A3-4
A3.1.1	Analysis Objective	A3-4
A3.1.2	Overview of Fault Tree Construction	A3-4
A3.1.3	Construction of Fault Trees for WIPP TRUDOCK Crane System	A3-6
A3.1.4	Calculation of Unavailability	A3-8
A3.2	Assumptions for Fault Tree Analysis	A3-14
A3.2.1	General Assumptions and Clarifications	A3-14
A3.3	Treatment of Common Cause in Fault Tree Models	A3-19
A3.3.1	Introduction and Background	A3-19
A3.3.2	Application of Multiple Greek Letter Method	A3-22
A3.3.3	Common Cause Calculations in Revised Analysis	A3-25

A3.1 FAULT TREE GUIDELINES FOR WIPP TRUDOCK CRANE SYSTEM ANALYSIS

A3.1.1 General Analysis Objectives and Methodology

The objective of the WIPP TRUDOCK crane system analysis is to identify and quantify the annual probability of failure of systems, subsystems and components which could lead to a dropped load and hazardous waste material release.

A3.1.2 General Overview of Fault Tree Construction and Analysis

Fault tree techniques are used as the basis for quantitative analyses of critical safety systems. This section describes the conceptual description of a fault tree, its uses and its benefits. In addition, the Westinghouse fault tree analysis methodology and the primary symbols used in the fault tree construction are briefly described.

A fault tree is used to represent a reliability model of a physical system, just as a process and instrumentation diagram (P&ID) is used to represent a process model. Fault tree analysis is a systematic method for identifying, analyzing, prioritizing, and documenting potential safety or reliability problems.

Fault tree analysis is performed using system design information such as P&IDs and operating procedures established for test, maintenance, and plant operation. Fault tree construction is based on guidelines contained in the "Fault Tree Handbook," (NUREG-0492, March 1980). The top of the tree is established with a statement of the undesired event. The fault tree is logically developed using computer graphics and appropriate software from the "top" undesired event through progressively greater detail to the root cause of the system malfunction, such as individual component failure. Included are failures, such as random component failures, common cause faults and human errors, as well as test and maintenance time are included in the fault tree to evaluate the safety hazards or unavailability of the system.

A fault tree is composed of logic gates which permit or inhibit the passage of lower fault events to the "top" undesired event of the tree. These gates show the relationships of the input fault events required for the occurrence of intermediate fault events that cause the "top" undesired event.

Primary events (referred to as INITIATING EVENTS) are fault events that need no further development. Probabilities can be assigned to these events to determine the probability of undesired events.

An octagon or circle depicts an INITIATING EVENT (also known as a basic fault) that requires no further development and signifies that the appropriate limit of resolution has been reached. Unique identifiers will be assigned based on the guidance in the fault tree guidelines.

A diamond depicts a SYSTEM FAULT, an event that is not further developed, either because the event is insignificant or because information relevant to the event is unavailable. Unique identifiers will be assigned based on the guidance in the fault tree guidelines.

An INTERMEDIATE EVENT identifies a system malfunction that results from the combination of lower level fault events passing through a logic gate and is represented by a rectangle. A description of the INTERMEDIATE EVENT is given within the rectangle.

Gates serve to permit or inhibit the passage of fault tree logic up the tree. There are three frequently used types of fault tree logic gates: the OR GATE, the AND GATE, and the COMBINATION GATE. Other gates exist, but their use depends on the types of fault events being considered, the redundancy used in the system design, and other analysis factors.

An OR GATE defines the situation whereby the output event exists if any or all of the fault input events are present.

An AND GATE defines the situation whereby the output event exists only if all the fault events occur.

A COMBINATION GATE defines the situation whereby the output event exists if any combination of x of the y fault events occur.

Gate types represented by triangles are introduced as transfer symbols for the duplication of fault tree logic and primary events with a fault tree. These are more than just a convenient method of avoiding duplication. They are critical to ensure faults common to the contribution of an undesired event are properly represented.

A vertical line from the apex of the triangle denotes a TRANSFER IN symbol, and a horizontal line from the side denotes a TRANSFER OUT symbol. A TRANSFER IN symbol attached to a logic gate or an intermediate event must be linked to a TRANSFER OUT symbol. The TRANSFER OUT symbol contains that portion of the fault tree logic being transferred to another event or logic gate represented by the TRANSFER IN symbol.

A3.1.3 Construction of Fault Trees for WIPP TRUDOCK Crane System

Basis for Guidelines

In order to assure consistency in the system fault trees for the WIPP TRUDOCK crane system analysis, a set of basic guidelines was followed. The guidelines have been developed with the intent of following the principal methods now used in PRAs and as described in the "PRA Procedures Guide" (NUREG/CR-2300, Revision 1) and also outlined in "Probabilistic Safety Analysis Procedures Guide" (NUREG/CR-2815, Jan. 1984). Engineering judgment will be the final arbiter in taking exception to these guidelines and should be noted by the analyst in his/her tree documentation.

Identification of Components

The system fault tree includes key components. That is, those components that are important or essential to the operation of the system.

System Failure Modes

The top event of a system fault tree describes the failure of the system to perform a required function. For this analysis, the failure of cranes resulting in a hazardous waste material release is the top event developed in the tree based on the conditions that define the failure of the system.

The failure modes of a system are developed in a fault tree based on investigating and understanding the effects of various system component failures and the effects of support system and interfacing system failures. The failure of a system is usually the result of one or more of the following:

1. Failure of one or more active components such as motors,
2. Loss of main system function due to the failure of a support system such as electric power.

The failure of an electric power system to supply control or motive power to essential components and systems, is the most common type of electric power system failure that is described at the top of the fault tree. The other type of system failure is one that results in unintentional energization of one or more components, or in failure to deenergize a component. The modes of failure of electric power systems are : (1) failure of one or more

electrical components in the system, (2) improper operator actions, and (3) failure of systems that support electric power such as loss of cooling water to a diesel generator.

Structure and Content of Fault Trees

Fault trees for the WIPP TRUDOCK crane system analysis include the failure or unavailability of components due to random causes, human error, common cause and test and maintenance activities. The dependence that components have on shared subsystems or support systems are modeled in the system fault trees. Common cause failure of components will be analyzed according to the methodology described in Appendix A3. The calculations contained within the system analysis are in sufficient detail for later reproduction or sensitivity analysis.

Fault Tree Development

System fault trees were developed down to the level of major components failing to operate or function or to specific failure modes, as mandated by the needs of the analysis. Many components have two or more causes or modes of failure. For example, a valve failure may be the result of blockage, or failure of a contact to close and deenergize the valve to its appropriate relief path. A component of this type is described as having multiple modes of failure, because any one of the modes or causes of failure results in the failure of the component to function or operate. As a general guideline, multiple modes of failure will not be detailed in the fault trees because it is desirable that fault tree analyses not produce excessively long lists of minimal system cutsets as input to the fault tree linking model. The list of cutsets produced by quantification will be controlled by using single blocks in the fault tree that represent all of the multiple modes of failure of the major components. However, all modes of component failure will be properly accounted for in the process of quantifying the fault trees.

Fault tree development may include human error contributions involving incorrect positioning. This type of human error may include failure to restore a valve to its proper position following test or maintenance. Human errors of this type occur prior to the accident or fault sequences. In addition to the misposition errors, there may be errors that occur as a result of human interaction with the system during the fault sequence. The latter errors are not included in the fault trees. A general guideline for incorporating human error into the fault tree is to include the errors that occurred prior to the initiation of the fault sequence with the component multiple faults. Human errors that may occur during the fault sequence should be shown explicitly in the fault tree. If the human error results in the failure of a system, the error should appear at the second level of the fault tree.

Fault Event Identification Codes

Each system fault (diamond symbol) and basic component fault (round or octagonal symbol) in a fault tree will be given a fault event identification code that is exactly ten characters long.

The format of fault event identifiers in the system fault trees is XYYZZZZZWW where:

- X is the system code. This associates the identifier with a system specific analysis and is useful for the fault tree linking process. In the case of this analysis, the system code is "T", for TRUDOCK Crane, as no linking to other trees is performed.
- YY is the component type identification code from Table A3.1-1. This uniquely identifies the component type with which the identifier is associated. If a fault tree node is not associated with a specific component, these spaces should be filled with the independent identifier as described below.
- ZZZZZ is the component identifier. This identifier should clearly and uniquely identify the component involved and should be consistent with the component numbering that is used in the system analysis to describe the components. As far as possible, component identification codes should be the same as the component identification acronyms that appear on the plant drawings and documents. The identifier should be as descriptive as possible so that the event identifier can be associated with the component/failure mode when separated from its text block. If the system and component identification code is less than five characters long, it should be left justified and a dash (-) should be used to fill in the blanks to the right.
- WW is the failure mode identification code from Table A3.1-2. This identifier denotes the failure mode of the component or process identified by this node in the fault tree. If this component or process does not fail by a regular mode, these spaces should be filled with dashes (-) or an extension of the independent identifier, ZZZZZ.

A3.1.4 Calculation of Unavailability

Basic Component Unavailability

The unavailability of a basic component is the sum of the unavailabilities or failure probabilities of the individual modes of failure of the component.

Each system analysis should contain a tabulation of the unavailabilities of components that are modeled in the system fault tree. The general formula for calculating total component unavailability is:

$$Q = q(s) + q(o) + q(d) + q(e) + q(t) + q(m) + q(he)$$

Where:

$q(s)$	=	Component standby failure probability
$q(o)$	=	Component operating failure probability
$q(d)$	=	Component demand failure probability
$q(e)$	=	Failure probability of support systems
$q(t)$	=	Test outage unavailability
$q(m)$	=	Maintenance outage unavailability
$q(he)$	=	Component unavailability due to human error
Q	=	Total component unavailability

Not all of the failure modes will be applicable to each component. For example, a component may be in continuous operation during both normal operation and the accident sequences with the result that there would be no standby failure of the component. Entries for test and maintenance may also not be applicable to certain components.

In some cases the basic failure data selected for a component may encompass more than one mode of failure. For example failure of a pump to start encompasses a standby failure probability and a demand failure probability. The standby failure probability can be visualized as a probability that the pump is in a failed state or fails while idle. The demand failure probability involves the observation that the pump may fail each time that a demand is placed on it. For the sake of consistency, it is suggested that the probability of failure to start be listed as a demand failure probability. Other modes of pump failure such as failure of a valve in a seal or oil cooling subsystem for the pump can be included under pump standby failures if appropriate or included with the operating failure probability. Care should be taken to assure that there is no double-counting of standby and demand faults in the unavailability quantification.

Calculation of Hardware Failure Unavailability

When evaluating component failure contribution, one must consider whether the component is operating or in a standby mode. If the component is part of a standby system, the average unavailability is estimated using either a time-based failure rate or a demand failure probability for component failure in the standby mode.

A time-based failure rate is applicable when the failure mechanism causing the failure mode is related to the time the component is in standby between checks of its operability. The time between tests is thus an important part of the unavailability calculations of these components. A demand failure probability is appropriate for component failure modes that do not depend on the test period length, but rather are related to the number of times that the component is "demanded" to operate. The length of the test period is irrelevant for a component whose failure mode is truly demand dependent. The component average unavailability using a time-based failure rate is given by the expression:

$$q_c = 1/2 \lambda_s T_T \quad (1)$$

where q_c is the component average unavailability, λ_s is the standby failure rate (failures per hour), and T_T is the length of the test period (hours). An estimate obtained using this expression is adequate assuming an exponential failure distribution and if the product of $\lambda_s T_T \leq 0.1$.

The demand failure probability is given directly by the data base and thus:

$$q_c = q_d \quad (2)$$

where q_c is the component average unavailability and q_d is the demand failure probability.

A more appropriate model for calculation of the unavailability of components in standby, assuming that such components have both time-dependent and demand failure contributions, is given by:

$$q_c = q_d + 1/2 \lambda_s T_T \quad (3)$$

with the parameters q_c , q_d , λ_s and T_T defined as above. Data is usually not available, however, to estimate both the time-dependent and demand related portion of component standby unavailabilities.

The calculation model to compute the unavailability or failure probability of non-repairable components in an operating system is given by the expression:

$$q_c = \lambda_o T_M \quad (4)$$

with q_c as previously defined, λ_o is the operating failure rate (failures per hour) and T_M is the total defined mission time. Again, the expression is adequate assuming an exponential failure distribution and if the product of $\lambda_o T_M \leq 0.1$

In standby safety-related systems, components once actuated may fail to perform for the desired mission time (e.g., a pump fails to start and run for a desired time). The unavailability calculation model for such components is given as:

$$q_c = q_d + \lambda_o T_M \quad (5)$$

or

$$q_c = 1/2 \lambda_s T_T + \lambda_o T_M \quad (6)$$

with each parameter for both of the above expressions as previously defined. The selection of which expression to use for the quantification being performed is dependent on the type of data given by the selected data bank being used. Usually, expression (5) will be used to quantify the standby and operating failure probability of the component.

In some operating systems, component failures, once detected, may be repairable. The approximation expression for such components is given by:

$$q_c = \lambda_o \tau \quad (7)$$

where τ is the average total time in hours the component is out of service after it has failed and q_c and λ_o are as previously defined.

TABLE A3.1-1
COMPONENT IDENTIFICATION CODES

	<u>Code</u> <u>Letters</u>	<u>Component Identification</u>
Mechanical Components	FL	Strainer
	HX	Heat Exchanger
	CV	Valve, Check
	HV	Valve, Hydraulic Operated
	FV	Valve, Flow Control
	AV	Valve, Relief Pneumatic or Hydraulic Operated
	SV	Valve, Solenoid Operated
Electrical Components	RE	Relay
	TI	Timer
	TX	Proximity Sensor

TABLE A3.1-2
FAILURE MODE IDENTIFICATION CODES

<u>Code Letters</u>	<u>Failure Mode</u>
CC	Closed Fails Closed (Fails to Open)
FA	Loss of Function (i.e., Does Not Operate)
PL	Plugged
OC	Open Fails Closed (Spurious Closing or Fails Closed)
SP	Short to Power
CM	Common Cause (Common Mode Failure)

A3.2 ASSUMPTIONS FOR FAULT TREE ANALYSIS

A3.2.1 General Assumptions and Clarifications for Fault Tree Construction

Modeling Random Faults in Liquid and Air Systems

- a) Random mechanical failure of locked open manual valves need not be included in fault tree development since the probability of failure is not significant relative to other valve faults. The only credible random valve failure that might occur is plugging of an open valve.
- b) It was assumed that all piping is rated and specified to accommodate the maximum pressure which could be supplied by any single component failure. Both the piping and valves are rated at the maximum pressure which could be expected during blockage situations. Pipe ruptures and orifice plugging are usually not significant contributors to system unavailability or failure. Although a system may be in standby for long periods of time prior to the accident, other system faults such as valves being incorrectly positioned, valves not opening/closing on demand, or pumps not starting and running on demand will usually dominate. If plugging of orifices or piping can result from chemical crystallization, such as might occur if heat tracing were lost, then a local plugging fault in the pipe should be included in the fault tree.
- c) Incorrect positioning of normally open manual-, air-, and motor-operated valves prior to the event due to human error and/or spurious control signal will be considered a system fault, if credible (see subsection on test and maintenance unavailability for additional considerations).
- d) Incorrect positioning of valves prior to an event will not be included in the fault trees if the valve receives an automatic signal to return to its normal or safe position under event conditions. When opening or closing time is critical for the condition, it should be evaluated on a case-by-case basis.

- e) Potential flow diversion paths will be included as system faults if the diameter of the potential diversion path is greater than one third of the diameter of the main flow path. However, if the pressure differential between the desired path and the potential diversion path is extremely high, diversion paths with diameters less than one third of the main diameter may prove to be significant.
- f) Potential flow diversion paths isolated from the main flow path by normally closed valves can cause a system fault if one or more valves that isolate the path are inadvertently open. Incorrect positioning of a valve prior to the event due to human error and or spurious control signal should be considered in this analysis, if credible. Potential flow diversion paths of a fluid system that are isolated from the main flow path by one or more locked closed valves will not be considered as faults of the system.
- g) Control circuit faults of components after successful initial operation will be considered only in those cases where the component is expected to receive an additional signal during the course of the event to readjust or change its operating state.
- h) Tank failures related to plugging or blockage of the fluid path due to failure or mispositioning of valves in the line from the tank should be included in the fault trees.
- i) The failure of heat exchangers or coolers to transfer heat may be the result of plugging of the primary side or leakage from the primary to secondary side. Plugging need not be included as a component fault if the heat exchanger performance in this regard is checked periodically during normal operation and if accelerated plugging or fouling due to chemical crystallization (Refer to Item b in this section) is found to have a very low probability of occurrence or is not applicable. Leakage from tubes need not be considered if the heat exchanger is inspected and tested for leaks periodically when taken out of service.

- j) Check valves failing closed to flow in the forward direction and failing open to flow in the reverse direction will be included as credible faults only when the valve is located in a pipe not used in normal operation. The failure of those check valves and normally open manual valves located in a pipe used in normal operation will not be modeled in the fault trees.
- k) It is assumed that the system is structurally designed for thermal stresses/shocks and any necessary bounding analyses would be performed as part of the design. Therefore, these failure modes and structural failures in general are not explicitly analyzed.
- l) Ambient temperatures in this region are not expected to be at or below the freezing point of water precluding the need for development of equipment failures or system faults initiated by freezing.
- m) The cause and effects of sabotage are outside the scope of this analysis.

Considerations for Test and Maintenance Unavailability

- a) Unavailability of components due to test or maintenance and human errors associated with failing to restore components to their operable state, following test or maintenance, are considered along with random hardware faults.

A component can be tested or maintained during system operation if it can be isolated from the system by a manual valve or power operated valve in series with the component.

- b) The preferable method of treating test and maintenance unavailability in the fault trees is to include the unavailability with the multiple faults of the component.

- c) It is possible that the fault tree quantification may count the simultaneous test and maintenance unavailability of two or more redundant components in separate trains. If procedures prohibit this type of simultaneous outage, the quantification results would be conservative. However, this double-counting would not be immediately apparent since test and maintenance would be hidden in the random component failure modes. We will, however, examine all dominant cutsets to identify any such double-counting or other significant contributors and revise the modeling as necessary.
- d) Only those components that are tested during normal operation of the TRUDOCK crane system, or those that are rotated in and out of service during normal operation, will be considered maintainable.
- e) The test mode of a pump and its associated valves and other components that prevent a system from meeting its design safety function will be considered as a credible failure mode, unless automatically realigned within acceptable time limits.
- f) Stroke testing is assumed for all valves following a maintenance operation.
- g) One assumption that was made in conducting this evaluation was that sensors and related components are regularly tested and calibrated. No attempt was made in this study to evaluate the possible consequences of faulty signals due to the miscalibration of sensors.
- h) Proper maintenance is a critical factor in safe system operation. It must be recognized that poor maintenance and maintenance practices have the potential for being a critical contributor to problems. Explicit identification of specific failures which could occur during equipment maintenance is beyond the scope of this study. General problems which could occur during maintenance are identified.

Operator Action and Human Error

- a) Operator recovery of failed systems may be modeled if credible from diagnostic, time frame, and accessibility viewpoints. "Verify" statements in procedures which instruct the operator to verify the functioning of automatic safety systems are treated as recovery operations, and thus are not included in the fault tree analysis. Local indicators and alarms, such as those in a location not continually manned, should not normally be considered.
- b) At the start of the shift, a "pre-operational crane checks" test will be performed. This test will verify the crane system is operational. If the crane system does not pass this test, it will not be placed into service, until the necessary corrective actions are completed and the crane system passes the test. Further, during the crane system operation, if the crane system does not perform as required, the crane system will be removed from service. Again, it will not be returned to service until the malfunction is corrected and the crane system passes the same test.

If the crane system is to be operated more than one shift per day, or there is a change of operator, the crane system will be removed from service and the same "pre-operational crane checks" test will be performed as described above.

Consideration of Common Cause Faults

Common cause failure must be considered for active components such as pumps, fans, and valves that are of the same design and which operate in a redundant application in the same type of service or environment. Check valves and strainers (in open or once-through systems) may also be subject to common cause failure.

Common cause failure of two or more similar components that are not of the same design or manufacture should be considered if the components can be subjected to a common abnormal environment during an accident sequence which is outside of the design basis of the components.

Modeling Random Faults in Electrical Systems

Considerations for Random Faults

- a) Local faults of wiring or cables should be considered for inclusion in electrical system fault trees. The failure modes judged to be most appropriate for the facility are open circuit failures and short to ground faults. Short to power wiring faults are also included.

Considerations for Test and Maintenance Unavailability

- a) Components such as protective relays are not tested during normal operation. Normally, the required operational tests of these systems will be performed when the crane is shutdown.

A3.3 TREATMENT OF COMMON CAUSE IN FAULT TREE MODELS

Purpose

The purpose of this section is to describe the method for quantifying common cause failures in fault tree models. These types of dependent failures are typically analyzed as part of a system (fault tree) analysis and often represent the dominant contributors to system failure. The Multiple Greek Letter (MGL) method is used to analyze common cause failures.

A3.3.1 Introduction and Background

The term "common cause failure" (CC) is widely employed to describe events involving hardware failures or unavailabilities that are the result of the same (single) cause. Equipment redundancy, which has been utilized to avoid system and functional level failures, is potentially susceptible to this kind of event. Because dependent failures are extremely important in system unavailability quantifications, adequate treatment of common cause failures must be given to avoid a possible underestimation of system unavailability.

For this study, component related common cause failures will be explicitly quantified using the Multiple Greek Letter Method (MGL) applied to each system, for each distinct set of mission success requirements arising from distinct accident initiators.

This document provides a procedure for calculating common cause failures using the MGL method and the recommended factors to use in the calculation.

Background

The treatment of common cause in fault tree models and the specific use of the MGL method for this study is consistent with Westinghouse and industry practice (see references). The following describes the MGL method and its relation to the beta-factor method. The beta-factors are defined and used as the conditional probability of a common cause initiated failure of a component, given that a "similar" component has failed.

The MGL method is an extension of the beta-factor method. In the MGL method, other parameters in addition to the beta-factor are introduced to distinguish among common cause events affecting larger numbers of components in a higher order redundant system.

The beta-factor method assumes that Q , the total (constant) failure probability rate for each component, can be expanded into independent and dependent failure contributions:

$$Q = Q_r + Q_{cc}$$

where Q_r is the unit failure probability for independent failures and Q_{cc} is the unit failure probability for dependent failures.

For convenience, a parameter, β , is defined as the fraction of the total failure probability of a component attributable to dependent failures:

$$\beta = \frac{Q_{cc}}{Q_r + Q_{cc}} = \frac{Q_{cc}}{Q}$$

so that $Q_{cc} = \beta Q$

The MGL parameters are an extension of the beta factor and consist of a set of failure fractions (or extended beta-factors) used to quantify the conditional probabilities of all the possible ways a common cause failure of a component can be shared with other components in the same group, given component failure has occurred. For a system of "m" redundant components and for each given failure mode, "m" different parameters are defined.

For the MGL Method, different beta-factors are used to describe dual and multiple component dependencies:

$\beta_2 =$ failure of exactly two components due to common cause

$\beta_3 =$ failure of exactly three components due to common cause

$\beta_4 =$ failure of exactly four components due to common cause

In general:

$\beta_i =$ fraction of total failures of a given train or component that will result in the dependent failure of another i-1 specific trains or components

These fractions are easy to use as a multiplier to a total failure probability or unavailability. However, they should only be used for similar, applicable component populations in order to properly represent the magnitude of the common cause effects.

A3.3.2 Application of Multiple Greek Letter Method

This section identifies the approach for the application of the Multiple Greek Letter Method to fault tree analysis for both two and multiple component dependencies.

Two Component Dependencies

For a system (or cutset) containing two parallel and identical components and with a success criteria of either of the two components functioning, the unavailability of the system due to independent (random) failures is simply:

$$Q = Q_a * Q_b, \text{ where}$$

$Q_a =$ the total failure probability of component "a"

$Q_b =$ the total failure probability of component "b"

To account for component failure dependencies, the common cause failure contribution can be simply calculated as:

$$Q_{cc} = \beta * Q_a$$

Multiple Component Dependencies

The treatment of multiple component dependencies is similar to that for the treatment of dual components in that both independent and dependent failures must be considered. To properly account for component failure dependencies, the common cause failure contribution can be simply calculated as:

$$Q_{cc} = \text{SUM [Common Cause Failure Contribution of Each Combination of 2 Components (applying } \beta) * \text{Random Failure Contribution of Remaining Components]} + \\ \text{SUM [Common Cause Failure Contribution of Each Combination of 3 Components (applying } \beta_3) * \text{Random Failure Contribution of Remaining Components]} + \\ \text{etc.}$$

Higher order beta-factors were defined earlier to accommodate for the dependency potential between multiple parallel trains/components. In general:

To apply these beta-factors for higher order systems, the equations in Table A3.3-1 may be useful. These are derived from combinations of component dependent failures and independent failures.

The dependency data used for the treatment of common cause in these fault tree models is consistent with Westinghouse and industry practice. The general factors of $B_2 = 0.10$, $B_3 = 0.05$, and $B_4 = 0.04$ are used in this analysis.

TABLE A3.3-1
EQUATIONS USEFUL FOR COMMON CAUSE CALCULATIONS
MULTIPLE GREEK LETTER METHOD

Failure Criteria	Success Criteria	Common Cause Contribution
2/2	1/2	$\beta * Q$
3/3	1/3	$3 * \beta * Q^2 + \beta_3 * Q$
2/3	2/3	$3 * \beta * Q + \beta_3 * Q$
4/4	1/4	$6 * \beta * Q^3 + 4 * \beta_3 * Q^2 + \beta_4 * Q$
3/4	2/4	$12 * \beta * Q^2 + 4 * \beta_3 * Q + \beta_4 * Q$
2/4	3/4	$6 * \beta * Q + 4 * \beta_3 * Q + \beta_4 * Q$
<p>NOTE:</p> <p>1. Q is equal to the total unavailability for the particular component and failure mode.</p>		

A3.3.3 Common Cause Calculations in Revised Analysis

This section documents the common cause modeling of specific components identified in the fault tree analysis. Calculations are based on the Multiple Greek Letter methods. There are two such common cause events which are explicitly modeled because they are critical to system performance:

2 disc brakes fail (Master Data Bank Line #613)

The generalized equation for 2 component common cause failure is:

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

P_{cc} is the probability of common cause failure

Q is the random failure probability of the component

β is the Beta-factor (0.1 used for a generic component)

$$P_{cc} = 0.1(8.0E-05/\text{hr.})$$

$$P_{cc} = 8.0E-06/\text{hr.}$$

2 helix brakes fail (Master Data Bank Line #614)

$$P_{cc} = 0.1(8.0E-05/\text{hr.})$$

$$P_{cc} = 8.0E-06/\text{hr.}$$

This Page Intentionally Blank

Appendix A4
PLG Human Reliability Analysis
(August 20, 1996)

This Page Intentionally Blank

Evaluation of Human Reliability during Crane Operations with Contact Handled Waste in the Waste Handling Building

Improper Insertion of 2-Out-Of-3 Long Lift Leg Connector Pins (Locking Pins)

The following series of events are required for a drum drop due to failure to properly attach two long lifting legs to the crane load leveling fixture. Human error may occur at four points in the process.

1. **Human Error A.** Handler fails to fully insert one lift leg connector pin.
2. **Human Error B.** Handler fails to fully insert second pin, given previous failure.
3. Both improperly inserted pins function sufficiently to maintain the long lifting legs in alignment as crane is moved to the TRUPACT II container.
4. **Human Error C.** Spotter fails to detect improperly inserted pins as legs inserted into lift leg guide tubes in the drum stack and engage the lifting lugs on the TRUPACT pallet.
5. Both improperly inserted pins are capable of transferring sufficient torque to successfully rotate long lifting legs into the locked position.
6. The combination of properly and improperly inserted pins initially carry the load of the drums and are able to lift them clear of the TRUPACT II container.
7. **Human Error D.** Spotter fails to detect improperly inserted pins when the spotter inspects clearance and smoothness of the lifting process as drums are lifted from the TRUPACT II container, given his/her failure to observe the improperly inserted pins when the lift legs were inserted into the lift leg guide tubes on the TRUPACT pallet.

8. One improperly inserted pin disengages under load. The second improperly inserted pin is assumed to disengage if the first has disengaged, because of the shifting balance of the load.

The contribution of human error to this sequence of events has been quantified using the Technique for Human Error Rate Prediction (THERP) methodology of NUREG/CR-1278.⁸ The human reliability analysis event tree shown in Figure 1 depicts the relationship of the four errors required for failure. The opportunity to not fully insert two pins can occur only if the first or second pin is not properly inserted. Success will occur if any insertion error is detected, as this will generate a recheck of the security all pins.

Figure 1. Human Reliability Analysis Event Tree for Improper Insertion of 2-Out-Of-3 Long Lifting Leg Connector Pins

Table 1 provides the justification for the selection of human error probabilities (HEP) for each of these errors. No reduction in frequency is estimated to account for the likelihood that events 3, 5, 6, or 8 will occur. These events must also occur for the accident to result in a drop of waste drums from the maximum lift height of the crane.

Swain, A. D., and H. E. Guttman. "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications." Sandia National Laboratories, prepared for U.S. Nuclear Regulatory Commission, NUREG/CR-1278, SAND80-0200, August 1983.

Failure to Engage the Long Lifting Legs to the TRUPACT Pallet Lifting Lugs

Failure of the long lifting legs to engage the TRUPACT pallet lifting lugs due to human error is judged to be incredible for the following reasons:

1. The guide tubes provide an unobstructed and fully controlled access for the long lifting legs to the lifting lugs on the TRUPACT pallet.
2. The distance from the top of the waste package to the lifting lugs is fixed, and this distance is marked clearly with a red band on all three lifting legs. The tips of the lifting legs contact the top of the lifting lugs as the bottom of the red band becomes flush with the top of the waste package, and the lifting leg slots that allow engagement of the hooks are fully seated when the top of the red band is flush with the top of the package. All three bands must be flush before the lifting legs are rotated to the locked position.
3. All three long lifting legs are rotated at the same time to engage the lifting lugs. The rotation is verified by both the limit switch indications and by visual observation of the pistons providing the motive force and the rotating legs. The continued maintenance of the proper level for engagement of the lifting leg hook to the pallet lift lug is verified by the top of the red band staying flush with the package top.
4. When lifting begins, all three red bands rise about 1 inch out of the top of the waste package, corresponding to the free play to the seat of the lifting hook. As they engage the pallet lifting lugs, the bands stay at 1 inch and the crane hook and cables tension. If only one hook were engaged, the band width for the two unengaged hooks would become wider. In addition, the level indicators would indicate tilting.
5. As the waste package is lifted, the spotter inspects continued clearance and smoothness of the lifting process. An asymmetric pull that would be indicative of unengaged hooks would most likely be revealed by increase in scraping or binding.

Table 1. Point Estimate of Failure to Properly Insert 2-Out-Of-3 Lifting Leg Connector Pins to Crane Leveling Fixture

Symbol	HEP	Explanation of Error	Source of HEP
A ₁	3.7E-03	Improperly mate a connector, including failure to test the locking feature for engagement.	Table 20-12,* Item (13), mean value
B ₁	0.75	The operator repeating the action is modeled to have a high dependency for making the same error again. It is not complete dependence, because the operator moves to the second lifting leg and must physically push the locking balls to insert the pins.	Table 20-21,* Item (4)(a), high dependence for different pins. Two opportunities (the second and third pins) to repeat error is modeled as $0.5 \cdot (1 - 0.5) \cdot 0.5 = 0.125$.
C ₁	1.2E-03	Checker fails to verify the proper insertion of the connector pins, and that status affects safety when performing tasks.	Table 20-22,* Item (9), mean value
D ₁	0.15	Checker fails to verify the proper insertion of the connector pins at a later step, given the initial failure to recognize the error. Sufficient separation in time and additional cues to warrant moderate rather than total or high dependence.	Table 20-21,* Item (3)(a), moderate dependence for second check.
F ₁	5.2E-07	Failure rate if first pin improperly connected.	Product of above HEPs.
a ₁	0.996	Given the first pin was properly connected	$1 - F_1$
A ₂	3.7E-03	Improperly mate a connector, including failure to test the locking feature for engagement.	Table 20-12,* Item (13), mean value.
B ₂	0.5	The operator repeating the action is modeled to have a high dependency for making the same error again. It is not complete dependence because the operator moves to the second lifting leg and must physically push the locking balls to insert the pins.	Table 20-21,* Item (4)(a), high dependence. Only one opportunity for error (the third pin).
C ₂	1.2E-03	Checker fails to verify the proper insertion of the connector pins, and that status affects safety when performing tasks.	Table 20-22,* Item (9), mean value.
D ₂	0.15	Checker fails to verify the proper insertion of the connector pins at a later step, given the initial failure to recognize the error. Sufficient additional cues and separation in time to warrant moderate, rather than complete or high, dependence.	Table 20-21,* Item (3)(a), moderate dependence for second check.
F ₂	3.5E-07	Failure rate if first pin properly connected.	Product of above HEPs.
F _T	8.7E-07	Total failure rate due to human error.	$F_1 + F_2$

*Found in NUREG CR-1278.

Appendix A5
PLG Waste Isolation Pilot Plant Trupact Crane System Analysis

PLG, Inc.
4590 MacArthur Boulevard, Suite 400
Newport Beach, CA 92660-2027
(714) 833-2020 Fax (714) 833-2085

Member of The Failure Group, Inc.

September 11, 1996
WEC-3140-PLG-05

Mr. Doug Gertsner
Westinghouse Electric Company
Waste Isolation Pilot Plant
Nuclear Safety and Assessment
P.O. Box 2078
Carlsbad, NM 88221

Dear Doug:

WASTE ISOLATION PILOT PLANT TRUPACT CRANE SYSTEM ANALYSIS

The preliminary version of the subject analysis lists a failure "rate" of 2.0×10^{-5} per demand for crane cable/hook failures and cites NUREG-0612¹ as the basis for this value. A review of NUREG-0612 indicated no specific reference to cable or hook failures. An independent evaluation of the failure rate data provided in NUREG-0612 indicates that the crane cable/hook failure rate should be less than approximately 2.5×10^{-6} per demand. In addition, the crane failure rates cited in NUREG-0612 are based primarily on Navy crane data compiled in the 1970s. The operating environment existing at WIPP is much less demanding than those for Navy cranes, and the WIPP has established aggressive inspection and maintenance programs to assure the continuing reliability of the cranes. Taking the WIPP operating conditions and reliability controls into account would lower the failure rate even more but it is difficult to quantify this additional improvement.

The enclosed fault tree for crane failure represents the fault tree for crane failure which is shown on Page 5-15 of NUREG-0612. Relative to this fault tree, the contributions of cable and hook failures must be "embedded" in fault tree events CF1 ("Load Hangup" Event), CF2 ("Failure Due to Random Component Failure"), CF3 ("Two-Blocking" Event), and CF4 ("Failure of Component That Doesn't Have Backup"). Event CF2 involves components that have backup. Events CF1 and CF3 represent failures due to operator error. Crane failure is assumed to occur if the overload devices and limit switches fail. Since events CF2 and CF4 could contain other component failures as well, the failure rates associated with the top event "Failure of Crane"

¹ U.S. Nuclear Regulatory Commission, "Control of Heavy Loads at Nuclear Power Plants," NUREG-0612, July 1980.

Mr. Doug Gertsner
Westinghouse Electric Company

September 11, 1996
Page 3

wire rope (cable), hook, and power/control cables "prior to the first crane operation each shift."
The hook and wire rope are also inspected monthly.⁵

In summary, a re-evaluation of the NUREG-0612 database used for crane failures suggests that the crane cable/hook contribution is of the order of 2.5×10^{-6} per demand. In addition, there appears to be sufficient evidence to demonstrate that the design conservatism and operating environments associated with the WIPP cranes is much better than that of the Navy cranes which form the database for the NUREG-0612 analysis. However, the impact of this evidence is extremely difficult to quantify and no additional credit has been taken for this potential improvement.

Very truly yours,

for: R. Kenneth Deremer

KRD/jhp
Enclosure
W413005.RKD
MS Word 6.0

cc: Mr. Bert C. Morris, P.E., Westinghouse Electric Company, Pittsburgh

⁵ Monthly Maintenance Procedure PM041111, "Inspection of Hook and Rope on 5 Ton Crane 41-T-151A & B," Rev. 1, April 4, 1996.

Figure 1. Fault Tree for Crane Failure

Appendix A6
WIPP Power Outages

WIPP POWER OUTAGE HISTORY

<u>Date</u>	<u>SPS (utility/offsite)</u>	<u>WIPP (onsite)</u>	<u>Comment</u>
12/08/82	X		Probably preventable with additional transmission line (under construction)
10/23/83		X	
05/16/84		X	
01/31/85		X	
1995	X		Post-'85 data per Lahey discussion
~04/96	X		Post-'85 data per Lahey discussion
Thru 05/96	3	3	

Elapsed time, 08/82 to 05/96, yr		1.383E+01
Failure rate lambda, SPS, failure/yr	$3/(1.383E+01) =$	2.169E-01
Failure rate lambda, WIPP, failure/yr	$3/(1.383E+01) =$	2.169E-01
Lambda projected, SPS with additional transmission line, failure/yr	$2/(1.383E+01) =$	1.446E-01

Sources: 1) Facilities Engineering letter to R.M. Coleman, HA:85:0549
 2) Discussion with Dave Lahey, Electrical Engineering Department

ANNUAL PROBABILITY OF LOSS OF POWER TO TRUDOCK CRANE

	Offsite	Offsite Projected + Onsite	Projected Offsite Offsite	Projected Offsite + Onsite
Failure rate lambda(l), failure/yr	2.169E-01	4.338E-01	1.446E-01	3.615E-01
Mission time t, yr	1.563E-01	1.563E-01	1.563E-01	1.563E-01
$l*t$	3.389E-02	6.778E-02	2.259E-02	5.648E-02
Probability $p = 1 - \exp(-lt)$	3.332E-02	6.553E-02	2.234E-02	5.491E-02

TRUDock Crane System Analysis

- page 1-1, ¶1
Is "annual frequency of failure" a standard technical term? It gives the impression (especially since it is at the start of the executive summary) that a failure is expected annually. Can the word "annual" be dropped? *Incorp. mnc*
- page 1-1, Section 1.1
"The cranes had not been previously analyzed and ..." Analyzed for what? for failure modes? -?- *Corrected mnc*
- page 1-2
About 2/3 of the way down the statement is made that the cranes are rated at 5 tons, and the max payload is 3.5 tons. This could imply a safety factor that is not truly present, since the max payload, the heaviest ACGLF and the heaviest SWB lift fixture total 9,985 lb. *No change mnc*
- page 1-3, Section 1.6
The next-to-last sentence says there is a TDOP lift fixture adaptor. To my knowledge there is no such unit on the site at this time; I don't think one exists at any other site either. *No change mnc*
- General suggestion for section 2.0 and following.
Define a "payload" (or any other suitable term) as the contents of the TRUPACT-II, which may be two 7-packs; two SWBs, or one TDOP early in the section. Then use the term selected through the rest of the document. *Incorp. mnc*
- page 2-1, Section 2.1.1, ¶1 Editorial
Change "containers" to "container" in the first line. *Corrected mnc*
- page 2-1, Section 2.1.1, ¶3
The radiological surveys are conducted before and during lid removal. *No change mnc*
- page 2-2, Section 2.1.1, last ¶
Lift legs are rotated for 7-packs, but not when handling SWBs. Actions for TDOP are indeterminate, but will probably parallel the SWB. *mnc
No change. Corrected mnc
10/24/96*

*mnc
10/24/96*