SAA09FTB3-003
REV. A
DECEMBER 1993

SYSTEM ASSURANCE ANALYSIS

OF THE

90-TON PAYLOAD HOIST

AT THE

ROTATING SERVICE STRUCTURE HOIST

EQUIPMENT ROOM PAD-B

Baseline Number: 422.00

PMN: K61-0168

WUC: RWFHTRA000

SS/FC: RW

SYSTEM: CRITICAL

National Aeronautics and
Space Administration

John F. Kennedy Space Center

NASA

KSC FORM 16-12 (REV. 8/76) (C/G 8/91)

NOTICE - When Government drawings, specifications, or other data are used for any purpose other than in connection with a definitely related Government procurement operation, the United States Government thereby incurs no responsibility nor obligation whatsoever; and the fact that the Government may have formulated, furnished, or in any way supplied the said drawings, specifications or other data is not to be regarded by implication or otherwise as in any manner licensing the holder or any other person or corporation, or conveying any rights or permission to manufacture, use, or sell any patented invention that may in any way be related thereto.

APPLICATION		PART NO.	MF
NEXT ASSY	USED ON		

REVISIONS

SYM	DESCRIPTION	DATE	APPROVAL
NEW	THIS SAA CANCELS AND SUPERSEDES SAA09FY05-001. PERFORMED 1R ANALYSIS.	3-23-90	MKG Jr
A	GENERAL REVISION TO INCORPORATE SYSTEM MODIFICATIONS. EO 1 INCORPORATED ADDING HAZARD RT-ENG-1019. OPEN AREA OF CONCERN ELIMINATED.	1/28/94	MKG

Prepared By: Bruce J Kalle 12/15/93
B. KALLE, LSOC 52-11
RELIABILITY ENGINEER

Concurrence: Gary M Whitmore 12/15/93
G. WHITMORE, LSOC 52-11
SYSTEM SAFETY ENGINEER

Approval: for J. JOYNER, RT-ENG

Concurrence: Tony Shibly 1-19-94
T. SHIBLY, LSOC 32-20
SYSTEM DESIGN ENGINEER

Approval: Larry D. Jones 1/19/94
L. JONES, TE-FAC-2

Concurrence: 1/18/94
J. BENEFIELD, LSOC 33-27
SYSTEM ENGINEER

UNLESS OTHERWISE SPECIFIED DIMENSIONS ARE IN INCHES TOLERANCES ON FRACTIONS DECIMALS ANGLES	ORIGINAL DATE OF DRAWING SEPT 1989	SYSTEM ASSURANCE ANALYSIS OF THE 90-TON HOIST AT THE ROTATING SERVICE STRUCTURE HOIST EQUIPMENT ROOM PAD-B OMD BASELINE NO. 422.00	JOHN F. KENNEDY SPACE CENTER, NASA
MATERIAL	DRAFTSMAN / CHECKER		
	TRACER / CHECKER		KENNEDY SPACE CENTER FLORIDA
	ENGINEER KALLE / ENGINEER		
HEAT TREATMENT	SUBMITTED F. HARPER, RE SUPV.		
FINAL PROTECTIVE FINISH	APPROVED A. STEVENS, RE MGR.	SCALE / UNIT WT	DWG SIZE A / SAA09FTB3-003
			SHEET 1 OF 83

KSC FORM 21-2C (REV. 3/76) (C/G 8/91)

TABLE OF CONTENTS

1.0 SUMMARY OF FINDINGS AND RECOMMENDATIONS 4
1.1 CRITICALITY ASSESSMENT SUMMARY 4
1.2 MECHANICAL FMEA SUMMARY 4
1.3 ELECTRICAL FMEA SUMMARY 4
1.4 FLEXHOSE FMEA SUMMARY 4
1.5 ORIFICE FMEA SUMMARY 4
1.6 FILTER FMEA SUMMARY 4
1.7 HAZARD ANALYSIS SUMMARY 4
1.8 LPS CONTROL/MONITOR FUNCTIONS REVIEW SUMMARY 4
1.9 SNEAK CIRCUIT ANALYSIS SUMMARY 5
1.10 RECOMMENDATIONS 5
1.11 AREAS OF CONCERN SUMMARY 5
1.12 CRITICALITY CATEGORY 1R ITEMS SUMMARY 5

2.0 SYSTEM BASELINE/GROUND RULES/DEFINITIONS/DOCUMENTATION 5
2.1 SYSTEM BASELINE 5
2.2 GROUND RULES 5
2.3 DEFINITIONS OF CRITICALITY AND HAZARD CATEGORIES 5
2.3.1 Criticality Definitions and Categories. 5
2.3.2 Hazard Definitions and Categories. 7
2.4 DOCUMENTATION LIST 8

3.0 SYSTEM DESCRIPTION 10
3.1.1 ANALYSIS OF WIRE ROPE DRUM, GEARBOX SHAFT, AND GEAR RETENTION METHODS. 11

4.0 CRITICALITY ASSESSMENT 17

5.0 FAILURE MODES AND EFFECTS ANALYSIS (FMEA) 21
5.1 MECHANICAL FMEA 21
5.2 ELECTRICAL FMEA 25
5.3 FLEXHOSE FMEA 47
5.4 ORIFICE FMEA 47
5.5 FILTER FMEA 47

6.0 CRITICAL ITEMS LIST 47

7.0 HAZARD ANALYSIS 47
7.1 SAFETY CRITICALITY ASSESSMENT 47
7.2 SCOPE 47
7.3 SUMMARY OF ANALYSIS 48
7.4 FAULT TREE ANALYSIS 62
7.5 HAZARD ANALYSIS WORKSHEETS 71

8.0 LPS CONTROL/MONITOR FUNCTIONS REVIEW 78

9.0 END-TO-END ANALYSIS 78

10.0 SNEAK CIRCUIT ANALYSIS 80

11.0 EMERGENCY SAFING ANALYSIS 80

12.0 AREAS OF CONCERN 80

13.0 CRITICALITY CATEGORY 1R ANALYSIS 80
13.1 RELIABILITY BLOCK DIAGRAM 80
13.2 CRITICALITY CATEGORY 1R ITEMS 82

LIST OF ILLUSTRATIONS

1. PAD-B 90-TON PAYLOAD HOIST 13
2. PAD-B 90-TON PAYLOAD HOIST, MECHANICAL ARRANGEMENT 14
3. PAD-B 90-TON PAYLOAD HOIST, BLOCK DIAGRAM 15
4. PAD-B 90-TON PAYLOAD HOIST, BAND BRAKE ASSEMBLY 16
5. SYSTEM FUNCTIONS BLOCK DIAGRAM 18
6. 90-TON HOIST PAD-B, ELECTRICAL SCHEMATIC 27
7. 90-TON HOIST PAD-B, ELECTRICAL SCHEMATIC (CONTINUED) 28
8. 90-TON HOIST PAD-B, ELECTRICAL SCHEMATIC (CONTINUED) 29
9. END-TO-END BLOCK DIAGRAM 79
10. RELIABILITY BLOCK DIAGRAM 81

LIST OF TABLES

1. SYSTEM DOCUMENTATION LIST 9
2. CRITICALITY ASSESSMENT - K61-0168 19
3. MECHANICAL PASSIVE ITEM LIST 22
4. MECHANICAL FMEA 23
5. ELECTRICAL FMEA 30
6. HAZARD ANALYSIS WORKSHEETS 72
7. INTERFACING SYSTEM LOSS ASSESSMENT 78
8. CRITICALITY CATEGORY 1R ITEMS SUMMARY 83

1.0 SUMMARY OF FINDINGS AND RECOMMENDATIONS

1.1 CRITICALITY ASSESSMENT SUMMARY

The 90-Ton RSS Pad-B Hoist is assessed as critical. Failure of the system to support a payload canister could cause loss of life and/or loss (damage) of a vehicle system. See section 4.0 on page 17 for additional information.

1.2 MECHANICAL FMEA SUMMARY

There were no mechanical Critical Items identified in the critical functions assessed in section 4.0. See section 5.1 on page 21 for additional information.

1.3 ELECTRICAL FMEA SUMMARY

There were no electrical Critical Items identified in the critical functions assessed in section 4.0 for this system. See section 5.2 on page 25 for additional information.

1.4 FLEXHOSE FMEA SUMMARY

There are no flexhoses associated with the critical functions assessed in section 4.0 for this system.

1.5 ORIFICE FMEA SUMMARY

There are no orifices associated with the critical functions assessed in section 4.0 for this system.

1.6 FILTER FMEA SUMMARY

There are no filters associated with the critical functions assessed in section 4.0 for this system.

1.7 HAZARD ANALYSIS SUMMARY

There was one controlled and one accepted risk hazard identified during this analysis which are summarized below. Additional information is contained in section 7.0.

Hazards Identified

Hazard No.	Hazard Description	Hazard Class.
SPC-5210-018-89	Abnormal rope spooling	Controlled
RT-ENG-1019	Personnel required to perform work while beneath a suspended load	Accepted Risk

1.8 LPS CONTROL/MONITOR FUNCTIONS REVIEW SUMMARY

There are no LPS control/monitor functions associated with this system.

1.9 SNEAK CIRCUIT ANALYSIS SUMMARY

There was no Sneak Circuit Analysis performed on this system. See section 10.0 on page 80 for additional information.

1.10 RECOMMENDATIONS

This system has been designed in accordance with NSTS 07700 Vol. X and meets the GSE "fail safe" requirement of paragraph 3.5.1.2.1.1. No changes are required or recommended for this system.

1.11 AREAS OF CONCERN SUMMARY

There were no Areas of Concern identified with this system.

1.12 CRITICALITY CATEGORY 1R ITEMS SUMMARY

There were two criticality category 1R items identified in the critical functions assessed in section 4.0 for this system. See section 13.0 on page 80 for additional information.

2.0 SYSTEM BASELINE/GROUND RULES/DEFINITIONS/DOCUMENTATION

2.1 SYSTEM BASELINE

This system is baselined for STS by 79K09579, "KSC Facilities, Systems, and Equipment Organizational Level OMD Baseline," dated 9/1/93. The OMD Baseline Number is 422.00.

2.2 GROUND RULES

This analysis has been developed in accordance with NSTS 22206, Rev. C, "Requirements for Preparation and Approval of Failure Modes and Effects Analysis (FMEA) and Critical Items List (CIL)."

2.3 DEFINITIONS OF CRITICALITY AND HAZARD CATEGORIES

The following criticality and hazard categories were used throughout this analysis.

2.3.1 Criticality Definitions and Categories. Criticality definitions and categories are defined as follows:

Category	Definitions
1	Single failure which could result in loss of life or vehicle.
1R	Two hardware items, which if failed, could result in loss of life or vehicle.
1S	Single failure in a safety or hazard monitoring system that could cause the system to fail to detect, combat, or operate when needed during the existence of a hazardous condition and could result in loss of life or vehicle.

Category	Definitions
2	Single failure that could result in loss (damage) of a vehicle system.
3	All others.

Cause - Major reason or event that produces a failure mode.

Component - A combination of parts, devices, and structures, usually self contained, which perform a distinctive function in the operation of the overall equipment. A "black box" (e.g., transmitter, power supply, cryogenic pump, filter assembly).

Correcting Action - An identification of actions, automatic or manual, which could be taken to mitigate the effect of failure.

Critical System - Ground Support Equipment/Facility Systems (GSE) is assessed as critical if loss of overall system function or improper performance of a system function could result in the loss of life, loss of vehicle, or loss (damage) of a vehicle system.

Critical Item - A critical item is defined as a Criticality Category 1, 1S, or 2 Single Failure Point or a redundant hardware item where the second failure results in loss of life or vehicle and the item is not capable of checkout prior to use.

Criticality Assessment - An analysis of each system function to determine if loss or improper performance of the function could result in loss of life, vehicle, and/or loss (damage) of a vehicle system without regard to redundancy.

Fail Safe - The ability to sustain a failure without causing loss of life/vehicle or damage to a vehicle system. (Includes the capability to safe the systems and successfully terminate operations).

Failure - The inability of a system, subsystem, component, or part to perform its required function within specified limits, under specified conditions for a specified duration.

Failure Mode - A description of the manner in which an item can fail.

Function - The activity or operation that a part, component, or system must perform to accomplish its intended purpose.

Interface - The point or area where a relationship exists between two or more parts, systems, programs, persons, or procedures wherein physical and/or functional compatibility is required.

Like Redundancy - Identical hardware items performing the same function.

Redundancy Screens - The following screens will be evaluated for all identified criticality category 1R items.

Screen A - The redundant item is capable of being checked and verified prior to use.

Screen B - Loss of the redundant item is readily detectable by the ground crew. (This screen is not applicable to standby redundancy.)

Screen C - Loss of all redundant items cannot result from a single credible cause, such as contamination.

Line Replaceable Unit (LRU) - An item whose replacement constitutes the optimum organizational maintenance repair action for a higher indenture item, i.e., any assembly which can be removed and replaced as a unit from the system at the operating location.

Loss (Damage) of Vehicle System - Loss of the capability to provide the level of system performance required for normal or emergency operations.

Operational Redundancy - Redundant elements, all of which are fully energized during the subsystem operating cycle. Operational redundancy includes load sharing redundancy wherein redundant elements are connected in such a manner that, upon failure of one unit, the remaining redundant elements will continue to perform the subsystem function. Switching out the failed element is not required.

Passive Component - A component that may be necessary to the performance or structural integrity of the system but has no active function.

Prerequisite Control Logic - GSE software program logic that assures proper sequence of commands.

Reactive Control Logic - GSE software program logic that assures automatic reaction to indicated failures.

Safety or Hazard Monitoring System - A system whose function is to detect, combat, or operate when needed during a hazardous condition which has occurred because of prior failures or events.

Standby Redundancy - Redundant hardware items that are nonoperative until they are switched into the subsystem upon failure of the primary items. Switching can be accomplished by either automatic or manual means.

Unlike Redundancy - Non-identical items performing the same function.

2.3.2 Hazard Definitions and Categories. Hazard definitions and categories are defined as follows:

Hazard - The presence of a potential risk situation caused by an unsafe act or condition.

Hazard Analysis - The determination of potential sources of danger and recommended resolutions in a timely manner for those conditions found in either the hardware/software systems, the person-machine relationship, or both, which cause loss of personnel capability, loss of system, or loss of life or injury to the public.

Hazard Report Closure Classification.

a. Eliminated Hazard - A hazard that has been eliminated by removing the hazard source or by deleting the hazardous operations.

b. Controlled Hazard - The likelihood of occurrence has been reduced to an acceptable level by implementing the appropriate hazard reduction precedence sequence to comply with program requirements.

c. Accepted Risk - Hazard which has not been counteracted by redundancy purge provisions, appropriate safety factors, containment/isolation provision, backup system/operation, safety devices, alarm/caution and warning devices, or special automatic/manual procedures. Catastrophic hazards, critical hazards, hazards resulting from failure to meet program requirements, and Single Failure Points (SFPs) in emergency systems will be documented. A hazard will be classified as an "accepted risk" only after (1) all reasonable risk avoidance measures have been identified, studied, and documented; (2) project/program management has made a decision to accept the risk on the basis of documented risk acceptance rationale; and (3) Safety management has concurred in the accepted risk rationale.

Severity Level - Should the hazard occur, its worst case severity would be:

a. Catastrophic - Hazard could result in a mishap causing fatal injury to personnel, and/or loss of one or more major elements of the flight vehicle or ground facility.

b. Critical - Hazard could result in serious injury to personnel, and/or damage to flight or ground equipment which would cause mission abort or a significant program delay (one or more days).

c. Marginal - Hazard could result in a mishap of minor nature inflicting first-aid injury to personnel, and/or damage to flight or ground equipment which can be tolerated without abort or repaired without significant program delay (less than one day).

Hazard Report Status.

a. Closed - Corrective action to eliminate or control the hazard is completed, evaluated, and verified and management actions to accept the safety risks are completed. Actions taken, organization which performed actions and completion dates are to be documented in this data element.

b. Open - Corrective action evaluation and verification is in progress. The status shall remain open until management has reviewed the actions taken and accepted the safety risk. Actions required, organization responsible for performing the actions and due dates are to be documented in this data element.

2.4 DOCUMENTATION LIST

The following documents were used in completing this analysis:

Table 1 (Page 1 of 2). **SYSTEM DOCUMENTATION LIST**

Document/Drawing No.	Rev.	Outstanding EO Numbers	Title
NSTS 22206	C	-	Requirements for Preparation and Approval of Failure Modes and Effects Analysis (FMEA) and Critical Items List (CIL)
NSTS 22254	A	-	Methodology For Conduct Of NSTS Hazard Analyses
NSS/GO-1740.9B	-	-	NASA Safety Standard for Lifting Devices and Equipment
GP1098G	-	-	KSC Ground Operations Safety Plan
79K24954	Basic	1	LC39B Payload Canister 90-Ton Hoist
79K29056	Basic	None	LC39B RCS Room/RSS 90-Ton Hoist Mechanical Arrangement
79K40112	A	3-6	Operational Drawing LC 39 Pad B Rotating Service Structure
79K24955	Basic	None	Launch Complex 39B Payload Canister 90-Ton Hoist
EA-1813	C	None	Electrical Schematic Diagram (Ederer, Inc.)
EA-1814	A	None	Electrical Conduit Layout 90-Ton Fixed Hoist (Ederer, Inc.)
EA-1815	B	None	Electrical Interconnection Diagram (Ederer, Inc.)
EA-1844	B	None	A.C. Motor Hoist Panel Wiring Diagram (Ederer, Inc.)
EA-2123	A	None	Delay Set Module Assy. Drawing (Ederer, Inc.)
B-16497	Basic	None	4-F-375 Reducer Assy. (Ederer, Inc.)
A-13147	Basic	None	Hoist Assembly 90-Ton Capacity (Ederer, Inc.)
A-13106	A	None	Hoist Equipment General Arrangement 90-Ton Fixed Hoist (Ederer, Inc.)
A-13150	A	None	Band Brake Assy. 35" Brake Drum (Ederer, Inc.)

Table 1 (Page 2 of 2). **SYSTEM DOCUMENTATION LIST**

Document/Drawing No.	Rev.	Outstanding EO Numbers	Title
SAA09ELB2-001	A	None	System Assurance Analysis for the 60 Hertz Power Distribution System Pad B
OMI Q3437	C	-	Operating Instructions for the 90-Ton Hoist, Rotating Service Structure
OMI Q6325	A-1	-	Maintenance Instructions for the 90-Ton Payload Canister Hoist, Pad B
OMI M3160	C-3	-	Payload Canister Hoisting Operations, Launch Pads A and B
OMI E5026	A	-	Orbiter Payload Canister Handling - LC-39 Pads A or B

3.0 SYSTEM DESCRIPTION

The Pad B 90-Ton Hoist was manufactured by Ederer Incorporated of Seattle, Washington. The Hoist System includes electrical wiring, controls, remote control station, motor brakes, gear train, single drum with dual reeving, lebus grooving, blocks, hook and welded base. It is located in the Hoist Equipment Room on the roof of the Pad-B PCR. The hoist is used to handle Payload Canisters to install vertical payloads in the PCR.

The wire ropes (2 ropes) are fed through sheave assemblies in the RCS room and to the load block and equalizer bar. Twelve part double reeving is used. There is sufficient length of wire rope for the load block to reach the pad surface with at least two full wraps remaining on the wire rope drum. (See figures 1 and 2)

The hoist consists of an electric drive motor with attached solenoid disc brake (motor brake), which acts as a control brake during deceleration. There is another solenoid disc brake mounted on the input shaft of the gear reducer which acts as a holding brake. The reducer brake actuation is delayed via time delay device to prevent excessive deceleration of loads. The output shaft of the gear reducer is continuous thru the drum assembly and is keyed to it. An overspeed sensor and up/down geared limit switch are coupled axially to the hoist drum shaft. Both limit switches have back out capability. An additional final upper limit switch terminates power to the hoist and does not have back out capability. (See figures 2 and 3)

The hoist is operated by an AC motor acting through a gear reducer to the hoist drum. The AC motor is a dual speed type rated at 100 HP/1800 RPM and 25 HP/450 RPM producing hook (load block) speeds of 10.6 fpm and 2.6 fpm. The application of power to the drive motor energizes the motor brake solenoid and the reducer brake solenoid, causing the brakes to release and enabling vertical motion of the hoist. These brakes are the self adjusting disc type and are normally kept engaged by spring compression. Electric power to each brake

solenoid is sufficient to overcome the spring and cause the brake to release. (See figures 2 and 3)

There is also a spring actuated band brake on the hoist drum activated by an overspeed sensor and switch located on the hoist drum shaft. When the drum rotates at 120% of maximum rated drum speed for any reason, the overspeed sensor detects the increased RPM and causes the sensor switch to close. The switch de-energizes the band brake solenoid valve and energizes the band brake relay. The solenoid valve releases hydraulic fluid from a hydraulic cylinder which allows the spring loaded actuator to tighten (set) the band brake. The band brake relay activates the shunt trip circuit breaker terminating power to the hoist motors and prevents reset of the solenoid valve once the overspeed switch opens when the drum stops. The band brake relay is de-energized by a reset button located on the hoist main control panel. The band brake must be released manually by a hydraulic hand pump connected to the hydraulic cylinder which compresses the spring loaded actuator. (See figures 1, 2, and 3)

A strain gauge type load cell is installed in the pin of the equalizer bar. It is calibrated to activate the overload cutout and stop the hoist if the load on the hook exceeds 125% of the rated load. (See figure 2)

A power monitor is installed to prevent hoist operation if irregularities with 60 Hz power are present, such as low voltage or reverse phasing.

3.1.1 ANALYSIS OF WIRE ROPE DRUM, GEARBOX SHAFT, AND GEAR RETENTION METHODS. As a point of special concern for the safety of sensitive loads, the design integrity of hoist gearboxes was carefully reviewed for failure modes that, if they should occur, could cause or contribute to dropping a load. The particular failure modes under scrutiny are:

The ability of a gear to slip out-of-mesh with its associated gear or structural failure of a gear possibly caused by:

a. The gear itself slipping axially along the shaft, or

b. The shaft with gear firmly fixed thereon slipping axially out-of-alignment.

c. Broken gear teeth or complete destruction of a gear.

The effect of such a failure occurrence followed by a subsequent failure of the drum band brake would result in the load (payload canister) being dropped possibly causing damage to the load and/or loss of life. Such failure negates the additional redundancy of the motor and reducer brakes to the drum band brake.

The hoist gearbox consists of six helical gears. They are the high speed pinion, the high speed gear, the intermediate pinion, the intermediate gear, the low speed pinion, and the low speed gear. Motor and motor brake torque are transmitted to the input shaft of the gear reducer through a coupling keyed to the shaft. The reducer brake is keyed to the opposite end of the input shaft. The low speed pinion is integrally machined on the input shaft.

The low speed pinion meshes with the low speed gear which is keyed to the first idler shaft. The intermediate pinion is integrally machined on the first idler shaft. It meshes with the intermediate gear which is keyed to the second idler shaft. The low speed pinion is integrally

machined on the second idler shaft. It meshes with the low speed gear which is keyed to the output shaft. The gearbox output shaft is keyed to the hoist drum.

Axial slippage of gears and shafts are prevented by shoulders and the overlap of the gears themselves within the confined space of the gearbox. The cone bearings are supported by cups within the gearbox case structure and are retained in place by snap rings. There is insufficient space within the gear case to allow gears to slip out of mesh with each other or a shaft to pull free from a bearing.

The hoist drum is mounted such that bearing failure will not cause the load to drop. The drum is supported on one end by the gearbox output shaft and its associated cone bearings. The opposite end is supported by the drum bearing assembly such that the bearing and bearing retainers are loaded in compression when the hoist is in use.

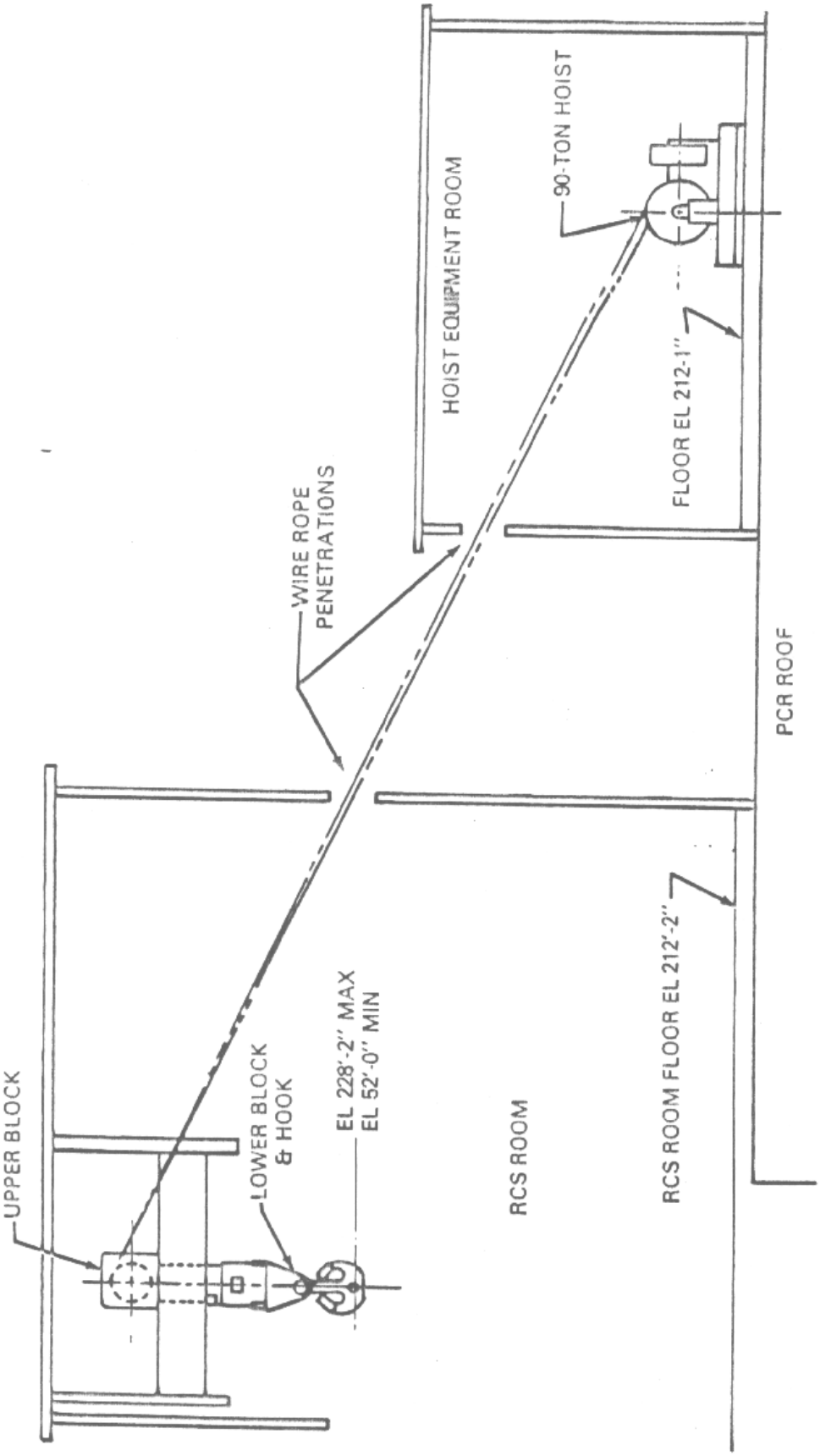


FIGURE 1. PAD-B 90-TON PAYLOAD HOIST

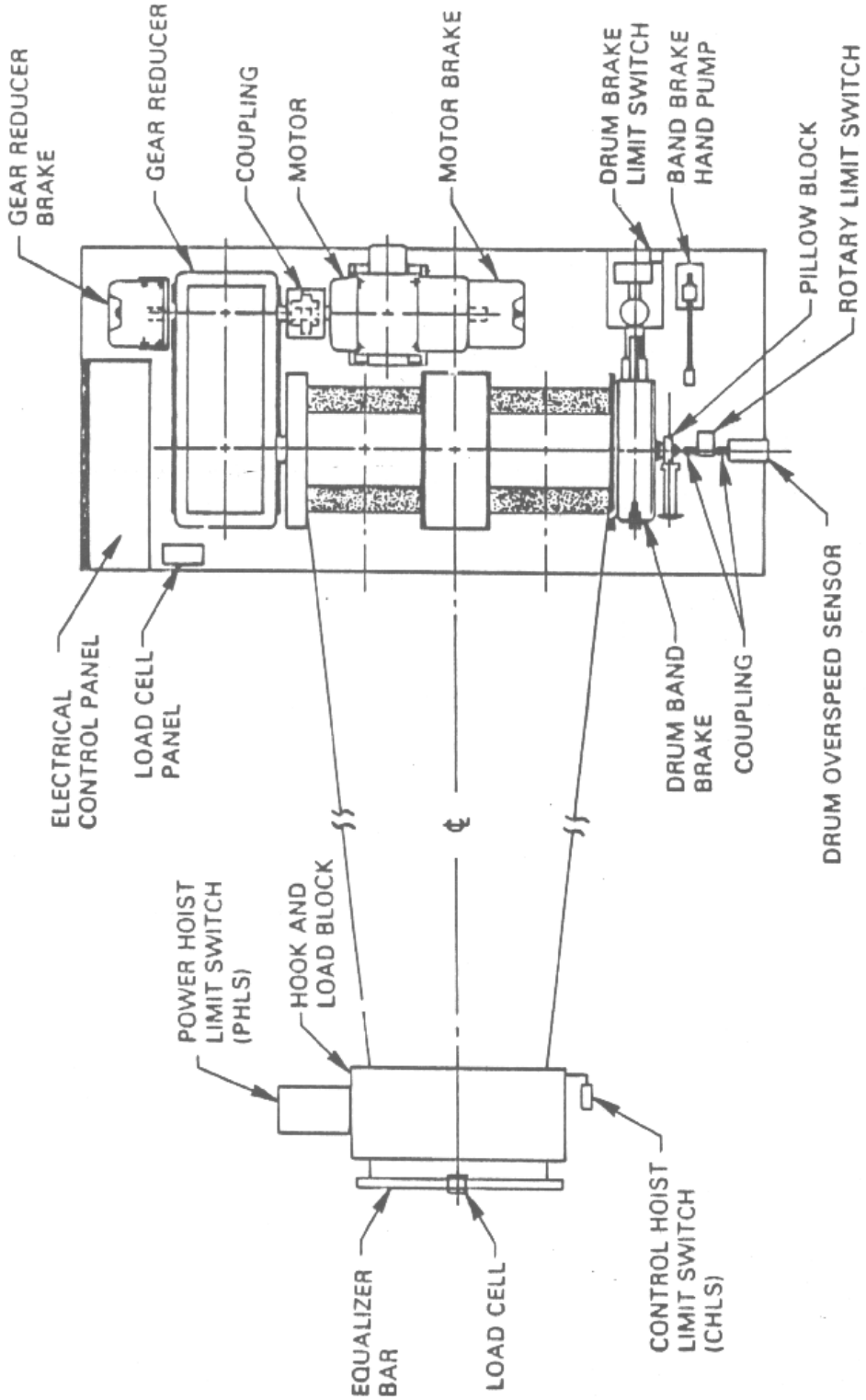


FIGURE 2. PAD-B 90-TON PAYLOAD HOIST, MECHANICAL ARRANGEMENT

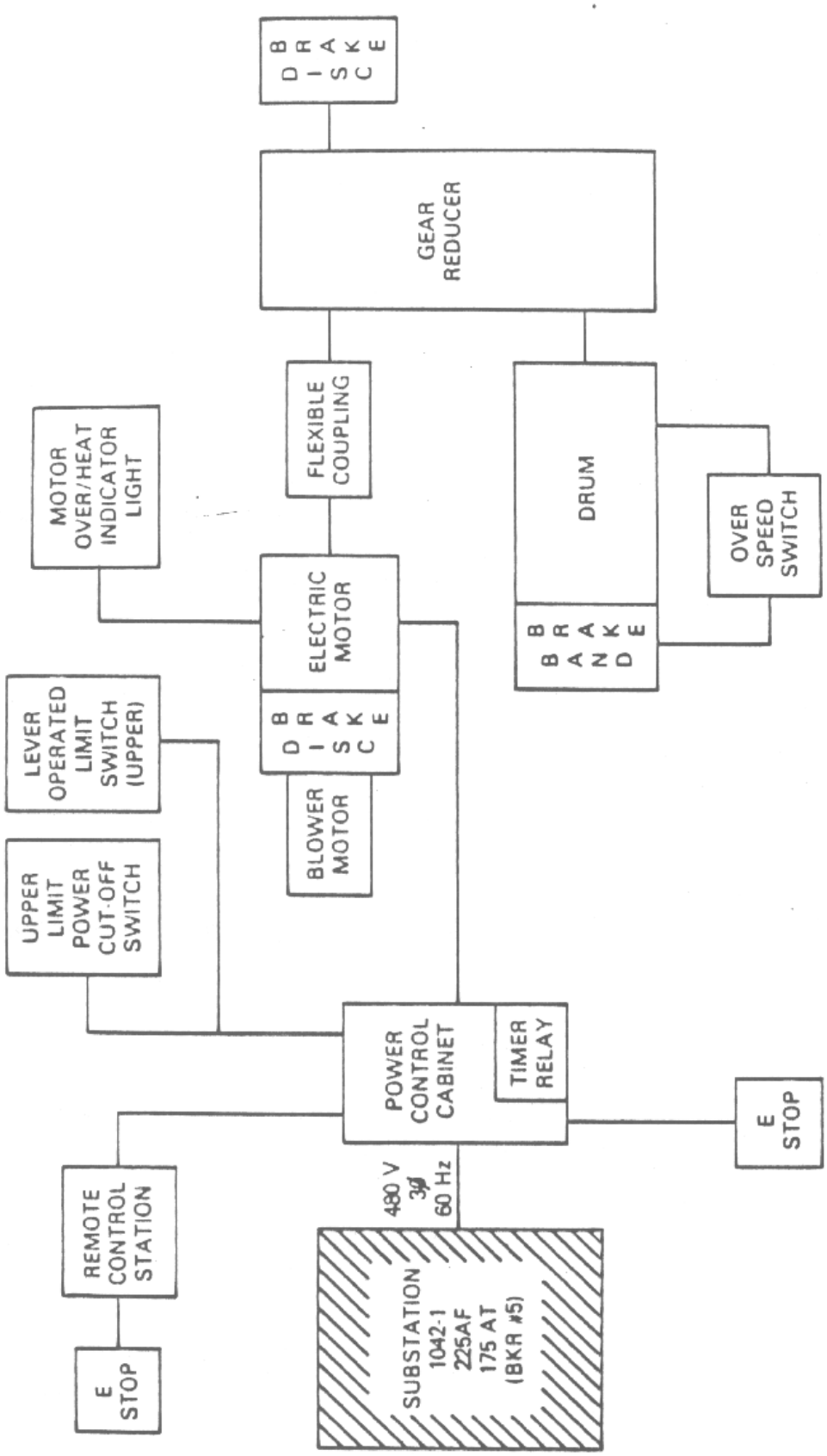


FIGURE 3. PAD-B 90-TON PAYLOAD HOIST, BLOCK DIAGRAM

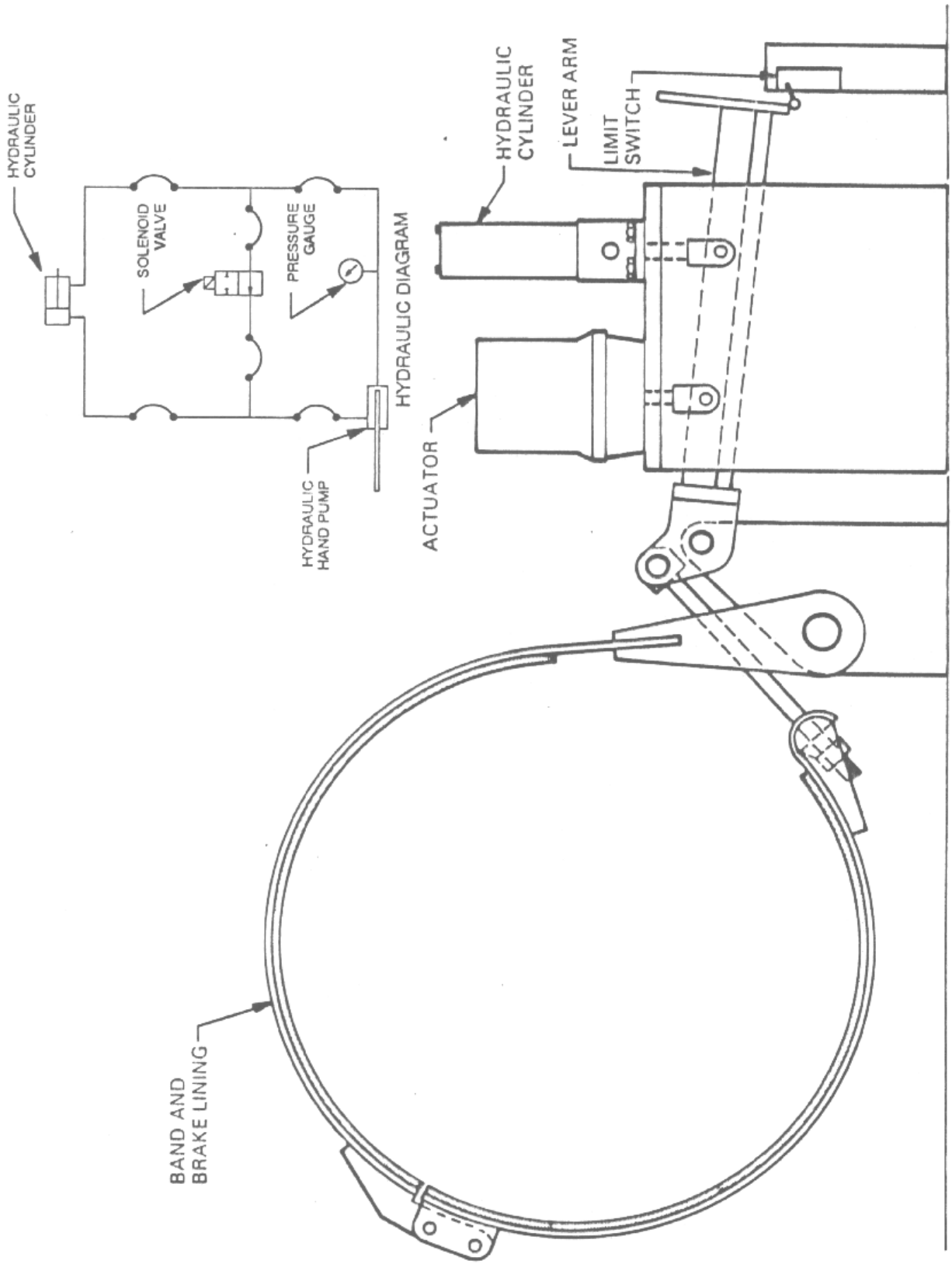


FIGURE 4. PAD-B 90-TON PAYLOAD HOIST, BAND BRAKE ASSEMBLY

4.0 CRITICALITY ASSESSMENT

The system functions are identified in Figure 5 on page 18 and assessed on the following Criticality Assessment Sheets (Worksheet 5312-001).

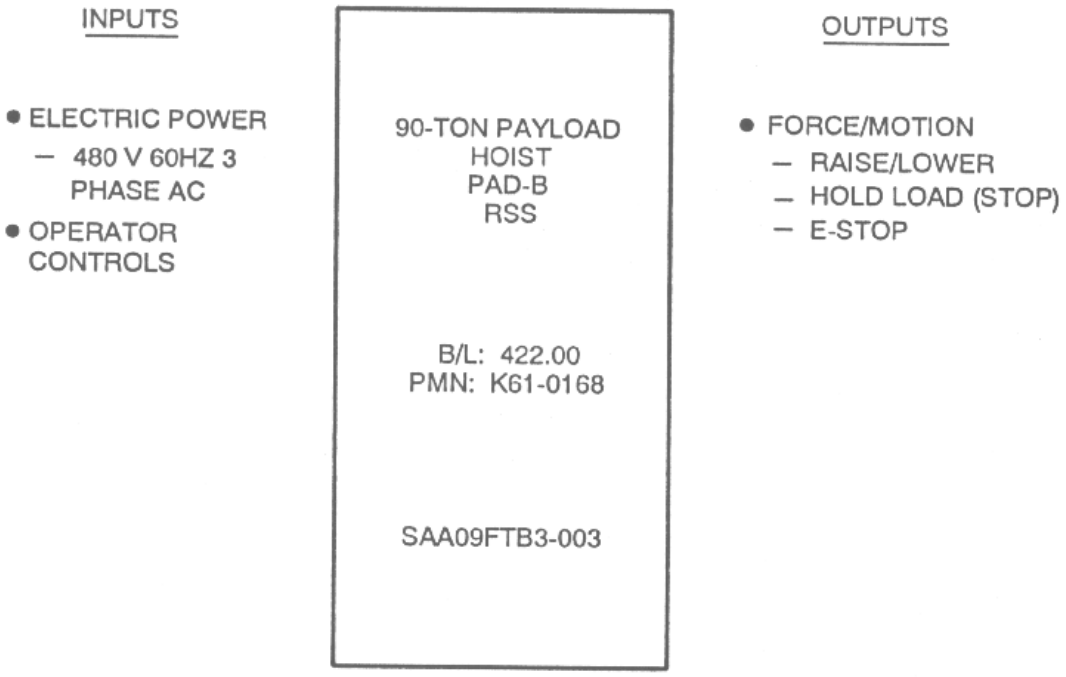


FIGURE 5. SYSTEM FUNCTIONAL BLOCK DIAGRAM

Table 2 (Page 1 of 2). **CRITICALITY ASSESSMENT - K61-0168**

Program Model Number K61-0168 **Baseline Number** 422.00	**System/Subsystem** 90-TON HOIST **Location** PAD-B RSS	**Station Set/Facility Code** RW **Date** DECEMBER 1993 **Prepared By** B. KALLE, LSOC 52-11

INPUT/OUTPUT	FUNCTION	TIME PERIOD	EFFECT OF LOSS/FAILURE IF: a. FAILS TO OPERATE ON TIME b. FAILS TO CEASE OPERATION ON TIME c. FAILS DURING OPERATION d. PREMATURELY OPERATES	CRIT/ NONCRIT	NOTES
INPUT					
• ELECTRIC POWER					
- 480V 60 HZ 3 PHASE AC	PRIMARY POWER SOURCE	AS NEEDED.	a. NA b. NO EFFECT c. HOIST WILL CEASE TO FUNCTION, ALL THREE BRAKES WILL SET HOLDING LOAD. d. NA	a. NA b. NC c. NC d. NA	
•OPERATOR CON-TROLS	OPERATES HOIST	AS NEEDED	a. NA b. INABILITY TO STOP NORMAL OR ABNORMAL HOIST MOTION. COULD CAUSE POSSIBLE LOSS OF LIFE FROM RELEASE OF TOXIC MATERIALS AND/OR FIRE/EXPLOSION OF PROPELLANTS AND/OR LOSS (DAMAGE) TO A PAYLOAD. c. NA d. NA	a. NA b. C c. NA d. NA	a. NONE b. OPERATOR ERROR REQUIRED. SEE HAZARD ANALYSIS. c. NONE d. NONE
OUTPUT					
•FORCE/MOTION					
- RAISE/LOWER	RAISE/LOWER PAYLOAD CANISTER BETWEEN PAD AND PCR.	AS NEEDED	a. NO EFFECT. DELAY OF OPERATION. b. LOAD COULD DROP AND COULD CAUSE POSSIBLE LOSS OF LIFE FROM RELEASE OF TOXIC MATERIALS, AND/OR FIRE/EXPLOSION OF PROPELLANTS. c. TERMINATION OF LIFTING OPERATION. d. NA	a. NC b. C c. NC d. NA	a. NONE. b. SEE FMEA. c. NONE. d. NONE.
- HOLD LOAD (STOP)	SUPPORT PAYLOAD CANISTER IN FIXED POSITION WHEN NOT ATTACHED BY CANISTER SUSPEN-SION CABLES.	AS NEEDED	a. LOAD COULD DROP AND COULD CAUSE POSSIBLE LOSS OF LIFE FROM RELEASE OF TOXIC MATERIALS, AND/OR FIRE/EXPLOSION OF PROPELLANTS. b. TERMINATION OF LIFTING OPERATION. c. LOAD COULD DROP AND COULD CAUSE POSSIBLE LOSS OF LIFE FROM RELEASE OF TOXIC MATERIALS, AND/OR FIRE/EXPLOSION OF PROPELLANTS. d. TERMINATION OF LIFTING OPERATION.	a. C b. NC c. C d. NC	a. SEE FMEA. b. NONE. c. SEE FMEA. d. NONE.

Table 2 (Page 2 of 2). **CRITICALITY ASSESSMENT - K61-0168**

Program Model Number K61-0168 **Baseline Number** 422.00		**System/Subsystem** 90-TON HOIST **Location** PAD-B RSS		**Station Set/Facility Code** RW **Date** DECEMBER 1993 **Prepared By** B. KALLE, LSOC 52-11	
INPUT/OUTPUT	**FUNCTION**	**TIME PERIOD**	**EFFECT OF LOSS/FAILURE IF:** **a. FAILS TO OPERATE ON TIME** **b. FAILS TO CEASE OPERATION ON TIME** **c. FAILS DURING OPERATION** **d. PREMATURELY OPERATES**	**CRIT/ NONCRIT**	**NOTES**
- E-STOP	PROVIDE ADDITIONAL STOP CAPABILITY	AS NEEDED	a. LOAD COULD DROP AND COULD CAUSE POSSIBLE LOSS OF LIFE FROM RELEASE OF TOXIC MATERIALS, AND/OR FIRE/EXPLOSION OF PROPELLANTS. b. TERMINATION OF LIFTING OPERATION. c. LOAD COULD DROP AND COULD CAUSE POSSIBLE LOSS OF LIFE FROM RELEASE OF TOXIC MATERIALS, AND/OR FIRE/EXPLOSION OF PROPELLANTS. d. TERMINATION OF LIFTING OPERATION.	a. C b. NC c. C d. NC	a. SEE FMEA. b. NONE. c. SEE FMEA. d. NONE.

5.0 FAILURE MODES AND EFFECTS ANALYSIS (FMEA)

5.1 MECHANICAL FMEA

The mechanical components of the critical functions assessed in section 4.0 for this system were identified from the documents and diagrams referenced in Table 1 on page 9 and are depicted on the following figure(s) and analyzed in the associated Mechanical FMEA (Worksheet 5312-003). A passive items list precedes the Mechanical FMEA and is shown in Table 3 on page 22.

MECHANICAL FAILURE MODES AND EFFECTS ANALYSIS

FOR THE

90-TON PAYLOAD HOIST

PMN K61-0168

The following components were considered passive in the analysis for this system.

Table 3. **MECHANICAL PASSIVE ITEM LIST**

Find Number	Nomenclature
17	HOOK
17	LOWER BLOCK
16	UPPER BLOCK
19, 20	WIRE ROPES
3	ROPE DRUM
2	DRUM SHAFT
4	PILLOW BLOCK

Table 4 (Page 1 of 2). **MECHANICAL FMEA**

System 90-TON HOIST RSS
Subsystem MECHANICAL
Drawing No. 79K29056 **Sheet No.** 1
PMN K61-0168

Program SPACE SHUTTLE

Station Set/Facility Code RW
Date DECEMBER 1993
Reference Figure Used
Prepared By B. KALLE, LSOC 52-11

FIND NO. PART NO.	PART NAME	PART FUNCTION	a. FAILURE MODE b. CAUSE c. FMN d. DETECTION METHOD e. CORRECTING ACTION f. TIME TO EFFECT g. TIMEFRAME	FAILURE EFFECT ON SYSTEM PERFORMANCE	FAILURE EFFECT ON VEHICLE SYSTEMS AND/OR PERSONNEL SAFETY	CRIT CAT
1 B16497	GEAR REDUCER 86.9:1	REDUCES MOTOR OUTPUT SPEED. PROVIDES MECHANICAL LINKAGE BETWEEN, AND MULTIPLIES EFFECTIVE TORQUE OF MOTOR, MOTOR BRAKE, AND REDUCER BRAKE APPLIED TO THE WIRE ROPE DRUM.	a. GEAR DISENGAGEMENT b. STRUCTURAL FAILURE c. 09FTB3-003.001 d. ABNORMAL HOIST MOTION e. DRUM BAND BRAKE SET AUTOMATICALLY f. SECONDS g. SECONDS	NOISY AND/OR JERKY OPERATION TO DROPPING OF LOAD DEPENDING ON SEVERITY OF FAILURE. OVERSPEED SENSOR WILL AUTOMATICALLY SET DRUM BAND BRAKE AND STOP LOAD IN APPROXIMATELY 4 INCHES.	SUBSEQUENT FAILURE OF THE DRUM BAND BRAKE TO SET COULD RESULT IN A DROPPED PAYLOAD CONTAINING SOLID PROPELLANT HYPERGOLS. POSSIBLE LOSS OF LIFE AND/OR PAYLOAD.	1R
8 F-103	MOTOR COUPLING	COUPLES MOTOR OUTPUT TO SPEED REDUCER INPUT SHAFT.	a. STRUCTURAL FAILURE	IF THE COUPLING BREAKS WHILE IN USE, THE HOIST WILL FREE-WHEEL ALLOWING THE LOAD TO DESCEND. THE LOAD CAN BE STOPPED BY RELEASING THE HOIST UP OR DOWN SWITCH (WHICHEVER IS IN USE) THUS SETTING THE BRAKES, OR AUTOMATICALLY BY THE OVERSPEED SENSOR WHICH WILL SET THE DRUM BAND BRAKE.	NO EFFECT.	3
18 1-082-051-02	DISC BRAKE (SPEED REDUCER)	SPRING SET, MAGNETICALLY RELEASED DISC BRAKE	a. FAILS TO SET	DRUM WILL NOT BE STOPPED OR HELD BY ELECTRIC DISC BRAKE. MOTOR BRAKE AND BAND BRAKE WILL STOP AND HOLD LOAD.	NO EFFECT.	3
			a. FAILS TO RELEASE	HOIST IS INOPERATIVE.	NO EFFECT.	3
12 1-082-051-02	DISC BRAKE (MOTOR)	SPRING SET DISC BRAKE ASSEMBLY	a. FAILS TO SET	BRAKE WILL NOT HOLD LOAD. REDUNDANT DISC AND BAND BRAKES WILL STOP AND HOLD LOAD.	NO EFFECT.	3
			a. FAILS TO RELEASE	HOIST IS INOPERATIVE.	NO EFFECT.	3

Table 4 (Page 2 of 2). **MECHANICAL FMEA**

System 90-TON HOIST RSS
Subsystem MECHANICAL
Drawing No. 79K29056 **Sheet No.** 1
PMN K61-0168

Program SPACE SHUTTLE

Station Set/Facility Code RW
Date DECEMBER 1993
Reference Figure Used
Prepared By B. KALLE, LSOC 52-11

FIND NO. PART NO.	PART NAME	PART FUNCTION	a. FAILURE MODE b. CAUSE c. FMN d. DETECTION METHOD e. CORRECTING ACTION f. TIME TO EFFECT g. TIMEFRAME	FAILURE EFFECT ON SYSTEM PERFORMANCE	FAILURE EFFECT ON VEHICLE SYSTEMS AND/OR PERSONNEL SAFETY	CRIT CAT
9 A-13190	BAND BRAKE ASSEMBLY	BAND BRAKE ASSEMBLY THAT ACTS DIRECTLY UPON DRUM WHEN OVERSPEED IS SENSED.	a. BRAKE SLIPS OR FAILS TO SET b. SOLENOID VALVE FAILS CLOSED, HYDRAULIC CYLINDER FAILS TO ACTUATE, ACTUATOR SPRING FAILURE, OVER-SPEED SWITCH FAILS c. 09FTB3-003.002 d. NONE e. NONE f. SECONDS g. NA	UNABLE TO SET BAND BRAKE. TWO REDUNDANT BRAKE CAN STOP AND HOLD LOAD.	SUBSEQUENT FAILURE OF THE GEAR REDUCER COULD RESULT IN A DROPPED PAYLOAD CONTAINING SOLID PROPELLANT AND HYPERGOLS. POSSIBLE LOSS OF LIFE AND/OR PAYLOAD.	1R
			a. SETS PREMATURELY (FALSE ALARM)	HOIST IS INOPERATIVE.	NO EFFECT.	3

5.2 ELECTRICAL FMEA

The electrical components of the critical functions assessed in section 4.0 for this system were identified from the documents and diagrams referenced in Table 1 on page 9 and are depicted on the following figure(s) and analyzed in the associated Electrical FMEA (Worksheet 5312-005).

ELECTRICAL FAILURE MODES AND EFFECTS ANALYSIS

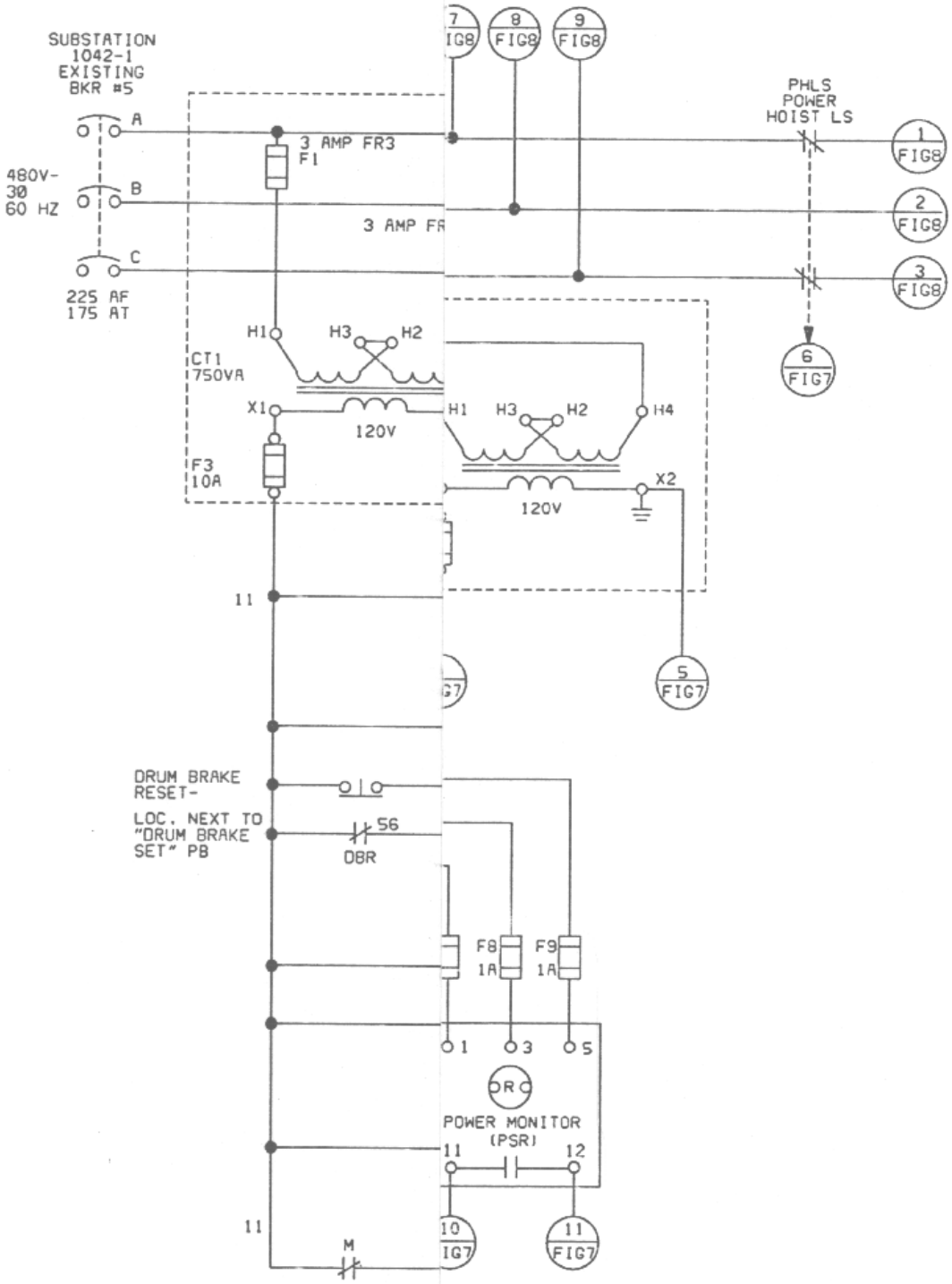
FOR THE

90-TON PAYLOAD HOIST

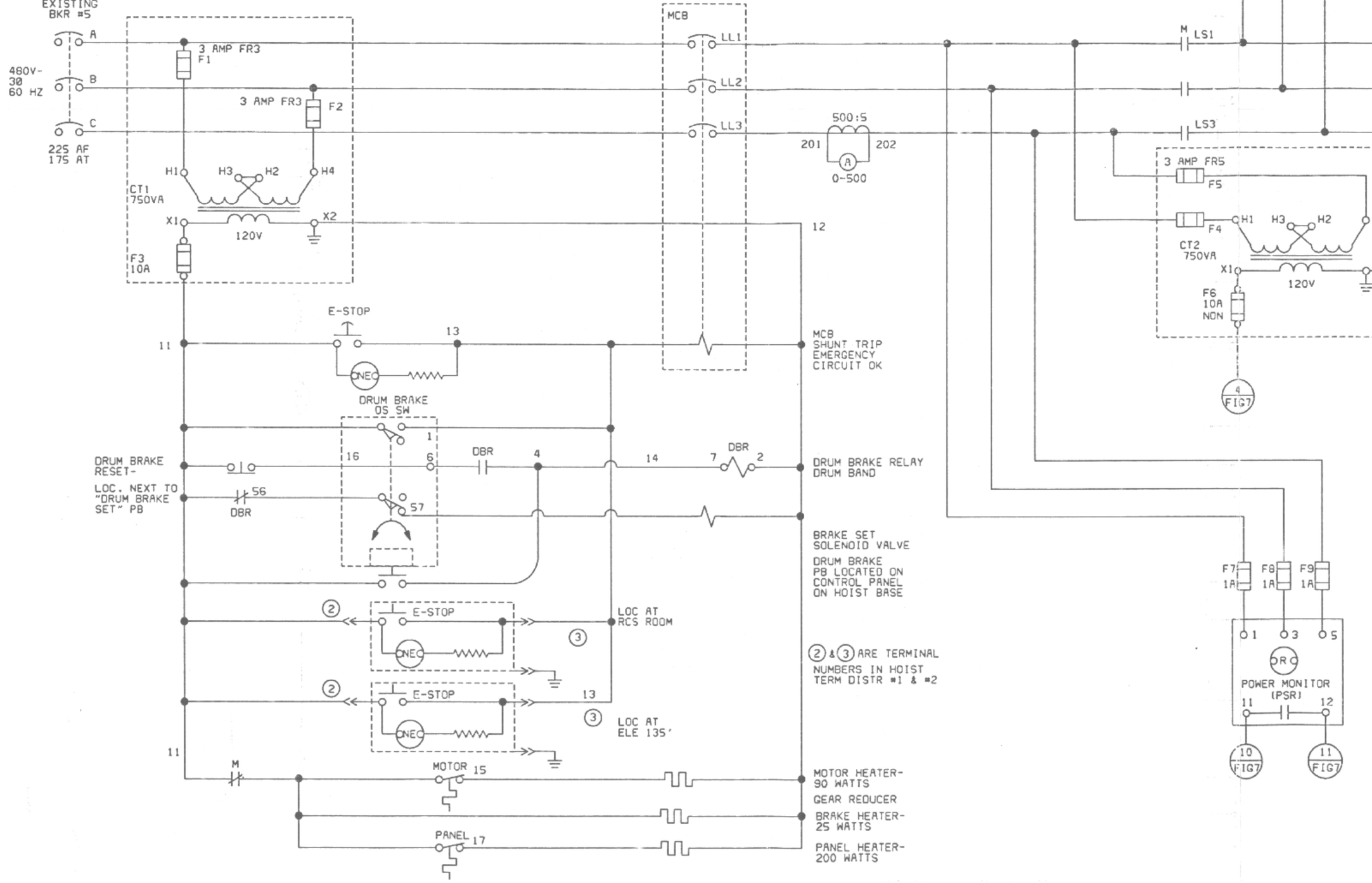
PMN K61-0168

Wire harnesses, cables, or connectors were not analyzed in the Electrical FMEA for this system since a single failure (open or short) could not result in loss of life or vehicle. (Ref. NSTS 22206 section 4.0, paragraph 4.4.1, subparagraph b[2])

SAA09FTB3-003
REV. A



SAA09FTB3003A_S06
LW092893


EXISTING BKR #5
480V-
3Ø
60 HZ
A
B
C
225 AF
175 AT
3 AMP FR3
F1
3 AMP FR3
F2
H1
H3
H2
H4
CT1
750VA
X1
X2
120V
F3
10A
MCB
LL1
LL2
LL3
500:5
201
202
A
0-500
M
LS1
LS3
3 AMP FR5
F5
F4
CT2
750VA
F6
10A
NON
4
FIG7
12
11
13
E-STOP
ONEC
DRUM BRAKE
OS SW
1
16
6
DBR
4
14
7
2
DRUM BRAKE
RESET-
LOC. NEXT TO
"DRUM BRAKE
SET" PB
56
57
MCB
SHUNT TRIP
EMERGENCY
CIRCUIT OK
DRUM BRAKE RELAY
DRUM BAND
BRAKE SET
SOLENOID VALVE
DRUM BRAKE
PB LOCATED ON
CONTROL PANEL
ON HOIST BASE
LOC AT
RCS ROOM
LOC AT
ELE 135'
2 & 3 ARE TERMINAL
NUMBERS IN HOIST
TERM DISTR #1 & #2
F7
1A
F8
1A
F9
1A
1
3
5
OR
POWER MONITOR
(PSR)
11
12
10
FIG7
11
FIG7
MOTOR
15
MOTOR HEATER-
90 WATTS
GEAR REDUCER
BRAKE HEATER-
25 WATTS
PANEL
17
PANEL HEATER-
200 WATTS

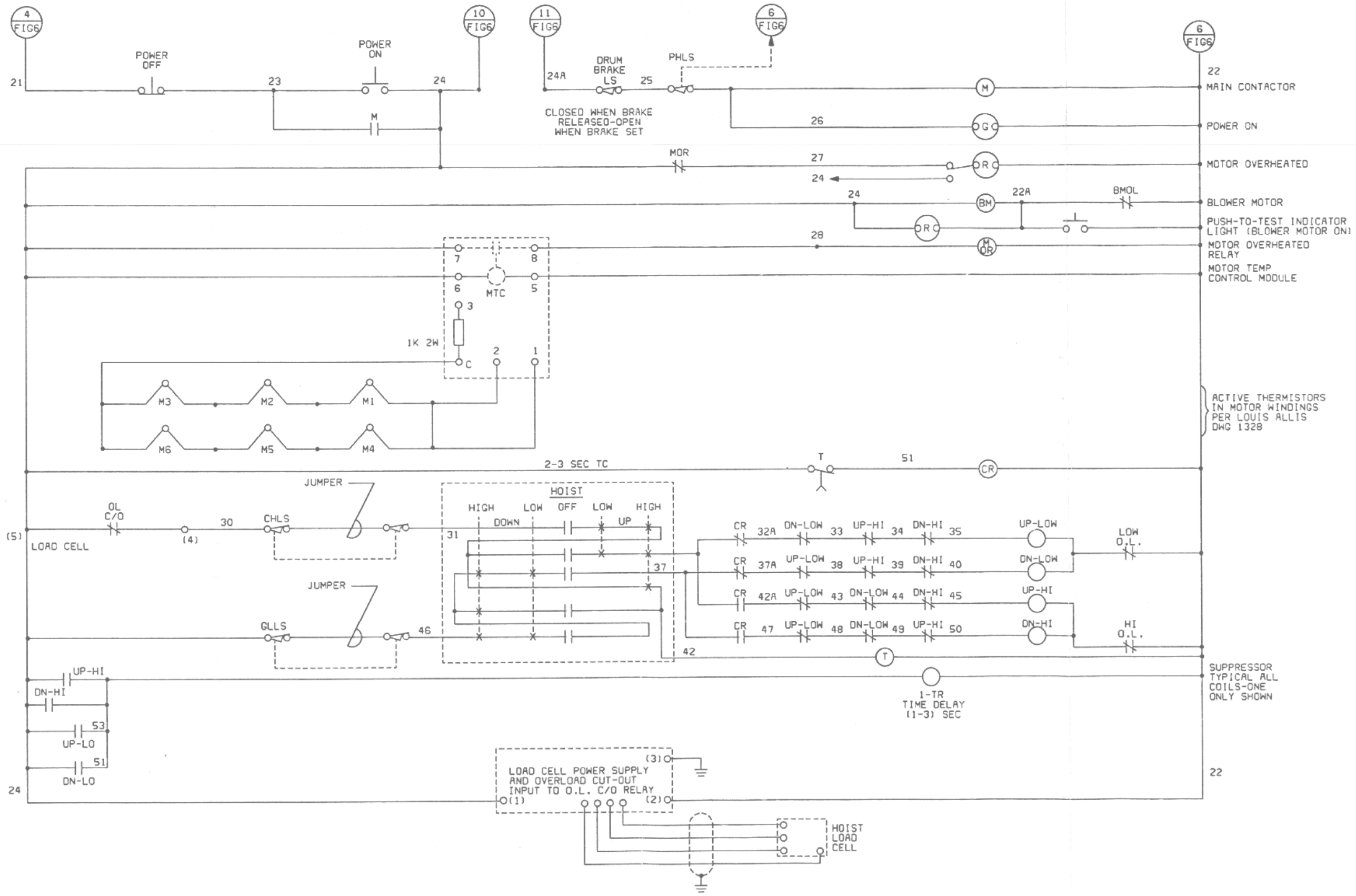


FIGURE 7. 90-TON HOIST PAD-B ELECTRICAL SCHEMATIC (CONTINUED)

SAA09FTB3-003
REV. A

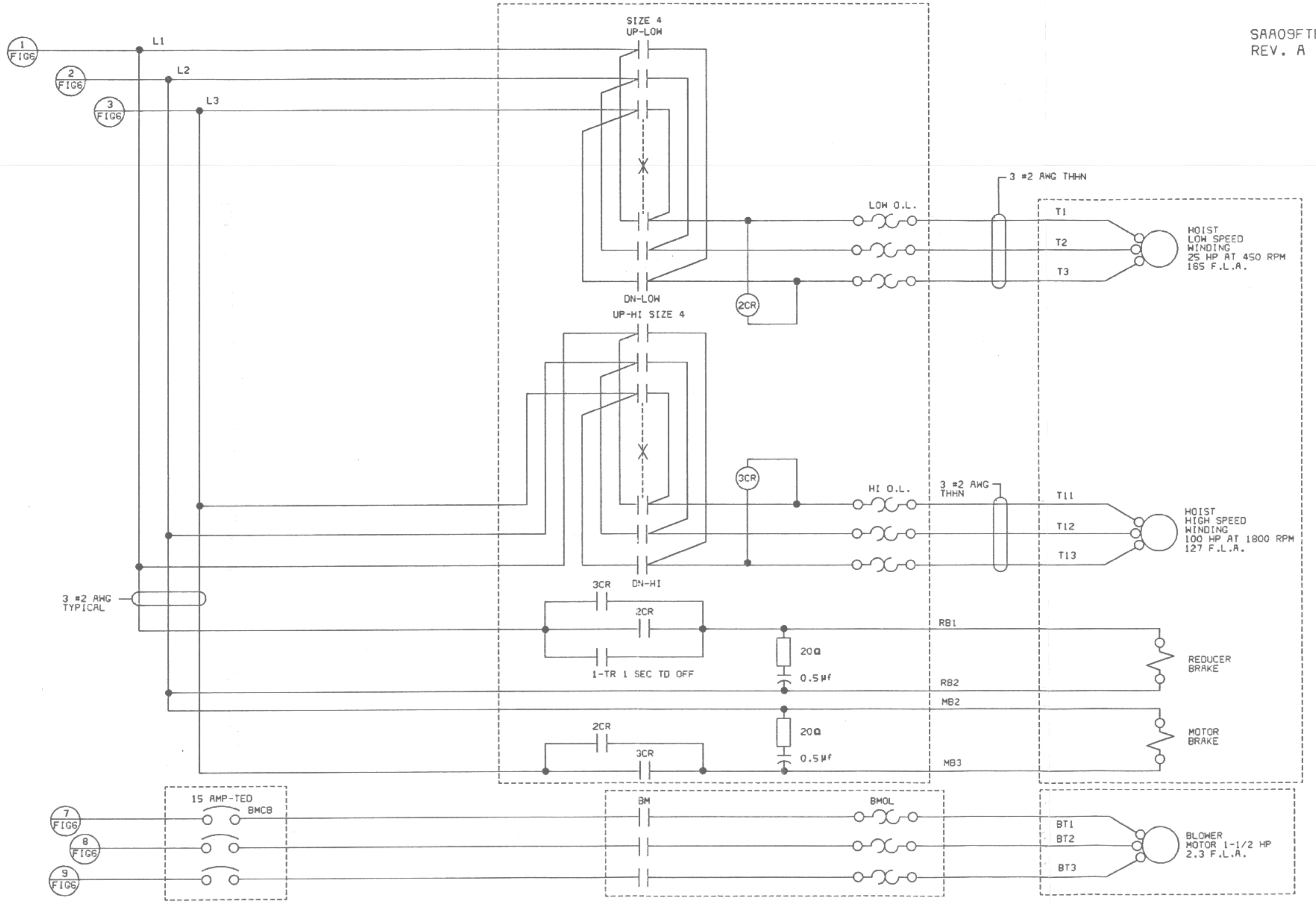


FIGURE 8. 90-TON HOIST PAD B ELECTRICAL SCHEMATIC (CONTINUED)

SAA09FTB3003_S08
LW093093

Table 5 (Page 1 of 17). **ELECTRICAL FMEA**

System 90-TON HOIST RSS
Subsystem ELECTRICAL
Drawing No. 79K40112 **Sheet No.** ALL
PMN K61-0168

Program SPACE SHUTTLE

Station Set/Facility Code RW
Date DECEMBER 1993
Reference Figure Used 6,7,8
Prepared By B. KALLE, LSOC 52-11

FIND NO. PART NO.	PART NAME	PART FUNCTION	a. FAILURE MODE b. CAUSE c. FMN d. DETECTION METHOD e. CORRECTING ACTION f. TIME TO EFFECT g. TIMEFRAME	FAILURE EFFECT ON SYSTEM PERFORMANCE	FAILURE EFFECT ON VEHICLE SYSTEMS AND/OR PERSONNEL SAFETY	CRIT CAT
33 TYPE CB5ND FRAME 445T	ELECTRIC MOTOR	TRANSFORMS ELECTRICAL ENERGY INTO MECHANICAL ENERGY.	a. INOPERATIVE	HOIST IS INOPERATIVE. BOTH MOTOR AND REDUCER BRAKES ARE RELEASED. RETURN OF MASTER SWITCH TO OFF POSITION OR USE OF E-STOP BY OPERATOR OR DRUM OVERSPEED SWITCH WILL PREVENT LOAD FROM DROPPING.	NO EFFECT.	3
	INDICATOR LIGHT (MOTOR OVERHEAT)	LIGHT ILLUMINATES WHEN MOTOR OVERHEATS.	a. FAILS OPEN	HOIST CAN BE OPERATED WITH OVER-HEATED MOTOR AND THE OPERATOR WARNING WILL BE BLOCKED. PRO-LONGED USE COULD DAMAGE MOTOR.	NO EFFECT.	3
MOR 11 NONE	MOTOR OVERHEAT RELAY	LIGHTS OVERHEAT LIGHT WHEN DE-ENERGIZED BY EITHER HIGH OR LOW MOTOR TEMPERATURE CONTROL-LERS.	a. RELAY FAILS TO ACTI-VATE (DE-ENERGIZED)	MOTOR OVERHEAT LIGHT WILL REMAIN ON GIVING FALSE INDI-CATION.	NO EFFECT	3
			a. RELAY FAILS ACTIVATED (ENERGIZED)	MOTOR OVERHEAT LIGHT WILL NOT LIGHT WHEN AN OVERHEAT CONDI-TION IS DETECTED.	NO EFFECT.	3
40 2210-132-CC4SS	DRUM OVERSPEED SWITCH	MONITORS DRUM ROTATION; SPEED SWITCH IS ACTUATED WHEN DRUM SPEED IS 120% ABOVE NORMAL OPERATING SPEED, BASED UPON MOTOR SPEED OF 1800 RPM.	a. FAILS OPEN	ROPE DRUM IS ALLOWED TO OVER-SPEED LOWERING LOAD AT A RATE FASTER THAN DESIRED BAND BRAKE IS NOT ACTIVATED. TWO REDUNDANT BRAKES CAN STOP AND HOLD LOAD BY RETURN OF MASTER SWITCH TO OFF POSITION OR USE OF E-STOP BY OPERATOR.	SUBSEQUENT FAILURE OF THE GEAR REDUCER COULD RESULT IN A DROPPED PAYLOAD CONTAINING SOLID PROPELLANT AND HYPERGOLS. POSSIBLE LOSS OF LIFE AND/OR PAYLOAD.	3
			a. SWITCH FAILS TO RESET	HOIST IS INOPERATIVE.	NO EFFECT.	3
NONE NONE	BLOWER MOTOR	DRIVES A FAN TO MOVE AIR ACROSS THE HOIST MOTOR.	a. INOPERATIVE	HOIST MOTOR MAY OVERHEAT.	NO EFFECT.	3

Table 5 (Page 2 of 17). **ELECTRICAL FMEA**

System 90-TON HOIST RSS
Subsystem ELECTRICAL
Drawing No. 79K40112 **Sheet No.** ALL
PMN K61-0168

Program SPACE SHUTTLE

Station Set/Facility Code RW
Date DECEMBER 1993
Reference Figure Used 6,7,8
Prepared By B. KALLE, LSOC 52-11

FIND NO. PART NO.	PART NAME	PART FUNCTION	a. FAILURE MODE b. CAUSE c. FMN d. DETECTION METHOD e. CORRECTING ACTION f. TIME TO EFFECT g. TIMEFRAME	FAILURE EFFECT ON SYSTEM PERFORMANCE	FAILURE EFFECT ON VEHICLE SYSTEMS AND/OR PERSONNEL SAFETY	CRIT CAT
CHLS 38 9007-BRG1BN2	LEVER UPPER LIMIT SWITCH	UPPER SAFETY LIMITING DEVICE TO PREVENT HOIST FROM RAISING PAST THIS LIMIT. BACK OUT CAPABILITY, AUTO-RESET.	a. CONTACTS FAIL OPEN	HOIST IS INOPERATIVE.	NO EFFECT.	3
			a. CONTACTS FAIL CLOSED	HOIST WILL NOT STOP AT PRESET POINT. THE HOIST TRAVEL WILL BE LIMITED BY THE UPPER LIMIT POWER CUT OFF SWITCH.	NO EFFECT.	3
PHLS 36 TYPE 4220	POWER HOIST LIMIT SWITCH	FINAL UPPER LIMIT POWER CUT OFF SWITCH. NO BACK OUT CAPABILITY, MANUAL RESET.	a. CONTACTS FAIL CLOSED	HOOK BLOCK DOES NOT STOP AT LIMIT. THIS CONDITION REQUIRES DOUBLE FAILURE INVOLVING UPPER LIMIT SWITCHES.	NO EFFECT.	3
			a. CONTACTS FAIL OPEN	HOIST IS INOPERATIVE	NO EFFECT.	3
GLLS 37 CR115E427 122	GEARED ROTARY LOWER LIMIT SWITCH	SAFETY LIMITING DEVICE TO PREVENT THE LOAD BLOCK FROM TRAVELING BELOW A SPECIFIED HEIGHT.	a. CONTACTS FAIL OPEN	DOWN MODE OF HOIST WILL NOT FUNCTION.	NO EFFECT.	3
			a. CONTACTS FAIL CLOSED	LOAD BLOCK COULD BE LOWERED PAST THE SAFETY LIMIT POSSIBLY CAUSING ROPE TO WIND IN THE OPPOSITE DIRECTION BREAKING CLAMP DEVICES AND DROPPING HOOK BLOCK. OBSERVERS ON STATION WILL STOP OPERATION.	NO EFFECT.	3
29, 30 9001-KR25R	E-STOP SWITCH (3)	ENERGIZES RELAY COIL OF MAINLINE SHUNT TRIP CIRCUIT BREAKER MCB.	a. CONTACT FAILS OPEN	E-STOP SWITCH COULD NOT TERMINATE HOIST OPERATIONS. TWO REDUNDANT E-STOP SWITCHES COULD HALT HOIST OPERATIONS.	NO EFFECT.	3
			a. CONTACT FAILS CLOSED	HOIST IS INOPERATIVE.	NO EFFECT.	3

Table 5 (Page 3 of 17). **ELECTRICAL FMEA**

System 90-TON HOIST RSS
Subsystem ELECTRICAL
Drawing No. 79K40112 **Sheet No.** ALL
PMN K61-0168

Program SPACE SHUTTLE

Station Set/Facility Code RW
Date DECEMBER 1993
Reference Figure Used 6,7,8
Prepared By B. KALLE, LSOC 52-11

FIND NO. PART NO.	PART NAME	PART FUNCTION	a. FAILURE MODE b. CAUSE c. FMN d. DETECTION METHOD e. CORRECTING ACTION f. TIME TO EFFECT g. TIMEFRAME	FAILURE EFFECT ON SYSTEM PERFORMANCE	FAILURE EFFECT ON VEHICLE SYSTEMS AND/OR PERSONNEL SAFETY	CRIT CAT
1-TR 58 849A-Z002S	REDUCER BRAKE TIME DELAY RELAY	PROVIDES APPROXIMATELY 1 SECOND DELAY BEFORE APPLYING THE REDUCER BRAKE.	a. RELAY FAILS TO ACTIVATE (DE-ENERGIZED)	REDUCER BRAKE WILL NOT DISENGAGE, HOIST WILL NOT OPERATE.	NO EFFECT.	3
			a. RELAY FAILS ACTIVATED (ENERGIZED)	REDUCER BRAKE WILL BE DISENGAGED WHENEVER POWER IS APPLIED TO HOIST. MOTOR BRAKE WILL HOLD LOAD, BAND BRAKE WILL STOP FALLING LOAD IF MOTOR BRAKE HAS FAILED. REQUIRES TRIPLE FAILURE.	NO EFFECT.	3
CT 1 9 NONE	CONTROL TRANSFORMER 1 750VA 480/120AC	PROVIDES 120 VOLT AC POWER TO ALL 3 E-STOPS AND DRUM BRAKE.	a. FAILS OPEN	LOSS OF E-STOP CAPABILITY, INDICATOR LIGHT ON EACH E-STOP WILL GO OUT. HOIST CAN BE STOPPED BY MAIN POWER OFF PUSH BUTTON.	NO EFFECT.	3
			a. FAILS SHORT	LOSS OF E-STOP CAPABILITY, INDICATOR LIGHT ON EACH E-STOP WILL GO OUT. HOIST CAN BE STOPPED BY MAIN POWER OFF PUSH BUTTON.	NO EFFECT.	3
CT 2 9 NONE	CONTROL TRANSFORMER 2 750VA 480/120AC	PROVIDES 120 VOLT POWER TO HOIST CONTROLS.	a. FAILS OPEN	HOIST IS INOPERATIVE.	NO EFFECT.	3
			a. FAILS SHORT	HOIST IS INOPERATIVE.	NO EFFECT.	3

Table 5 (Page 4 of 17). **ELECTRICAL FMEA**

System 90-TON HOIST RSS
Subsystem ELECTRICAL
Drawing No. 79K40112 **Sheet No.** ALL
PMN K61-0168

Program SPACE SHUTTLE

Station Set/Facility Code RW
Date DECEMBER 1993
Reference Figure Used 6,7,8
Prepared By B. KALLE, LSOC 52-11

FIND NO. PART NO.	PART NAME	PART FUNCTION	a. FAILURE MODE b. CAUSE c. FMN d. DETECTION METHOD e. CORRECTING ACTION f. TIME TO EFFECT g. TIMEFRAME	FAILURE EFFECT ON SYSTEM PERFORMANCE	FAILURE EFFECT ON VEHICLE SYSTEMS AND/OR PERSONNEL SAFETY	CRIT CAT
MCB 4 NONE	MAIN CIRCUIT BREAKER, SHUNT TRIP 480 VOLTS AC 3-PHASE 225A (SUB-STATION CIRCUIT BREAKER TRIPS AT 175A)	PROVIDES E-STOP CAPABILITY.	a. PREMATURE TRIP	HOIST IS INOPERATIVE.	NO EFFECT.	3
			a. FAILS TO TRIP (OPEN IN COIL)	LOSS OF E-STOP CAPABILITY. HOIST CAN BE STOPPED BY MAIN POWER OFF PUSH BUTTON.	NO EFFECT.	3
DBR 16 KRPA5AG-120	BAND BRAKE RELAY	DE-ENERGIZES BAND BRAKE VALVE IF AN OVERSPEED IS DETECTED. REMAINS ENERGIZED UNTIL BRAKE RESET BUTTON IS PRESSED TO RESET (ENERGIZE) BAND BRAKE SOLENOID VALVE.	a. RELAY FAILS TO ACTIVATE (DE-ENERGIZED)	BAND BRAKE VALVE WILL RESET AS SOON AS OVERSPEED SWITCH RESETS. BRAKE WILL REMAIN ON UNTIL MANUALLY PUMPED OFF.	NO EFFECT.	3
			a. RELAY FAILS ACTIVATED (ENERGIZED)	BAND BRAKE IS SET AT ALL TIMES, HOIST IS INOPERATIVE.	NO EFFECT.	3
18 CR2940 U202	BAND BRAKE RESET PUSH-BUTTON SWITCH (NORMALLY CLOSED)	DE-ENERGIZES BAND BRAKE RELAY, ENERGIZING BAND BRAKE VALVE.	a. FAILS OPEN	BAND BRAKE VALVE WILL RESET AS SOON AS OVERSPEED SWITCH RESETS. BRAKE WILL REMAIN ON UNTIL MANUALLY PUMPED OFF.	NO EFFECT.	3
			a. FAILS CLOSED	UNABLE TO RELEASE BAND BRAKE. HOIST IS INOPERATIVE.	NO EFFECT.	3

Table 5 (Page 5 of 17). **ELECTRICAL FMEA**

System 90-TON HOIST RSS
Subsystem ELECTRICAL
Drawing No. 79K40112 **Sheet No.** ALL
PMN K61-0168

Program SPACE SHUTTLE

Station Set/Facility Code RW
Date DECEMBER 1993
Reference Figure Used 6,7,8
Prepared By B. KALLE, LSOC 52-11

FIND NO. PART NO.	PART NAME	PART FUNCTION	a. FAILURE MODE b. CAUSE c. FMN d. DETECTION METHOD e. CORRECTING ACTION f. TIME TO EFFECT g. TIMEFRAME	FAILURE EFFECT ON SYSTEM PERFORMANCE	FAILURE EFFECT ON VEHICLE SYSTEMS AND/OR PERSONNEL SAFETY	CRIT CAT
18 CR2940 UA200B	BAND BRAKE SET PUSH-BUTTON SWITCH (NORMALLY OPEN)	ENERGIZES BAND BRAKE RELAY AND DE-ENERGIZES BAND BRAKE SOLENOID VALVE SETTING BAND BRAKE.	a. FAILS OPEN	UNABLE TO SET BAND BRAKE EXCEPT IN AN OVERSPEED CONDITION.	NO EFFECT.	3
			a. FAILS CLOSED	UNABLE TO RELEASE BAND BRAKE, HOIST IS INOPERATIVE.	NO EFFECT.	3
25 9001-KR-1BHG	POWER OFF PUSH-BUTTON SWITCH (NORMALLY CLOSED)	SHUTS OFF POWER TO HOIST.	a. FAILS OPEN	UNABLE TO PROVIDE POWER TO HOIST.	NO EFFECT.	3
			a. FAILS CLOSED	UNABLE TO CUT OFF POWER VIA POWER OFF BUTTON. ANY E-STOP WILL TERMINATE POWER.	NO EFFECT.	3
26 9001-K1L1O	POWER ON PUSH-BUTTON SWITCH (NORMALLY OPEN)	TURNS ON POWER TO HOIST BY ENERGIZING MAIN CONTACTOR.	a. FAILS OPEN	UNABLE TO PROVIDE POWER TO HOIST.	NO EFFECT.	3
			a. FAILS CLOSED	UNABLE TO CUT OFF POWER VIA POWER OFF BUTTON. ANY E-STOP WILL TERMINATE POWER.	NO EFFECT.	3
M 3 NONE	MAIN LINE CONTACTOR	SUPPLIES 480 VOLT 3-PHASE AC POWER TO HOIST.	a. RELAY FAILS TO ACTIVATE (DE-ENERGIZED)	UNABLE TO SUPPLY POWER, HOIST IS INOPERATIVE. BOTH MOTOR AND REDUCER BRAKES ARE RELEASED. RETURN OF MASTER SWITCH TO OFF POSITION, USE OF E-STOP OR DRUM OVERSPEED SWITCH WILL PREVENT LOAD FROM DROPPING.	NO EFFECT.	3

Table 5 (Page 6 of 17). **ELECTRICAL FMEA**

System 90-TON HOIST RSS
Subsystem ELECTRICAL
Drawing No. 79K40112 **Sheet No.** ALL
PMN K61-0168

Program SPACE SHUTTLE

Station Set/Facility Code RW
Date DECEMBER 1993
Reference Figure Used 6,7,8
Prepared By B. KALLE, LSOC 52-11

FIND NO. PART NO.	PART NAME	PART FUNCTION	a. FAILURE MODE b. CAUSE c. FMN d. DETECTION METHOD e. CORRECTING ACTION f. TIME TO EFFECT g. TIMEFRAME	FAILURE EFFECT ON SYSTEM PERFORMANCE	FAILURE EFFECT ON VEHICLE SYSTEMS AND/OR PERSONNEL SAFETY	CRIT CAT
			a. RELAY FAILS ACTIVATED (ENERGIZED)	UNABLE TO CUT OFF POWER VIA POWER OFF BUTTON. ANY E-STOP WILL TERMINATE POWER.	NO EFFECT.	3
M1 NA	RELAY CONTACT NORMALLY OPEN	SUPPLIES 480 VOLT AC PHASE A POWER.	a. FAILS OPEN	3-PHASE AC GOES TO 1 PHASE. HOIST MOTOR MAY BE UNABLE TO TO OPERATE. BOTH MOTOR BRAKES AND REDUCER BRAKES ARE RELEASED. RETURN OF MASTER SWITCH TO OFF POSITION, USE OF E-STOP OR DRUM OVERSPEED SWITCH WILL PREVENT LOAD FROM DROPPING.	NO EFFECT.	3
			a. FAILS CLOSED	NO EFFECT.	NO EFFECT.	3
M2 NA	RELAY CONTACT NORMALLY OPEN	SUPPLIES 480 VOLT AC PHASE B POWER.	a. FAILS OPEN	3-PHASE AC GOES TO 1 PHASE. HOIST MOTOR MAY BE UNABLE TO OPERATE. BOTH MOTOR AND REDUCER BRAKES ARE RELEASED. RETURN OF MASTER SWITCH TO OFF POSITION, USE OF E-STOP OR DRUM OVERSPEED SWITCH WILL PREVENT LOAD FROM DROP-PING.	NO EFFECT.	3
			a. FAILS CLOSED	NO EFFECT.	NO EFFECT.	3
M3 NA	RELAY CONTACT NORMALLY OPEN	SUPPLIES 480 VOLT AC PHASE C POWER.	a. FAILS OPEN	3-PHASE AC GOES TO 1 PHASE. HOIST MOTOR MAY BE UNABLE TO OPERATE. BOTH MOTOR AND REDUCER BRAKES ARE RELEASED. RETURN OF MASTER SWITCH TO OFF POSITION, USE OF E-STOP OR DRUM OVERSPEED SWITCH WILL PREVENT LOAD FROM DROP-PING.	NO EFFECT.	3
			a. FAILS CLOSED	NO EFFECT.	NO EFFECT.	3

Table 5 (Page 7 of 17). **ELECTRICAL FMEA**

System 90-TON HOIST RSS
Subsystem ELECTRICAL
Drawing No. 79K40112 **Sheet No.** ALL
PMN K61-0168

Program SPACE SHUTTLE

Station Set/Facility Code RW
Date DECEMBER 1993
Reference Figure Used 6,7,8
Prepared By B. KALLE, LSOC 52-11

FIND NO. PART NO.	PART NAME	PART FUNCTION	a. FAILURE MODE b. CAUSE c. FMN d. DETECTION METHOD e. CORRECTING ACTION f. TIME TO EFFECT g. TIMEFRAME	FAILURE EFFECT ON SYSTEM PERFORMANCE	FAILURE EFFECT ON VEHICLE SYSTEMS AND/OR PERSONNEL SAFETY	CRIT CAT
M4 NA	RELAY CONTACT NORMALLY OPEN	MAINTAINS 120 VOLT AC POWER TO MAIN CONTACTOR RELAY COIL AFTER POWER ON PUSH BUTTON IS RELEASED.	a. FAILS OPEN	AC POWER WILL CUT OFF AS SOON AS THE POWER ON BUTTON IS RELEASED.	NO EFFECT.	3
			a. FAILS CLOSED	UNABLE TO SHUT OFF POWER VIA POWER OFF BUTTON. ANY E-STOP WILL SHUT OFF POWER.	NO EFFECT.	3
BM 7 NONE	BLOWER MOTOR RELAY	SUPPLIES 480 VOLT 3-PHASE AC POWER TO BLOWER MOTOR TO MAINTAIN AIR FLOW THROUGH HOIST MOTOR.	a. RELAY FAILS TO ACTIVATE	HOIST MOTOR MAY OVERHEAT.	NO EFFECT.	3
			a. RELAY FAILS ACTIVATED	BLOWER WILL OPERATE NORMALLY.	NO EFFECT.	3
MTC 13 TYPE 51AA	MOTOR TEMPERATURE CONTROL MODULE	SENSES OVERHEAT CONDITION IN MOTOR HIGH OR LOW SPEED WINDINGS AND DE-ENERGIZES MOTOR OVERHEAT RELAY TO ACTIVATE OVERHEAT LIGHT.	a. RELAY FAILS TO ACTIVATE (DE-ENERGIZED)	FALSE OVERHEAT INDICATION.	NO EFFECT.	3
			a. RELAY FAILS ACTIVATED (ENERGIZED)	FAILS TO DETECT OVERHEAT CONDITION. HOIST MOTOR MAY BE DAMAGED.	NO EFFECT.	3
NA 45 4211	HOIST MASTER SWITCH	SELECTS DIRECTION AND EITHER HIGH OR LOW SPEED IN EACH DIRECTION.	a. FAILS OPEN	HOIST INOPERATIVE.	NO EFFECT.	3
			a. FAILS CLOSED	HOIST CONTINUES TO OPERATE WHEN OFF IS DESIRED. HOIST CAN BE STOPPED BY POWER OFF PUSH-BUTTON OR ANY E-STOP.	POSSIBLE PAYLOAD DAMAGE. REQUIRES 2 OR 3 CONTACTS TO STICK CLOSED TO OPERATE AT LOW AND HIGH SPEEDS RESPECTIVELY.	3

Table 5 (Page 8 of 17). **ELECTRICAL FMEA**

System 90-TON HOIST RSS
Subsystem ELECTRICAL
Drawing No. 79K40112 **Sheet No.** ALL
PMN K61-0168

Program SPACE SHUTTLE

Station Set/Facility Code RW
Date DECEMBER 1993
Reference Figure Used 6,7,8
Prepared By B. KALLE, LSOC 52-11

FIND NO. PART NO.	PART NAME	PART FUNCTION	a. FAILURE MODE b. CAUSE c. FMN d. DETECTION METHOD e. CORRECTING ACTION f. TIME TO EFFECT g. TIMEFRAME	FAILURE EFFECT ON SYSTEM PERFORMANCE	FAILURE EFFECT ON VEHICLE SYSTEMS AND/OR PERSONNEL SAFETY	CRIT CAT
	SWITCH CONTACTS NOS. 1 AND 2	SELECTS UP DIRECTION BOTH HIGH AND LOW SPEEDS. CONTACT IN SERIES.	a. EITHER CONTACT FAILS OPEN	HOIST UP DIRECTION INOPERATIVE.	NO EFFECT.	3
			a. EITHER CONTACT FAILS CLOSED	NO EFFECT.	NO EFFECT.	3
	SWITCH CONTACTS NOS. 3 AND 6	SELECTS DOWN DIRECTION BOTH HIGH AND LOW SPEEDS. CONTACTS IN SERIES.	a. EITHER CONTACT FAILS OPEN	HOIST DOWN DIRECTION INOPERATIVE.	NO EFFECT.	3
			a. EITHER CONTACT FAILS CLOSED	NO EFFECT.	NO EFFECT.	3
	SWITCH CONTACT NO. 4	SELECTS HIGH SPEED UP.	a. FAILS OPEN	HOIST HIGH SPEED UP IS INOPERATIVE.	NO EFFECT.	3
			a. FAILS CLOSED	HOIST WILL CONTINUE TO OPERATE IN HIGH SPEED UP OR WILL SHIFT INTO HIGH SPEED UP 2-3 SECONDS AFTER UP DIRECTION IS SELECTED REGARDLESS OF WHICH SPEED IS DESIRED. RETURN OF MASTER SWITCH TO OFF POSITION OR USE OF E-STOP WILL STOP AND HOLD THE LOAD. UPPER LIMIT SWITCHES WILL PREVENT OVERTRAVEL. DOES NOT COMPLY WITH NSS/GO 1740.9 REQUIREMENTS WITH REGARD TO UNDESIRED CHANGES IN SPEED RANGE.	NO EFFECT.	3
	SWITCH CONTACT NO. 5	SELECTS HIGH SPEED DOWN.	a. FAILS OPEN	HOIST HIGH SPEED DOWN IS IN OPERATIVE.	NO EFFECT.	3

Table 5 (Page 9 of 17). **ELECTRICAL FMEA**

System 90-TON HOIST RSS
Subsystem ELECTRICAL
Drawing No. 79K40112 **Sheet No.** ALL
PMN K61-0168

Program SPACE SHUTTLE

Station Set/Facility Code RW
Date DECEMBER 1993
Reference Figure Used 6,7,8
Prepared By B. KALLE, LSOC 52-11

FIND NO. PART NO.	PART NAME	PART FUNCTION	a. FAILURE MODE b. CAUSE c. FMN d. DETECTION METHOD e. CORRECTING ACTION f. TIME TO EFFECT g. TIMEFRAME	FAILURE EFFECT ON SYSTEM PERFORMANCE	FAILURE EFFECT ON VEHICLE SYSTEMS AND/OR PERSONNEL SAFETY	CRIT CAT
			a. FAILS CLOSED	HOIST WILL CONTINUE TO OPERATE IN HIGH SPEED DOWN OR WILL SHIFT INTO HIGH SPEED DOWN 2-3 SECONDS AFTER DOWN DIRECTION IS SELECTED REGARDLESS OF WHICH SPEED IS DESIRED. RETURN OF MASTER SWITCH TO OFF POSITION OR USE OF E-STOP WILL STOP AND HOLD THE LOAD. DOES NOT COMPLY WITH NSS/GO 1740.9 REQUIREMENTS WITH REGARD TO UNDESIRED CHANGES IN SPEED RANGE.	SUFFICIENT TIME (17 SECONDS) AND DISTANCE (3 FT) EXISTS FOR FAILURE TO MANIFEST ITSELF AND CORRECTIVE ACTION TO BE TAKEN.	3
2-CR 59 700BP200-AA	MOTOR / REDUCER BRAKE RELAY LOW SPEED HOIST	RELEASES MOTOR AND REDUCER DISC BRAKES WHEN LOW SPEED HOIST MODE IS IN OPERATION.	a. RELAY FAILS TO ACTIVATE (DE-ENERGIZED) CONTACT FAILS OPEN	MOTOR AND REDUCER BRAKES WILL REMAIN SET. HOIST WILL NOT OPERATE.	NO EFFECT.	3
			a. RELAY FAILS ACTIVATED (ENERGIZED) CONTACT FAILS CLOSED b. STUCK OR WELDED CONTACTS c. NA d. VISUAL OBSERVATION OF FALLING LOAD e. ACTIVATION OF OPERATOR E-STOP OR OVERSPEED TRIP f. SECONDS g. 3-11 SECONDS	MOTOR AND REDUCER BRAKES WILL REMAIN OFF WHEN HOIST IS STOPPED. OPERATOR USE OF E-STOP WILL SET BOTH BRAKES OR OVERSPEED TRIP WILL SET ALL THREE BRAKES.	NO EFFECT. THERE SHOULD BE SUFFICIENT TIME FOR THE OPERATOR OR OVERSPEED SYSTEM TO WORK TO PREVENT LOSS/DAMAGE TO A PAYLOAD.	3
3-CR 59 700BP200-AA	MOTOR / REDUCER BRAKE RELAY HIGH SPEED HOIST	RELEASES MOTOR AND REDUCER DISC BRAKES WHEN HIGH SPEED HOIST MODE IS IN OPERATION.	a. RELAY FAILS TO ACTIVATE (DE-ENERGIZED) CONTACT FAILS OPEN	MOTOR AND REDUCER BRAKES WILL REMAIN SET. HOIST WILL NOT OPERATE.	NO EFFECT.	3

Table 5 (Page 10 of 17). **ELECTRICAL FMEA**

System 90-TON HOIST RSS
Subsystem ELECTRICAL
Drawing No. 79K40112 **Sheet No.** ALL
PMN K61-0168

Program SPACE SHUTTLE

Station Set/Facility Code RW
Date DECEMBER 1993
Reference Figure Used 6,7,8
Prepared By B. KALLE, LSOC 52-11

FIND NO. PART NO.	PART NAME	PART FUNCTION	a. FAILURE MODE b. CAUSE c. FMN d. DETECTION METHOD e. CORRECTING ACTION f. TIME TO EFFECT g. TIMEFRAME	FAILURE EFFECT ON SYSTEM PERFORMANCE	FAILURE EFFECT ON VEHICLE SYSTEMS AND/OR PERSONNEL SAFETY	CRIT CAT
			a. RELAY FAILS ACTIVATED (ENERGIZED) CONTACT FAILS CLOSED b. STUCK OR WELDED CONTACTS c. NA d. VISUAL OBSERVATION OF FALLING LOAD e. ACTIVATION OF OPERATOR E-STOP OR OVERSPEED TRIP f. SECONDS g. 3-11 SECONDS	MOTOR AND REDUCER BRAKES WILL REMAIN OFF WHEN HOIST IS STOPPED. OPERATOR USE OF E-STOP WILL SET BOTH BRAKES OR OVERSPEED TRIP WILL SET ALL THREE BRAKES.	NO EFFECT. THERE SHOULD BE SUFFICIENT TIME FOR THE OPERATOR OR OVERSPEED SYSTEM TO WORK TO PREVENT LOSS/DAMAGE TO A PAYLOAD.	3
T 50, 51 SCARXS11 XXAPXA	TIME DELAY RELAY (2-3 SECONDS TO CLOSE)	PREVENTS THE HOIST FROM BEING STARTED ON THE MOTOR'S HIGH SPEED WINDINGS.	a. RELAY FAILS TO ACTIVATE (DE-ENERGIZED) CONTACT FAILS OPEN	LOSS OF HIGH SPEED HOIST FUNCTIONS.	NO EFFECT.	3
			a. RELAY FAILS ACTIVATED (ENERGIZED) CONTACT FAILS CLOSED	LOSS OF LOW SPEED HOIST FUNCTIONS.	NO EFFECT.	3
			a. RELAY ACTIVATES PREMATURELY	MAY REDUCE LIFETIME OF MOTOR HIGH SPEED WINDINGS.	NO EFFECT.	3
CR 48 CR12B04 022	RELAY	SWITCHES FROM HOIST MOTOR LOW SPEED WINDINGS TO HIGH SPEED WINDINGS WHEN TIME DELAY CONTACT CLOSES.	a. RELAY FAILS TO ACTIVATE (DE-ENERGIZED)	LOSS OF HIGH SPEED HOIST FUNCTIONS.	NO EFFECT.	3
			a. RELAY FAILS ACTIVATED (ENERGIZED)	LOSS OF LOW SPEED HOIST FUNCTIONS.	NO EFFECT.	3
N.C. 1 NA	RELAY CONTACT NORMALLY CLOSED	ACTIVATES LOW SPEED UP MOTOR STARTER RELAY.	a. CONTACT FAILS OPEN	LOSS OF LOW SPEED UP FUNCTION.	NO EFFECT.	3

Table 5 (Page 11 of 17). **ELECTRICAL FMEA**

System 90-TON HOIST RSS
Subsystem ELECTRICAL
Drawing No. 79K40112 **Sheet No.** ALL
PMN K61-0168

Program SPACE SHUTTLE

Station Set/Facility Code RW
Date DECEMBER 1993
Reference Figure Used 6,7,8
Prepared By B. KALLE, LSOC 52-11

FIND NO. PART NO.	PART NAME	PART FUNCTION	a. FAILURE MODE b. CAUSE c. FMN d. DETECTION METHOD e. CORRECTING ACTION f. TIME TO EFFECT g. TIMEFRAME	FAILURE EFFECT ON SYSTEM PERFORMANCE	FAILURE EFFECT ON VEHICLE SYSTEMS AND/OR PERSONNEL SAFETY	CRIT CAT
			a. CONTACT FAILS CLOSED	LOSS OF HIGH SPEED UP FUNCTION.	NO EFFECT.	3
N.C. 2 NA	RELAY CONTACT NORMALLY CLOSED	ACTIVATES LOW SPEED DOWN MOTOR STARTER RELAY.	a. CONTACT FAILS OPEN	LOSS OF LOW SPEED DOWN FUNCTION.	NO EFFECT.	3
			a. CONTACT FAILS CLOSED	LOSS OF HIGH SPEED DOWN FUNCTION.	NO EFFECT.	3
N.O. 1 NA	RELAY CONTACT NORMALLY OPEN	ACTIVATES HIGH SPEED UP MOTOR STARTER RELAY.	a. CONTACT FAILS OPEN	LOSS OF HIGH SPEED UP FUNCTION.	NO EFFECT.	3
			a. CONTACT FAILS CLOSED	LOSS OF LOW SPEED UP FUNCTION.	NO EFFECT.	3
N.O. 2 NA	RELAY CONTACT NORMALLY OPEN	ACTIVATES HIGH SPEED DOWN MOTOR STARTER RELAY.	a. CONTACT FAILS OPEN	LOSS OF HIGH SPEED DOWN FUNCTION.	NO EFFECT.	3
			a. CONTACT FAILS CLOSED	LOSS OF LOW SPEED DOWN FUNCTION.	NO EFFECT.	3
41, 42 309501 REV. B 390A-3095	LOAD CELL LOAD CELL SET POINT CONTROLLER AND OVERLOAD CUT OUT (O.L. C/O) RELAY	DETECTS HOIST OVERLOAD CONDITIONS AND DISABLES HOIST UP FUNCTIONS.	a. ERRONEOUS HIGH INDICATION	LOSS OF HOIST UP FUNCTIONS IN NON-OVERLOADED CONDITION.	NO EFFECT.	3
			a. ERRONEOUS LOW INDICATION	OVERLOAD CONDITION MAY GO UNDETECTED. REQUIRES HUMAN ERROR TO ATTEMPT TO LIFT HIGHER THAN RATED LOADS.	NO EFFECT.	3

Table 5 (Page 12 of 17). **ELECTRICAL FMEA**

System 90-TON HOIST RSS
Subsystem ELECTRICAL
Drawing No. 79K40112 **Sheet No.** ALL
PMN K61-0168

Program SPACE SHUTTLE

Station Set/Facility Code RW
Date DECEMBER 1993
Reference Figure Used 6,7,8
Prepared By B. KALLE, LSOC 52-11

FIND NO. PART NO.	PART NAME	PART FUNCTION	a. FAILURE MODE b. CAUSE c. FMN d. DETECTION METHOD e. CORRECTING ACTION f. TIME TO EFFECT g. TIMEFRAME	FAILURE EFFECT ON SYSTEM PERFORMANCE	FAILURE EFFECT ON VEHICLE SYSTEMS AND/OR PERSONNEL SAFETY	CRIT CAT
			a. O.L. C/O RELAY FAILS TO ACTIVATE	OVERLOAD CONDITION MAY GO UNDETECTED. REQUIRES HUMAN ERROR TO ATTEMPT TO LIFT HIGHER TAN RATED LOADS.	NO EFFECT.	3
			a. O.L. C/O RELAY FAILS ACTIVATED	LOSS OF HOIST UP FUNCTIONS.	NO EFFECT.	3
UP-LOW 2 SIZE 4	MOTOR STARTER RELAY UP LOW SPEED	ENERGIZES HOIST MOTOR LOW SPEED WINDINGS IN UP DIRECTION. DISABLES REMAINING HOIST FUNCTIONS. RELEASES MOTOR AND REDUCER DISC BRAKES.	a. RELAY FAILS TO ACTIVATE (DE-ENERGIZED)	LOSS OF LOW SPEED UP FUNCTION.	NO EFFECT.	3
			a. RELAY FAILS ACTIVATED (ENERGIZED)	HOIST WILL CONTINUE TO DRIVE IN THE UP DIRECTION IN LOW SPEED UNLESS POWER OFF PUSHBUTTON OR E-STOP IS USED OR AN UP LIMIT SWITCH IS TRIPPED.	NO EFFECT.	3
UP-LOW N.O. 1-3 NA	MAIN RELAY CONTACTS NORMALLY OPEN	ENERGIZES HOIST MOTOR LOW SPEED WINDINGS IN UP DIRECTION.	a. ANY ONE CONTACT FAILS OPEN	3-PHASE AC POWER GOES TO 1 PHASE, MOTOR MAY DEVELOP INSUFFICIENT TORQUE TO OPERATE. BOTH MOTOR AND REDUCER BRAKES ARE RELEASED. RETURN OF MASTER SWITCH TO OFF POSITION OR USE OF E-STOP BY OPERATOR OR DRUM OVERSPEED SWITCH WILL PREVENT LOAD FROM DROPPING.	NO EFFECT.	3
			a. ANY ONE CONTACT FAILS CLOSED	HOIST WILL OPERATE NORMALLY IN SELECTED MODE. SELECTION OF OPPOSITE DIRECTION WILL CAUSE A PHASE-TO-PHASE SHORT TRIPPING A CIRCUIT BREAKER.	NO EFFECT.	3

Table 5 (Page 13 of 17). **ELECTRICAL FMEA**

System 90-TON HOIST RSS
Subsystem ELECTRICAL
Drawing No. 79K40112 **Sheet No.** ALL
PMN K61-0168

Program SPACE SHUTTLE

Station Set/Facility Code RW
Date DECEMBER 1993
Reference Figure Used 6,7,8
Prepared By B. KALLE, LSOC 52-11

FIND NO. PART NO.	PART NAME	PART FUNCTION	a. FAILURE MODE b. CAUSE c. FMN d. DETECTION METHOD e. CORRECTING ACTION f. TIME TO EFFECT g. TIMEFRAME	FAILURE EFFECT ON SYSTEM PERFORMANCE	FAILURE EFFECT ON VEHICLE SYSTEMS AND/OR PERSONNEL SAFETY	CRIT CAT
UP-LOW N.C. 1-3 NA	AUX. RELAY CONTACTS NORMALLY CLOSED	DISABLES ALL OTHER HOIST FUNCTIONS OTHER THAN UP-LOW.	a. ANY ONE CONTACT FAILS OPEN	LOSS OF EFFECTED HOIST FUNCTION.	NO EFFECT.	3
			a. ANY ONE CONTACT FAILS CLOSED	NO EFFECT. REQUIRES A SECOND CONTACT FAILURE TO INITIATE TWO HOIST FUNCTIONS SIMULTANEOUSLY.	NO EFFECT.	3
UP-LOW N.O. 1 NA	AUX. RELAY CONTACT NORMALLY OPEN	ENERGIZES TIME DELAY RELAY (1-TR). DELAYS REDUCER BRAKE SETTING TILL 1 SECOND AFTER THE MOTOR BRAKE SETS.	a. FAILS OPEN	BOTH BRAKES SET SIMULTANEOUSLY RESULTING IN A HARDER STOP.	NO EFFECT.	3
			a. FAILS CLOSED	TIME DELAY RELAY (1-TR) REMAINS ENERGIZED. REDUCER BRAKE REMAINS OFF. MOTOR BRAKE WILL STOP AND HOLD LOAD.	NO EFFECT.	3
DN-LOW 2 SIZE 4	MOTOR STARTER RELAY DOWN LOW SPEED	ENERGIZES HOIST MOTOR LOW SPEED WINDINGS IN DOWN DIRECTION. DISABLES REMAINING HOIST FUNCTIONS. RELEASES MOTOR AND REDUCER DISC BRAKES.	a. RELAY FAILS TO ACTIVATE (DE-ENERGIZED)	LOSS OF LOW SPEED DOWN FUNCTION.	NO EFFECT.	3
			a. RELAY FAILS ACTIVATED (ENERGIZED)	HOIST WILL CONTINUE TO DRIVE IN THE DOWN DIRECTION IN LOW SPEED UNLESS POWER OFF PUSHBUTTON OR E-STOP IS USED.	NO EFFECT.	3

Table 5 (Page 14 of 17). **ELECTRICAL FMEA**

System 90-TON HOIST RSS
Subsystem ELECTRICAL
Drawing No. 79K40112 **Sheet No.** ALL
PMN K61-0168

Program SPACE SHUTTLE

Station Set/Facility Code RW
Date DECEMBER 1993
Reference Figure Used 6,7,8
Prepared By B. KALLE, LSOC 52-11

FIND NO. PART NO.	PART NAME	PART FUNCTION	a. FAILURE MODE b. CAUSE c. FMN d. DETECTION METHOD e. CORRECTING ACTION f. TIME TO EFFECT g. TIMEFRAME	FAILURE EFFECT ON SYSTEM PERFORMANCE	FAILURE EFFECT ON VEHICLE SYSTEMS AND/OR PERSONNEL SAFETY	CRIT CAT
DN-LOW N.O. 1-3 NA	MAIN RELAY CONTACTS NORMALLY OPEN	ENERGIZES HOIST MOTOR LOW SPEED WINDINGS IN DOWN DIRECTION.	a. ANY ONE CONTACT FAILS OPEN	3-PHASE AC POWER GOES TO 1 PHASE, MOTOR MAY DEVELOP INSUFFICIENT TORQUE TO OPERATE. BOTH MOTOR AND REDUCER BRAKES ARE RELEASED. RETURN OF MASTER SWITCH TO OFF POSITION OR USE OF E-STOP BY OPERATOR OR DRUM OVERSPEED SWITCH WILL PREVENT LOAD FROM DROPPING.	NO EFFECT.	3
			a. ANY ONE CONTACT FAILS CLOSED	HOIST WILL OPERATE NORMALLY IN SELECTED MODE. SELECTION OF OPPOSITE DIRECTION WILL CAUSE A PHASE-TO-PHASE SHORT TRIPPING A CIRCUIT BREAKER.	NO EFFECT.	3
DN-LOW N.C. 1-3 NA	AUX. RELAY CONTACTS NORMALLY CLOSED	DISABLES ALL OTHER HOIST FUNCTIONS OTHER THAN DOWN-LOW.	a. ANY ONE CONTACT FAILS OPEN	LOSS OF EFFECTED HOIST FUNCTION.	NO EFFECT.	3
			a. ANY ONE CONTACT FAILS CLOSED	NO EFFECT. REQUIRES A SECOND CONTACT FAILURE TO INITIATE TWO HOIST FUNCTIONS SIMULTANEOUSLY.	NO EFFECT.	3
DN-LOW N.O. 1 NA	AUX. RELAY CONTACT NORMALLY OPEN	ENERGIZES TIME DELAY RELAY (1-TR). DELAYS REDUCER BRAKE SETTING TILL 1 SECOND AFTER THE MOTOR BRAKE SETS.	a. FAILS OPEN	BOTH BRAKES SET SIMULTANEOUSLY RESULTING IN A HARDER STOP.	NO EFFECT.	3
			a. FAILS CLOSED	TIME DELAY RELAY (1-TR) REMAINS ENERGIZED. REDUCER BRAKE REMAINS OFF. MOTOR BRAKE WILL STOP AND HOLD LOAD.	NO EFFECT.	3

Table 5 (Page 15 of 17). **ELECTRICAL FMEA**

System 90-TON HOIST RSS
Subsystem ELECTRICAL
Drawing No. 79K40112 **Sheet No.** ALL
PMN K61-0168

Program SPACE SHUTTLE

Station Set/Facility Code RW
Date DECEMBER 1993
Reference Figure Used 6,7,8
Prepared By B. KALLE, LSOC 52-11

FIND NO. PART NO.	PART NAME	PART FUNCTION	a. FAILURE MODE b. CAUSE c. FMN d. DETECTION METHOD e. CORRECTING ACTION f. TIME TO EFFECT g. TIMEFRAME	FAILURE EFFECT ON SYSTEM PERFORMANCE	FAILURE EFFECT ON VEHICLE SYSTEMS AND/OR PERSONNEL SAFETY	CRIT CAT
UP-HIGH 2 SIZE 4	MOTOR STARTER RELAY UP HIGH SPEED	ENERGIZES HOIST MOTOR HIGH SPEED WINDINGS IN DOWN DIRECTION. DISABLES REMAINING HOIST FUNCTIONS. RELEASES MOTOR AND REDUCER DISC BRAKES.	a. RELAY FAILS TO ACTIVATE (DE-ENERGIZED)	LOSS OF HIGH SPEED UP FUNCTION.	NO EFFECT.	3
			a. RELAY FAILS ACTIVATED (ENERGIZED)	HOIST WILL CONTINUE TO DRIVE IN THE UP DIRECTION IN HIGH SPEED UNLESS POWER OFF PUSHBUTTON OR E-STOP IS USED OR AN UP LIMIT SWITCH IS TRIPPED.	NO EFFECT.	3
UP-HIGH N.O. 1-3 NA	MAIN RELAY CONTACTS NORMALLY OPEN	ENERGIZES HOIST MOTOR HIGH SPEED WINDINGS IN UP DIRECTION.	a. ANY ONE CONTACT FAILS OPEN	3-PHASE AC POWER GOES TO 1 PHASE, MOTOR MAY DEVELOP INSUFFICIENT TORQUE TO OPERATE. BOTH MOTOR AND REDUCER BRAKES ARE RELEASED. RETURN OF MASTER SWITCH TO OFF POSITION OR USE OF E-STOP BY OPERATOR OR DRUM OVERSPEED SWITCH WILL PREVENT LOAD FROM DROPPING.	NO EFFECT.	3
			a. ANY ONE CONTACT FAILS CLOSED	HOIST WILL OPERATE NORMALLY IN SELECTED MODE. SELECTION OF OPPOSITE DIRECTION WILL CAUSE A PHASE-TO-PHASE SHORT TRIPPING A CIRCUIT BREAKER.	NO EFFECT.	E
UP-HIGH N.C. 1-3 NA	AUX. RELAY CONTACTS NORMALLY CLOSED	DISABLES ALL OTHER HOIST FUNCTIONS OTHER THAN UP-HIGH.	a. ANY ONE CONTACT FAILS OPEN	LOSS OF EFFECTED HOIST FUNCTION.	NO EFFECT.	3
			a. ANY ONE CONTACT FAILS CLOSED	NO EFFECT. REQUIRES A SECOND CONTACT FAILURE TO INITIATE TWO HOIST FUNCTIONS SIMULTANEOUSLY.	NO EFFECT.	3

Table 5 (Page 16 of 17). **ELECTRICAL FMEA**

System 90-TON HOIST RSS
Subsystem ELECTRICAL
Drawing No. 79K40112 **Sheet No.** ALL
PMN K61-0168

Program SPACE SHUTTLE

Station Set/Facility Code RW
Date DECEMBER 1993
Reference Figure Used 6,7,8
Prepared By B. KALLE, LSOC 52-11

FIND NO. PART NO.	PART NAME	PART FUNCTION	a. FAILURE MODE b. CAUSE c. FMN d. DETECTION METHOD e. CORRECTING ACTION f. TIME TO EFFECT g. TIMEFRAME	FAILURE EFFECT ON SYSTEM PERFORMANCE	FAILURE EFFECT ON VEHICLE SYSTEMS AND/OR PERSONNEL SAFETY	CRIT CAT
UP-HIGH N.O. 1 NA	AUX. RELAY CONTACT NORMALLY OPEN	ENERGIZES TIME DELAY RELAY (1-TR). DELAYS REDUCER BRAKE SETTING TILL 1 SECOND AFTER THE MOTOR BRAKE SETS.	a. FAILS OPEN	BOTH BRAKES SET SIMULTANEOUSLY RESULTING IN A HARDER STOP.	NO EFFECT.	3
			a. FAILS CLOSED	TIME DELAY RELAY (1-TR) REMAINS ENERGIZED. REDUCER BRAKE REMAINS OFF. MOTOR BRAKE WILL STOP AND HOLD LOAD.	NO EFFECT.	3
DN-HIGH 2 SIZE 4	MOTOR STARTER RELAY DOWN HIGH SPEED	ENERGIZES HOIST MOTOR LOW SPEED WINDINGS IN DOWN DIRECTION. DISABLES REMAINING HOIST FUNCTIONS. RELEASES MOTOR AND REDUCER DISC BRAKES.	a. RELAY FAILS TO ACTIVATE (DE-ENERGIZED)	LOSS OF HIGH SPEED DOWN FUNCTION.	NO EFFECT.	3
			a. RELAY FAILS ACTIVATED (ENERGIZED)	HOIST WILL CONTINUE TO DRIVE IN THE DOWN DIRECTION IN HIGH SPEED UNLESS POWER OFF PUSHBUTTON E-STOP IS USED.	NO EFFECT.	3
DN-HIGH N.O. 1-3 NA	MAIN RELAY CONTACTS NORMALLY OPEN	ENERGIZES HOIST MOTOR HIGH SPEED WINDINGS IN DOWN DIRECTION.	a. ANY ONE CONTACT FAILS OPEN	3-PHASE AC POWER GOES TO 1 PHASE, MOTOR MAY DEVELOP INSUFFICIENT TORQUE TO OPERATE. BOTH MOTOR AND REDUCER BRAKES ARE RELEASED. RETURN OF MASTER SWITCH TO OFF POSITION OR USE OF E-STOP BY OPERATOR OR DRUM OVERSPEED SWITCH WILL PREVENT LOAD FROM DROPPING.	NO EFFECT.	3
			a. ANY ONE CONTACT FAILS CLOSED	HOIST WILL OPERATE NORMALLY IN SELECTED MODE SELECTION OF OPPOSITE DIRECTION WILL CAUSE A PHASE-TO-PHASE SHORT TRIPPING A CIRCUIT BREAKER.	NO EFFECT.	3

Table 5 (Page 17 of 17). **ELECTRICAL FMEA**

System 90-TON HOIST RSS
Subsystem ELECTRICAL
Drawing No. 79K40112 **Sheet No.** ALL
PMN K61-0168

Program SPACE SHUTTLE

Station Set/Facility Code RW
Date DECEMBER 1993
Reference Figure Used 6,7,8
Prepared By B. KALLE, LSOC 52-11

FIND NO. PART NO.	PART NAME	PART FUNCTION	a. FAILURE MODE b. CAUSE c. FMN d. DETECTION METHOD e. CORRECTING ACTION f. TIME TO EFFECT g. TIMEFRAME	FAILURE EFFECT ON SYSTEM PERFORMANCE	FAILURE EFFECT ON VEHICLE SYSTEMS AND/OR PERSONNEL SAFETY	CRIT CAT
DN-HIGH N.C. 1-3 NA	AUX. RELAY CONTACTS NORMALLY CLOSED	DISABLES ALL OTHER HOIST FUNCTIONS OTHER THAN DOWN-HIGH.	a. ANY ONE CONTACT FAILS OPEN	LOSS OF EFFECTED HOIST FUNCTION.	NO EFFECT.	3
			a. ANY ONE CONTACT FAILS CLOSED	NO EFFECT. REQUIRES A SECOND CONTACT FAILURE TO INITIATE TWO HOIST FUNCTIONS SIMULTANEOUSLY.	NO EFFECT.	3
DN-HIGH N.O. 1 NA	AUX. RELAY CONTACT NORMALLY OPEN	ENERGIZES TIME DELAY RELAY (1-TR). DELAYS REDUCER BRAKE SETTING TILL 1 SECOND AFTER THE MOTOR BRAKE SETS.	a. FAILS OPEN	BOTH BRAKES SET SIMULTANEOUSLY RESULTING IN A HARDER STOP.	NO EFFECT.	3
			a. FAILS CLOSED	TIME DELAY RELAY (1-TR) REMAINS ENERGIZED. REDUCER BRAKE REMAINS OFF. MOTOR BRAKE WILL STOP AND HOLD LOAD.	NO EFFECT.	3
PSR 57 SLA-440-AFE	POWER MONITOR 480 VOLTS AC 3-PHASE	ASSURES PROPERLY PHASED AC POWER IS PROVIDED TO THE HOIST. PROTECTS AGAINST OPERATION WITH REVERSED PHASING SINGLE PHASE AND LOW VOLTAGE.	a. FAILS TO DETECT LOW VOLTAGE	DAMAGE TO HOIST MOTOR. REQUIRES PRIOR FAILURE IN 60 HZ POWER.	NO EFFECT.	3
			a. FAILS TO DETECT PHASE REVERSAL	HOIST MAY OPERATE IN OPPOSITE OF COMMANDED DIRECTION DUE TO REVERSE PHASING OPERATION CAN BE STOPPED BY RETURNING MASTER SWITCH TO OFF POSITION OR USE OF E-STOP.	NO EFFECT.	3
			a. CONTACT FAILS OPEN	HOIST INOPERATIVE.	NO EFFECT.	3
			a. CONTACT FAILS CLOSED	LOSS OF POWER MONITORING.	NO EFFECT.	3

5.3 FLEXHOSE FMEA

There are no flexhoses associated with the critical functions assessed in section 4.0 for this system.

5.4 ORIFICE FMEA

There are no orifices associated with the critical functions assessed in section 4.0 for this system.

5.5 FILTER FMEA

There are no filters associated with the critical functions assessed in section 4.0 for this system.

6.0 CRITICAL ITEMS LIST

There were no Critical Items identified in this system.

7.0 HAZARD ANALYSIS

The hazard analysis for the 90-Ton Hoist, Pad B PCR was conducted in accordance with NSTS 22254. The objective of this analysis is to:

- Document the hazards identified from the analysis
- Provide visibility of the risks associated with operation of the system
- Evaluate the adequacy of existing controls for the identified hazards
- Propose additional controls and new hazard reports as required

7.1 SAFETY CRITICALITY ASSESSMENT

The 90-Ton Hoist, Pad-B RSS, is assessed as a safety critical system because it handles flight hardware (payloads).

7.2 SCOPE

The following were assessed in the preparation of this hazard analysis:

- Design hazards that could result in damage to flight hardware or injury to personnel
- Operational/procedural hazards that occur during system use
- Functional interfaces to determine if any hazardous conditions exist across the interfaces upstream and downstream of the equipment/system

7.3 SUMMARY OF ANALYSIS

System Safety Engineering performed an analysis of the 90-Ton Hoist at the Pad-B PCR. A KSC/RT Safety and Reliability Hazard Database search, for hazard reports pertaining to this system, was completed for baseline (B/L) number, and program model number (PMN). A walkdown of the associated system was conducted, and the system was analyzed with emphasis on the electrical and mechanical aspects.

A qualitative fault tree was developed for the system in which the top event was Injury/Loss of Life to personnel or flight hardware damage. The conditions "load drops" or "load contacts personnel" or "load collision due to downward overtravel," were considered to lead to the top event.

The search of the KSC/RT Safety and Reliability Hazard Database resulted in one controlled and one accepted risk hazard identified during this analysis.

The Hazard Analysis Documentation Sheet (KSC Form 29-736), fault tree analysis, and columnar format sheets provide additional information.

HAZARD ANALYSIS DOCUMENTATION

SAA Number	System / Subsystem
SAA09FTB3-003	90-Ton Payload Hoist at the Rotating Service Structure Hoist Equipment Room Pad-B

See SAA Cover Sheet for applicable Baseline Number(s), Program Model Number(s), Work Unit Code(s) and Station Set(s).

The Hazard Analysis was based on the following documentation:

Document Number	Title
NSTS 22254	Methodology For Conduct Of NSTS Hazard Analyses
GP1098G	KSC Ground Operations Safety Plan
NSS/GO 1740.9B	Safety Standards for Lifting Devices & Equipment
OMI ES026	Orbiter Payload Canister Handling - LC-39 Pads A or B
OMI M3160	Payload Canister Hoisting Operations, Pads A or B
OMI Q3437	90-Ton Hoist, RSS, Pad A/B, KSC
OMI Q6325	90-Ton Payload Canister Hoist, Pad B

The search of the KSC/RT Safety and Reliability Hazard Database resulted in one controlled and one accepted risk hazard identified during this analysis.

Safety Engineer	Approved
Gary Whitmore Gary M Whitmore	11/22/93 Supervisor, System Safety Engineering

HAZARD #: **RT-ENG-1019** REVISION: REVISION DATE: / /
MASTER #: **K-SPC-00355-I-CR** DATE IDENTIFIED: **04/05/88** TEAM/LOG: **RT/19**

TITLE: **PERSONNEL WORKING UNDER SUSPENDED LOAD FOR SRB PROCESSING (RPSF/VAB), ORBITER STACKING (VAB), SSME MAINTENANCE (VAB/PAD), AND MDD (SLF/CLS/KSC)**

CONFIGURATION DATA

RESP. ORGANIZATION: **SPC/LSOC**
LOCATION/STATION SETS: **20,23,29,31**
BASELINES: **389.00,400.15**
PROGRAM MODEL NUMBERS: **K60-0531,K60-0533,K60-0534,K60-0562,K60-0563**
MISSION EFFECTIVITY: **26+**
MISSION PHASE: **GROUND PROCESSING**
FLOW SEGMENTS: **LRR,MULTI,OPF,PAD,PLOAD,RPSF,SSME,VABM,VABO,VABS,VABT**

CR: **50404N**
SAA/SAR:
OMRSD:
OMI: **B5303,B5308,B5309,Q3008,S0004,T5149,V5044,V5E06,V9005**
ESR:
LCC:

HAZARD ANALYSIS DATA

REPORT STATUS: **CLOSED**

CLOSURE CLASS: **ACCEPTED RISK**

WORST CASE CAUSE: **CAUSE 1**
SEVERITY: **CATASTROPHIC**
LIKELIHOOD: **REMOTE**

HAZARD TYPE: **INDUSTRIAL**

PREPARED BY: **SPC**
MAIL CODE:

ANALYSIS TYPE: **OPERATING & SUPP.**

RISK MATRIX

HAZARD SEVERITY AND LIKELIHOOD OF OCCURRENCE WITH CONTROLS IN PLACE (SEE ASSOC'D CAUSE #)

LIKELIHOOD	MARGINAL	CRITICAL	CATASTR.
PROBABLE			
INFREQUENT			
REMOTE			1
IMPROBABLE			

-CONTROLLED
-ACCEPTED RISK
-UNACCEPTABLE

SEVERITY LEVELS

APPROVALS

SAFETY ENGINEER:	**RT-ENG**	DATE: **04/05/88**
CONTRACTOR SYSTEM/DESIGN ENGINEER:	_____	DATE: / /
CONTRACTOR SAFETY MANAGER (1):	**JOHN W. JAMBA**	DATE: **04/15/88**
CONTRACTOR SAFETY MANAGER (2):	**LEROY B. SPIVEY**	DATE: **04/15/88**
NASA SYSTEM ENGINEER:	_____	DATE: / /
NASA SAFETY MANAGER (1):	**J. ROBERT LANG**	DATE: **04/18/88**
NASA SAFETY MANAGER (2):	**J. A. THOMAS**	DATE: **04/23/88**

DATE APPROVED: CCB: **06/07/88** SSRP: **06/22/88** PRCB: / /

HAZARD #: **RT-ENG-1019** REVISION: REVISION DATE: / /
MASTER #: **K-SPC-00355-I-CR** DATE IDENTIFIED: **04/05/88** TEAM/LOG: **RT/19**

HAZARD DESCRIPTION:

Current KSC procedures for processing Solid Rocket Motors (SRMs) in the RPSF and VAB require personnel to work under a suspended load (Static). Personnel are also required to work under the Orbiter when it is lifted to the vertical position while in the VAB transfer aisle to remove landing gear pins prior to raising the gear. In the event an engine change or turbo pump change is required at the PAD, personnel would be working under the SSME area while the Orbiter is in the Vertical position on the FSS. Also, changing a turbo pump in the engine shop in the Low Bay at the VAB would require working under the engine pump when it is being installed/removed. Personnel are required to work under a suspended load when the Orbiter is mated to the Shuttle Carrier Aircraft (SCA) at DFRF and when the Orbiter is demated from the SCA at KSC to remove/install the landing gear pins. In the OPF, personnel are required to work under a suspended load during installation/removal of the Orbiter's manuevering system (OMS) POD. They are allowed under the load when the OMS post is within 6 inches of the ball socket.

Codes applicable to working under a suspended load are as follows:

A. Occupational Safety and Health Administration (OSHA) standards, 29CFR1910 subpart "N" 1986 edition.

a. 1910.179.n.3.vi (Overhead and Gantry Cranes) "The employer shall require that the operator avoid carrying the loads over people." (Dynamic Condition)
b. 1910.180.h.4.ii (Crawler, Locomotive and Truck Cranes) "No person should be permitted to stand or pass under a load on the hook." (Static Condition)

B. American National Standards Institute (ANSI) 1967, 1968, & 1983 editions read the same.

a. B30.2-3.2.3.e (Overhead and Gantry Cranes) "Loads should not be carried over people. (Dynamic Condition)
b. B30.5-3.2.1.4.e (Crawler, Locomotive and Truck Cranes) "Loads should not be carried over people. (Dynamic Condition)

C. NASA NSS/GO-1740 dated July 1982, (January 1988 Draft read the same).

a. Chapter 2 (Cranes) 2.7.14 "...Loads shall not be moved over people. (Dynamic Condition)

KSC/GP-1098E, Section 2.34, Ground Safety Plan, Volume 1 Safety Requirements contains requirements for a pretest briefing to be conducted just prior to the lift to ensure no open items, all systems and support personnel are ready to support. Loads are not raised, lowered or left suspended any longer than necessary to accomplish the task. In the event of a contingency or if a problem occurs during a lifting operation that prevents the completion of the task, within the shift in which it began, the load will be returned to the prelift position. However, presently there are two exceptions to this: 1) when the SRMs are suspended in the Rotating, Processing and Surge Facility (RPSF) - to be checked and inspected, and 2) during processing and stacking of the SRM segments in the VAB. In the RPSF, the air loads/fiber optic video inspection and ultrasonic inspection could require more than one work-shift. The tang inspection in the VAB requires approximately 12 hours to perform; depending on

HAZARD #: **RT-ENG-1019** REVISION: REVISION DATE: / /
MASTER #: **K-SPC-00355-I-CR** DATE IDENTIFIED: **04/05/88** TEAM/LOG: **RT/19**

HAZARD DESCRIPTION (CONTINUED):

the problems identified, such as an on-bonding problem, a SRM segment could be suspended in the VAB between 2 and 8 work-shifts.

While the above loads in the RPSF and VAB are suspended, two crane operators continuously monitor the load at their control stations. One crane operator is in the cab and the other crane operator is on the ground with the emergency stop switch.

HAZARD CAUSE(s):

1. (ACCEPTED RISK/CATASTROPHIC/REMOTE) - Failure of lifting devices: 200-ton crane in the RPSF, 250-ton crane in the VAB, 10-ton crane in the SSME shop, and the 140-ton 3900T Series 2 crane, the 800-ton TC-4000 Demag, the 250-ton HC-268 Linkbelt truck cranes, and MDD operations at the landing sites. Additional structural failures include the 250-ton hydraset and/or the SRM Four Point Lifting Beam. Any one of these failures could result in dropping the load.

HAZARD EFFECT(s):

Serious injury and/or loss of life to personnel.

ENGINEERING/SAFETY REQUIREMENTS:

KSC GP-1098E, Ground Safety Plan,
OSHA standard 29 CFR 1910, 1986 edition,
ANSI standard, 1983 edition,
NASA NSS/GO-1740, July 1982.

OMRSD REQUIREMENTS:

79K16835, "VARIANCE REQUEST MTI 24-80"

LAUNCH COMMIT CRITERIA:

None.

DETAILED ELIMINATION/CONTROL/ACCEPTED RISK RATIONALE:

At the present time there is not an acceptable method to perform SRM/Orbiter processing and stacking which would prevent personnel from temporarily working under a suspended load (static condition). The necessary operations include segment cleaning, inspection, greasing, measuring, insulation debond repairs, defect analysis, and other functions associated with preparing an SRM segment for mating/stacking to minimize the hazard and reduce the risk to an acceptable level. Each lifting device was thoroughly analyzed in accordance with NSTS 22206 and NSTS 22254. The 175-ton crane, the two 200-ton cranes in the RPSF, and the two 250-ton Bridge Cranes in the VAB completed Design Certification Reviews in January 1988. The only critical items identified pertain to the 250-ton VAB cranes. These critical items are covered in hazard report RT-ENG-1027. The 200-ton cranes in the RPSF are being modified to use DC motors and controls instead of AC to eliminate erratic Trolley and bridge movement.

HAZARD #: **RT-ENG-1019** REVISION: REVISION DATE: / /
MASTER #: **K-SPC-00355-I-CR** DATE IDENTIFIED: **04/05/88** TEAM/LOG: **RT/19**

DETAILED ELIMINATION/CONTROL/ACCEPTED RISK RATIONALE (CONTINUED):

At DFRF, the MDD is used to mate the Orbiter to the SCA. At contingency landing sites, the 800-ton TC-4000 Demag and 250-ton HC-268 Linkbelt truck cranes are used to mate the Orbiter to the SCA. The MDD is used to demate the Orbiter from the SCA after it arrives at KSC. No single failure points have been identified on the MDD or the mobile crane lifting devices. Also, the pinned landing gear to be cycled require a landing gear clear area (2 ft. forward, 2 ft. each side, 2 ft. aft and gear doors clear to ground). Clearance must be acknowledged prior to raising/lowering the landing gear and/or removing/installing the gear pins.

The SRM Four-Point Lifting Beam which is used for lifting the SRMs has a design safety factor of greater than 5:1 based on ultimate yield stress. The System Assurance Analysis for the 250-ton Hydraset SAA00KS01-001, identified only one seal which is a Category 2 critical item. The failure effect would be a maximum 1/2" hydraset lowering due to O-ring failure/bleed down. The hydraset structural design safety factor is greater than 5:1 based on ultimate yield stress. In accordance with NASA and Industry standards, initial proofload testing has been accomplished for all segment lifting system components. Annual load testing and scheduled maintenance programs are currently in place (79K Documents) for the KSC lifting hardware.

SAA09FY12-011, 10-ton Bridge Crane, for the Space Shuttle Main Engines (SSME) in the VAB low bay identified two single failure points. The Gear Reducer (Criticality 1) failure mode would require disengagement or structural failure, and the Solenoid Holding Brake (Criticality 1R) failure would be failure to engage, or failure of the Mechanical Load Brake. The four hazards identified include the lack of an upper limit switch (it has one upper switch) and the undetectable failure of either the electric brake and/or the mechanical brake. The fourth hazard pertains to personnel working under a suspended load during SSME turbo pump installation which is included in this accepted risk. A safety analysis was accomplished in SAA09PPF134-001 (preliminary), Hypergol Safing System, in the OPF and indicated no single failure points. SAA09FY01-001, 30-ton Bridge Crane, indicated no single failure points. An analysis on the 10-ton Hydraset was performed in SAA00KS01-002 and indicated 2 single failure points; the seals on the piston head and the seals on the up/down pump assembly. This analysis was a generic KSC center-wide review of all the hydraulic operated hydrasets.

These in-depth system analyses of the lifting devices insure that safety and operational personnel, as well as KSC management, are aware that all potential hazards have been identified and controls established to reduce the risk of working under a suspended load to an acceptable level.

All crane operators are certified and licensed per KMI 6430.4 Examination and Licensing of KSC Facility Crane Operators. Annual physicals for crane operators are required. To further minimize these hazards, only the personnel absolutely necessary to perform the operation are allowed to work near or under the suspended load.

All operations at KSC, with regard to working under a suspended load, are under "STATIC CONDITIONS" only. In no case is a load moved over personnel.

HAZARD #: **RT-ENG-1019** REVISION: REVISION DATE: / /
MASTER #: **K-SPC-00355-I-CR** DATE IDENTIFIED: **04/05/88** TEAM/LOG: **RT/19**

OMI/TPS/WAD VERIFICATION (CONTINUED):

Aft booster assembly on MLP
B5303 Connection of GEI umbilical plate to bottom of Aft skirt prior to set down of Aft booster assembly on MLP
B5303 Reshimming of HDP Spherical bearings to meet HDP load distribution requirements
B5303 Sighting of HDP Spherical bearing DELTA scales during reshimming operation
B5303 Cleaning of segment tang/capture feature for inspections
B5303 Cleaning of Aft end SRM insulation and J-Joint surfaces for inspections
B5303 Inspection of tang/capture feature (visual)
B5303 Inspection of SRM Aft end insulation, propellant relief flap and J-Joint surfaces (visual)
B5303 Air load/fiber optic video inspection of the capture feature-to-insulation bondline
B5303 Ultrasonic inspection of the insulation bondline behind the capture feature barrier O-ring groove
B5303 SRM tang J-Joint and relief flap profile measurements
B5303 V-2 volume filler installation in tang capture feature
B5303 O-ring and barrier seal installation during field joint mating
B5303 J-Seal abrading
B5303 J-Joint adhesive application
B5303 Final joint closeout inspection
B5303 Field joint assembly fixture (FJAF) installation
B5303 Field joint mating process
B5303 Forward assembly clevis cleaning
B5303 Forward assembly clevis inspection
B5303 Forward assembly clevis grease application
B5303 O-ring groove inspection

T-5149 ET OFFLOAD MOVE AND SECURE IN C/O CELL

ET transporter is driven out from under external tank (technicians steer transporter).

Disconnect Aft hardpoint- (2 persons under external tank raised slightly off transporter)

VAB ORBITER HANDLING/HOISTING

S0004 Slowly raise both 175-ton and 250-ton cranes until Orbiter main gear clears floor 6 inches +/- 4 inches.

S0004 Remove safety pin (G070-502453) from Nose Landing Gear Door and Ground Pin (GW70-500696-002) from Nose Landing Gear Lock Brace Assembly.

S0004 Remove safety pin (G070-502461-001) from left main gear door and Ground Pin (GW70-500696-003) from left main gear.

S0004 Remove safety pin (G070-502461-001) from right gear door and

HAZARD #: **RT-ENG-1019** REVISION: REVISION DATE: / /
MASTER #: **K-SPC-00355-I-CR** DATE IDENTIFIED: **04/05/88** TEAM/LOG: **RT/19**

SUMMARY ACCEPTANCE RATIONALE:

None.

OMI/TPS/WAD VERIFICATION:

The following OMIs contain steps and/or cautions to alert personel of the hazard and the requirement to minimize time under the suspended load:

RPSF

OMI NUMBER	TASK/OPERATION
B5308	Cleaning of segment tang/capture feature for inspections
B5308	Cleaning of Aft end SRM insulation and J-Joint surfaces for inspections
B5308	Inspection of tang/capture feature (visual)
B5308	Inspection of SRM Aft end insulation, propellant relief flap and J-Joint surfaces (visual)
B5308	Air load/fiber optic video inspection of the capture feature-to-insulation bondline
B5308	Ultrasonic inspection of the insulation bondline behind the capture feature barrier O-ring groove
B5308	Installation/removal of protective pie-shapes over forward insulation and propellant surfaces of SRM while handling ring/end cover assembly is suspended above
B5308	Mating of Aft skirt to RPSF build-up stand support post ball fittings (cleaning surfaces)
B5308	Installation of protective velostat sheeting on tang aft surfaces
B5308	Inspection of SRM leak ports
B5308	Application of grease to bare metal surfaces of tang/capture feature
B5309	Cleaning of SRM Aft segment tang
B5309	Inspection of SRM Aft segment tang and crotch
B5309	Application of grease to Aft segment tang
B5309	Positioning of external tank attach (ETA) Ring on Aft segment stubs
B5309	Installation/removal of protective pie-shapes over forward insulation and propellant surfaces of SRM while handling ring/end cover assembly is suspended above
B5309	Mating of Aft skirt to SRM transportation pallet support post ball fittings.
B5309	Installation of O-ring prior to segment mate. (Segment suspended 3' above another segment. Technicians hands/arms under suspended load).

VAB

(B5303 work)	Repairs of defects on SRM insulation, J-Joint, or metal parts in (SRM or FWD ASSY) - not used for STS-26R.
B5303	Cleaning Aft skirt shoes and HDP bearings prior to set down of

HAZARD #: **RT-ENG-1019** REVISION: REVISION DATE: / /
MASTER #: **K-SPC-00355-I-CR** DATE IDENTIFIED: **04/05/88** TEAM/LOG: **RT/19**

OMI/TPS/WAD VERIFICATION (CONTINUED):

Ground Pin from the right main gear.

S0004 Inspect tile on and around landing gear doors.

SSME LRU COMPONENT INSTALLATION/REMOVAL IN VAB - LOW BAY

V5E06 Lifting operations in SSME area to remove/install SSME turbo pump.

ORBITER AND SCA MATE/DEMATE

S5022 Orbiter SCA mate/demate at DFRF/KSC

S5044 Orbiter SCA mate/demate at contingency landing sites.

V9005VL1 Hydraulic standard power up/power down for raising/lowering landing gear.

V5011 Q3199 OMS POD removal/installation in the OPF.

SAA REFERENCES:

SAA09FY012-005,, "SAA09FY012-004"

FMEA/CIL REFERENCES:

None.

BACKGROUND:

The Occupational Safety and Health Administration (OSHA) has stated that OSHA will not issue waivers to authorize the exposure of employees working beneath suspended loads. OSHA also states that any work procedures requiring such exposure are done so at the risk of the employer. The following reduces this risk to an acceptable level:

a. All GSE developed for processing and inspection is designed to preclude the exposure of employees under suspended loads where ever possible.

b. All inspection techniques are developed with proper inspection tools that would eliminate inspection procedures under suspended loads where ever possible.

c. In those cases where it is not feasible to eliminate employee exposure working under a suspended load, an appropriate risk assessment must be made to assure the controls employed and the risk acceptance rationale is approved by management.

INTERFACES:

None.

HAZARD #: **RT-ENG-1019** REVISION: REVISION DATE: / /
MASTER #: **K-SPC-00355-I-CR** DATE IDENTIFIED: **04/05/88** TEAM/LOG: **RT/19**

STATUS OF OPEN WORK:

The current Operations and Maintenance Requirements Specifications (OMRS) for the 200-ton crane in the RPSF and the 250-tone crane in the VAB are 79K27158 and 79K16835. These documents are currently under review and the requirements for the OMRSD File VI are being prepared.

REMARKS:

6/22/88 - SSRP changed to Industrial. This HR was neither approved nor disapproved with CR 50404N, but left to KSC to control as an Industrial hazard. This hazard will be maintained in the KSC Hazard Data Base. Status changed to closed. "Damage to flight hardware" deleted from hazard effect data element.

2/17/89 - Added O-ring inspectoscope operation and references to cranes and OMIs used for Orbiter/SCA mate/demate at DFRF/KSC/CLS. Also added reference to hazard report RT-ENG-1027, which covers the 250-ton VAB crane single failure points.

HAZARD #: **SPC-5210-018-89** REVISION: REVISION DATE: / /
MASTER #: **K-SPC-00000-S-HT** DATE IDENTIFIED: **03/28/89** TEAM/LOG: **POST/94**

TITLE: **DAMAGE TO PAYLOAD AND/OR PAYLOAD CANISTER DURING PAD-B PCR 90-TON HOIST OPERATIONS**

CONFIGURATION DATA

RESP. ORGANIZATION: **LSOC**
LOCATION/STATION SETS: **23**
BASELINES: **422.00**
PROGRAM MODEL NUMBERS: **K61-0168**
MISSION EFFECTIVITY: **36+**
MISSION PHASE: **GROUND PROCESSING**
FLOW SEGMENTS: **PAD**

CR: **50414H**
SAA/SAR: **SAA09FY05-001**
OMRSD:
OMI: **M3160,Q3437,Q6325**
ESR:
LCC:

HAZARD ANALYSIS DATA

REPORT STATUS: **CLOSED**

CLOSURE CLASS: **CONTROLLED**

WORST CASE CAUSE: **NONE**
SEVERITY: **CRITICAL**
LIKELIHOOD: **IMPROBABLE**

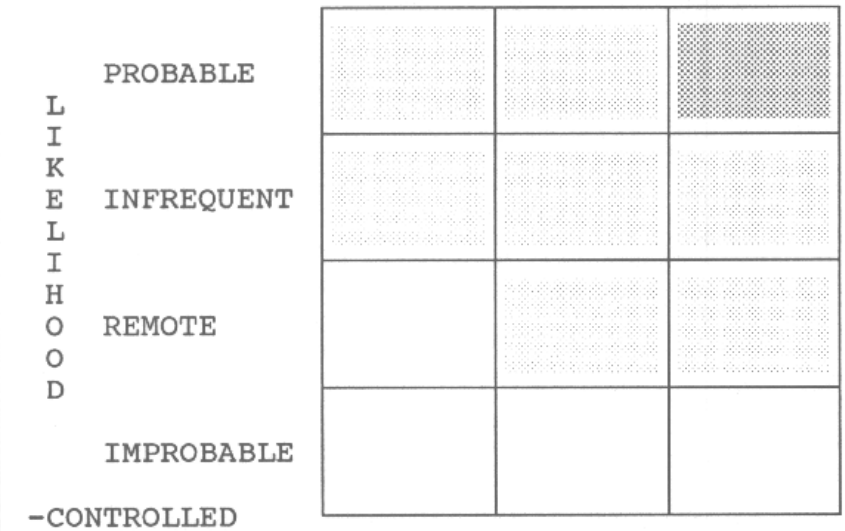
HAZARD TYPE: **SHUTTLE**

PREPARED BY: **SPC**
MAIL CODE:

ANALYSIS TYPE: **OPERATING & SUPP.**

RISK MATRIX

HAZARD SEVERITY AND LIKELIHOOD OF OCCURRENCE WITH CONTROLS IN PLACE (SEE ASSOC'D CAUSE #)



-CONTROLLED
-ACCEPTED RISK
-UNACCEPTABLE

APPROVALS

SAFETY ENGINEER:	**J. YARBORO**	DATE: **04/07/89**
CONTRACTOR SYSTEM/DESIGN ENGINEER:	_____	DATE: / /
CONTRACTOR SAFETY MANAGER (1):	**J. R. HANKINS**	DATE: **12/20/89**
CONTRACTOR SAFETY MANAGER (2):	**DAVID T. HOGGE**	DATE: **12/21/89**
NASA SYSTEM ENGINEER:	_____	DATE: / /
NASA SAFETY MANAGER (1):	**RONALD R. GILLETT**	DATE: **12/21/89**
NASA SAFETY MANAGER (2):	**J. ROBERT LANG**	DATE: **12/21/89**

DATE APPROVED: CCB: **01/04/90** SSRP: **01/18/90** PRCB: **02/06/90**

HAZARD #: **SPC-5210-018-89** REVISION: REVISION DATE: / /
MASTER #: **K-SPC-00000-S-HT** DATE IDENTIFIED: **03/28/89** TEAM/LOG: **POST/94**

HAZARD DESCRIPTION:

The 90-Ton, base-mounted Payload Canister Hoist is installed in the Hoist Equipment Room at the 212-foot level of the Rotating Service Structure (RSS) at Pad-B. The primary operational use for the 90-Ton hoist is to raise the payload canister and its associated payload for payload off-loading into the Payload Changeout Room. The hoist is operated by an AC motor acting through a gear reducer to a single drum with dual reeving.
The dual reeving system consists of the upper sheave nest and lower block made of alternating large and small diameter sheaves. Wire rope from the drum alternately crosses from one sheave to the next sheave of the same diameter, and eventually dead ends through a spelter socket to an equalizer bar opposite the wire rope's original starting point on the first high speed sheave. The equalizer bar distributes the load evenly between the two wire ropes by pivoting about a rocker pin. With this configuration, two separate wire ropes are provided which are capable of supporting the load if the other rope fails.

During hoisting operations, the wire ropes are spooled onto the drum. The wire rope drum is double reeved; each rope is spooled with ten layers on each drum half. The drum is equipped with grooving to provide proper rope spooling. As the load is raised, abnormal spooling occurs at about the seventh wire rope layer resulting in the length of the two ropes becoming uneven. As the uneven spooling continues, the equalizer bar begins to tilt from its horizontal position to a slanted position (approximately 6-8 inches of rotation [15 degrees] at the end of the bar) trying to distribute the load evenly between the two wire ropes. If the uneven spooling is allowed to continue, the equalizer bar will move further until one of the spelter sockets begins to bear against the under surface of the equalizer bar, thus, kinking the wire rope and possibly damaging the spelter connection. Upon futher travel, it is possible for the equalizer bar to reach the vertical position, transferring all the load to one rope. This abnormal condition could result in damage to the hoist mechanism and/or hardware.

HAZARD CAUSE(s):

1) Uneven wire rope spooling on hoist drum.
2) Wire rope (structural) failure.

HAZARD EFFECT(s):

Possible damage to hoist mechanism and/or payload canister/payload.

ENGINEERING/SAFETY REQUIREMENTS:

NSS-GO/1740.9.

OMRSD REQUIREMENTS:

None.

LAUNCH COMMIT CRITERIA:

None.

HAZARD #: **SPC-5210-018-89** REVISION: REVISION DATE: / /
MASTER #: **K-SPC-00000-S-HT** DATE IDENTIFIED: **03/28/89** TEAM/LOG: **POST/94**

DETAILED ELIMINATION/CONTROL/ACCEPTED RISK RATIONALE:

1) OMI Q3437, Operating Instructions for 90-Ton Hoist, RSS, Pre-ops Setup, sequence 01-000 (prior to each hoist operation) requires a walkdown inspection of the entire hoist mechanism to ensure operational readiness of wire ropes, drum and block assemblies, and equalizer sheaves. Sequence 01-009 requires the hoist operator to establish communications with each observer involved with hoisting operations, which also includes the emergency stop operator in the forward reaction control room (207-foot level), the emergency stop operator (130-foot level-Side 2), the Pad level observer, and hoist room observer (207-foot level), who observes the hoist drum spooling.
OMI M3160, Payload Canister Hoisting Operations, Launch Pad A/B, requires OIS communications be maintained between all observers during hoisting operations. Emergency procedures require observers to halt hoisting operations if any anomalies occur.
2) OMI Q6325, Maintenance Instructions for the 90-Ton Payload Canister Hoist, Pad B, provides for monthly wire rope inspections and an annual 100% rated load test of the hoist. The wire rope safety factor is 5 to 1. Balanced dual reeving provides 2 separate ropes, each capable of supporting the load (dual failure required).

SUMMARY ACCEPTANCE RATIONALE:

None.

OMI/TPS/WAD VERIFICATION:

OMIs Q3437, Q6325, and M3160.

SAA REFERENCES:

SAA09FY05-001, "90-TON HOIST PAD-B"

FMEA/CIL REFERENCES:

None.

BACKGROUND:

The 90-Ton Payload Canister Hoist at Pad-B was modified to meet the July 1982 version of NSS/GO-1740.9 (NASA Safety Standard for Lifting Devices and Equipment), which required that hoists lifting critical flight hardware be equipped with two wire ropes. The July 1988 revision of NSS/GO-1740.9 does not require dual wire ropes for critical hoists. This condition does not exist for the Pad-A 90-Ton hoist, which is single reeved.

INTERFACES:

None.

STATUS OF OPEN WORK:

None.

HAZARD #: **SPC-5210-018-89** REVISION: REVISION DATE: / /
MASTER #: **K-SPC-00000-S-HT** DATE IDENTIFIED: **03/28/89** TEAM/LOG: **POST/94**

REMARKS:

1/04/90 - This hazard report was approved by the Joint Launch and Landing Level III Configuration Control Board/SPC Risk Review Board.

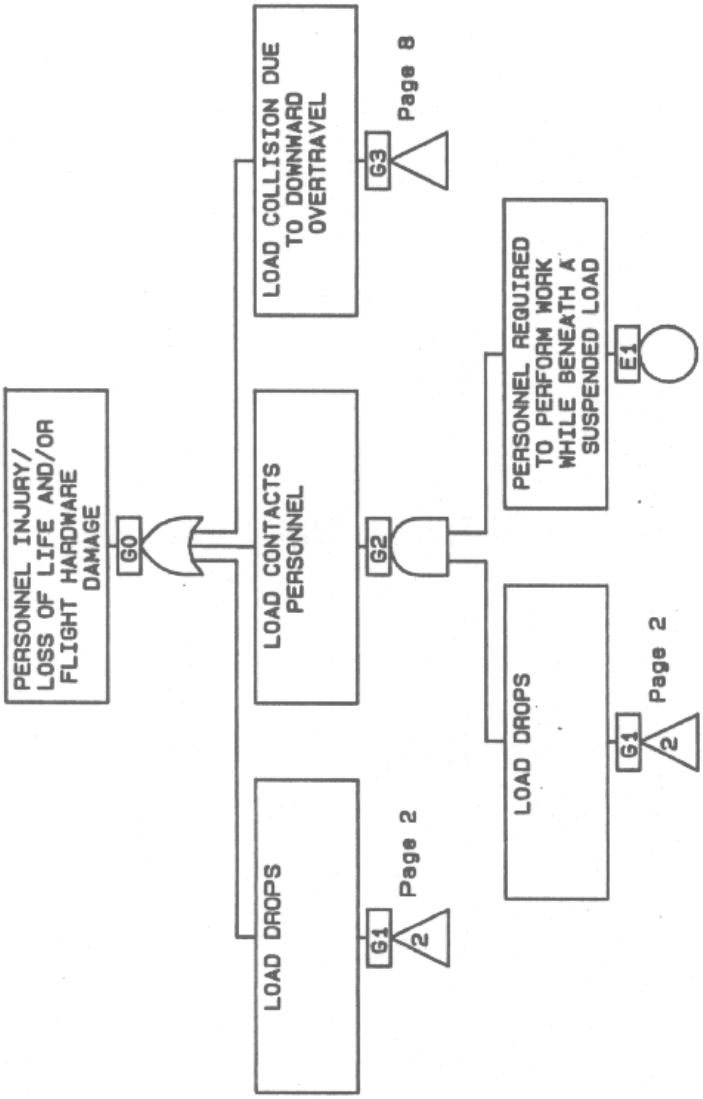
1/18/90 - Presented to and approved by the SSRP.

1/25/90 - Approved by the Level II PRCB.

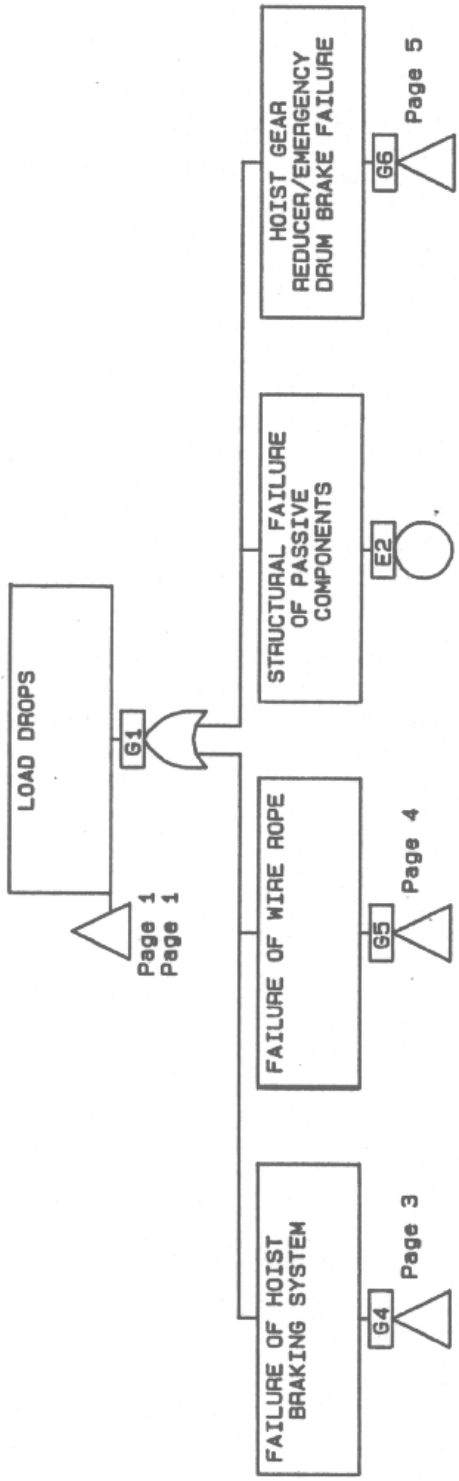
2/06/90 - Approved by the Level I PRCB.

7.4 FAULT TREE ANALYSIS

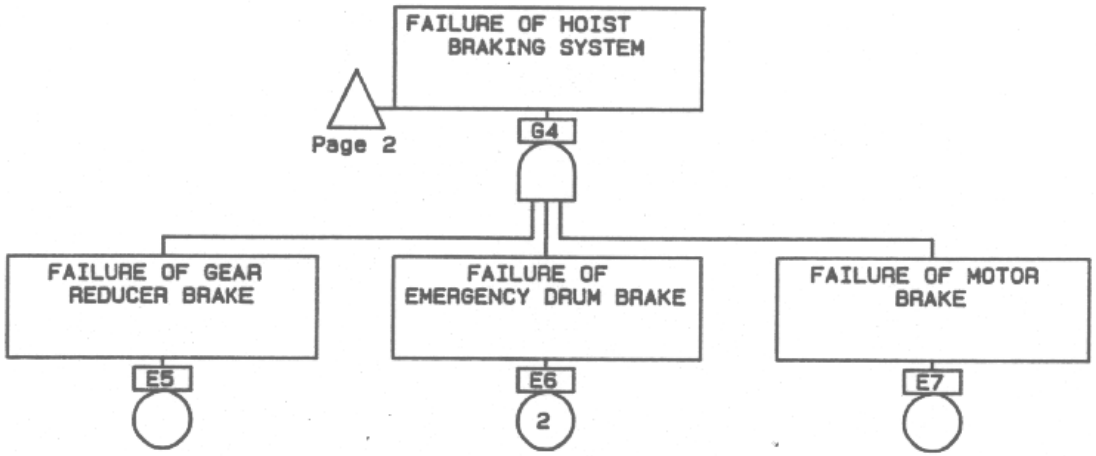
A qualitative fault tree analysis was developed with the top event identified as "Injury/Loss of Life to personnel or Flight Hardware Damage". Potential hazardous conditions leading to the top event have been assessed on the Hazard Analysis Worksheets located in Section 7.5.



90 TON HOIST, PAD B PCR | A: 90TON1.CAF | 11/17/93 | Page 1

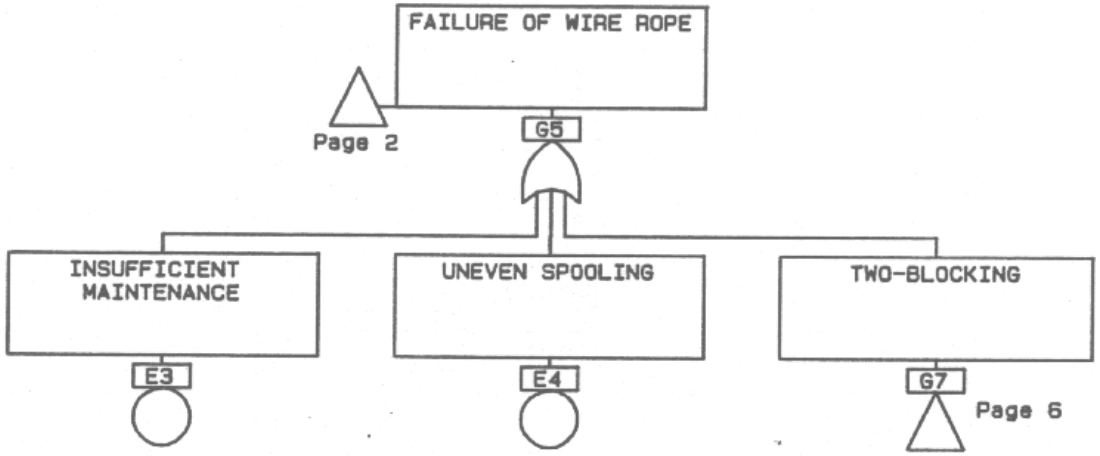


90 TON HOIST, PAD B PCR | A: 90TON1.CAF | 11/18/93 | Page 2



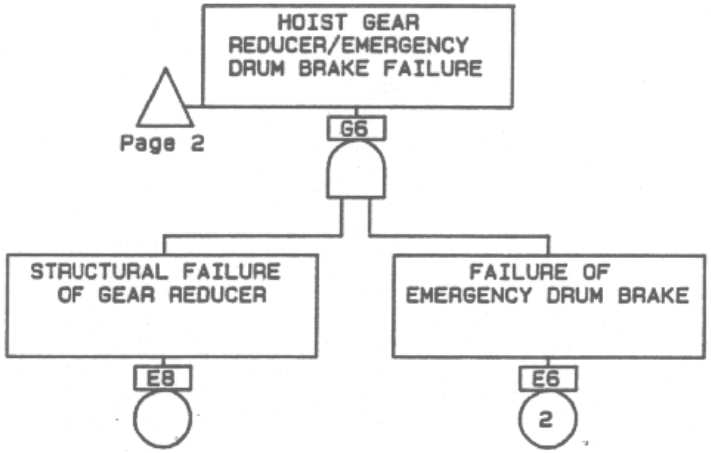
90 TON HOIST, PAD B PCR	A: 90TON1.CAF	11/17/93	Page 3

SAA09FTB3-003
REV. A



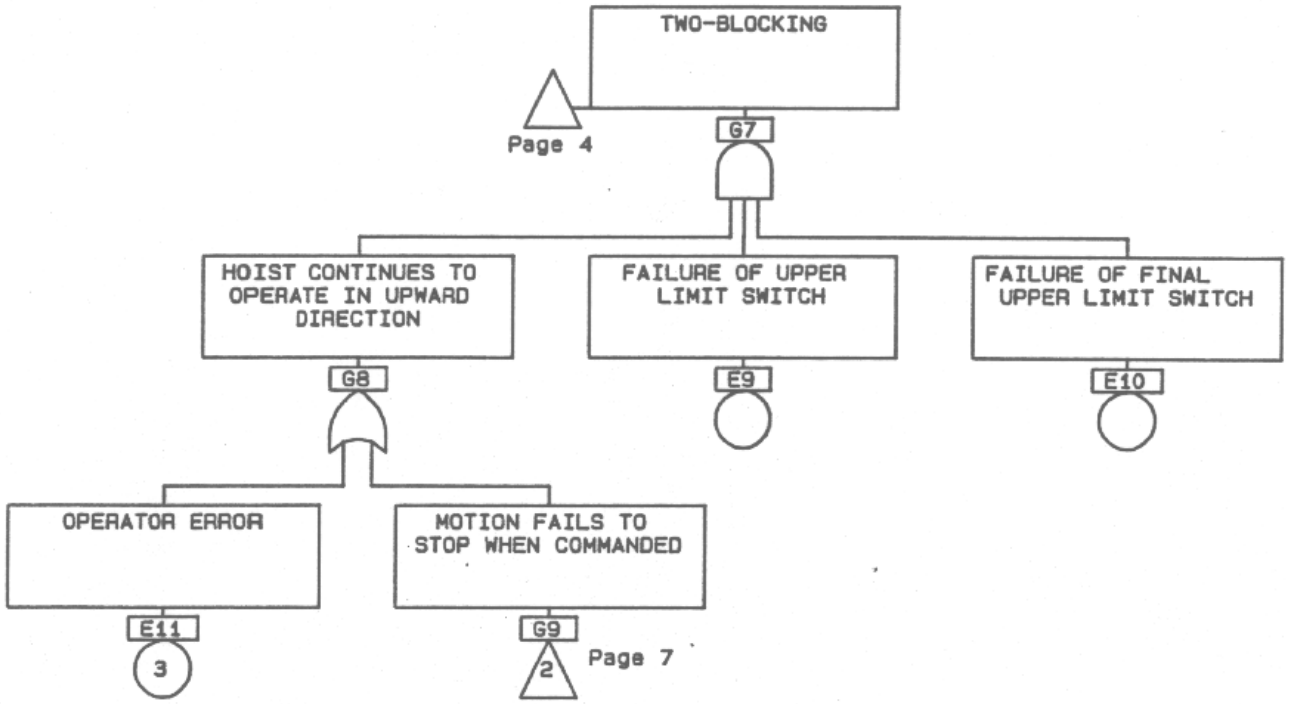
90 TON HOIST, PAD B PCR	A: 90TON1.CAF	11/18/93	Page 4

SAA09FTB3-003
REV. A



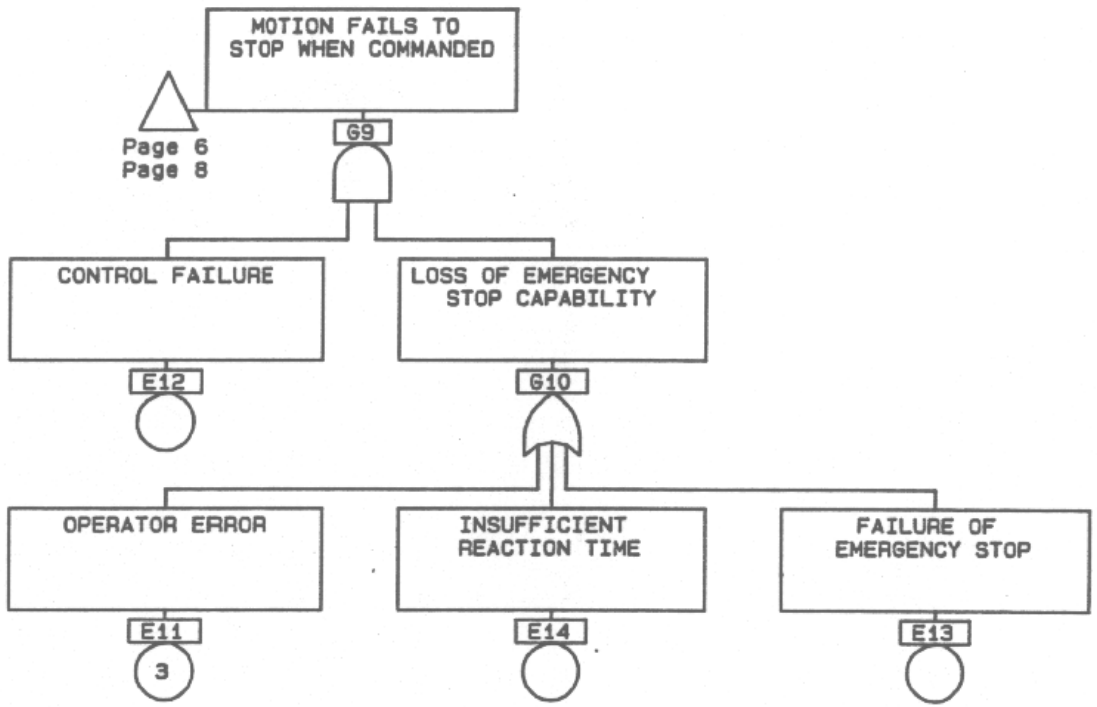
90 TON HOIST, PAD B PCR	A: 90TON1.CAF	11/17/93	Page 5

SAA09FTB3-003
REV. A



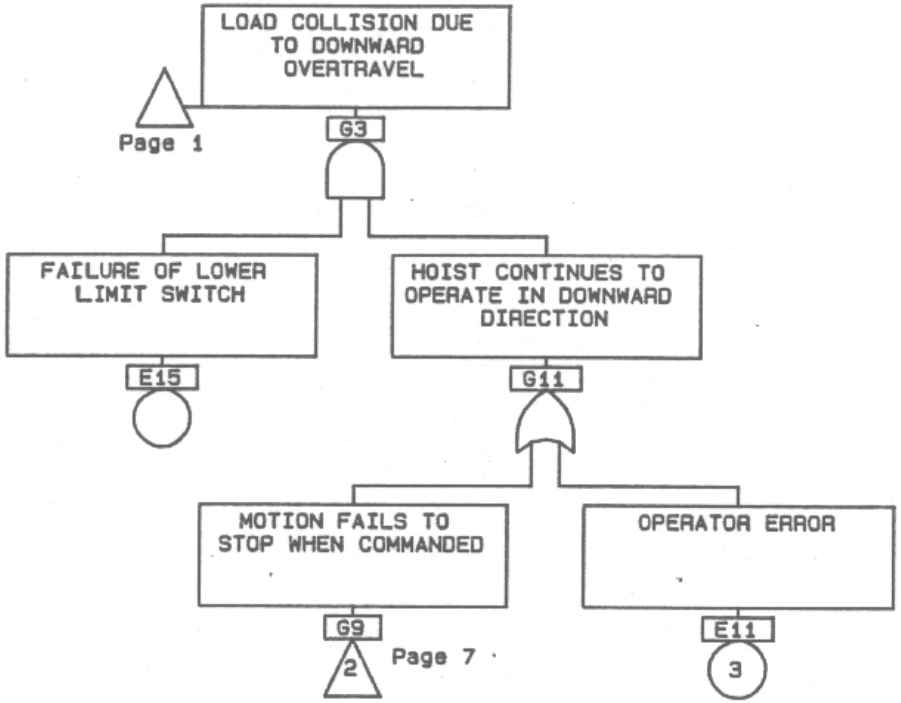
90 TON HOIST, PAD B PCR	A: 90TON1.CAF	11/18/93	Page 6

SAA09FTB3-003
REV. A



90 TON HOIST, PAD B PCR	A: 90TON1.CAF	11/17/93	Page 7

SAA09FTB3-003
REV. A



90 TON HOIST, PAD B PCR	A: 90TON1.CAF	11/18/93	Page 8

SAA09FTB3-003
REV. A

7.5 HAZARD ANALYSIS WORKSHEETS

The Hazard Analysis Worksheets were prepared in conjunction with the fault tree analysis depicting the specific hazardous conditions, causes, effects, safety/engineering requirements, and hazard elimination/control provisions. Worksheets are attached.

Table 6 (Page 1 of 6). **HAZARD ANALYSIS WORKSHEETS**

Phase/Mode Function 90-TON HOIST

Task/Operation or Facility PAD B PCR

Date DECEMBER 1993

Prepared by G. WHITMORE, LSOC 52-11

HAZARDOUS CONDITION	HAZARD CAUSE	HAZARD EFFECT	SAFETY/ENGINEERING REQUIREMENTS	HAZARD ELIMINATION/CONTROL PROVISIONS
G1 LOAD DROPS	G4 FAILURE OF HOIST BRAKING SYSTEM	G0 PERSONNEL INJURY/LOSS OF LIFE OR FLIGHT HARD-WARE DAMAGE.	G1 DEVELOPED UNDER HAZARDOUS COLUMN G4.	G1 DEVELOPED UNDER HAZARDOUS COLUMN G4.
	OR			
	G5 FAILURE OF WIRE ROPE		DEVELOPED UNDER HAZARDOUS COLUMN G5.	DEVELOPED UNDER HAZARDOUS COLUMN G5.
	OR			
	E2 STRUCTURAL FAILURE OF PASSIVE COM-PONENTS		E2 NSS/GO 1740.9B, SECTION 402, PROOFLOAD AND ANNUAL LOAD TEST REQUIRED; SECTION 403 FORMAL PERIODIC INSPECTION REQUIRED; SECTION 404 PREVENTATIVE MAINTENANCE REQUIRED.	E2 FORMAL PERIODIC MAINTENANCE AND INSPECTION INCLUDES SEMI-ANNUAL INSPECTION OF HOIST DRUMS AND SHEAVES, HOIST OPERATIONAL CHECK, ANNUAL LOAD TEST AND HOIST MAGNAFLUX CHECK PER OMI Q6325. PRE-OPERATION SETUP INCLUDES INSPECTION OF HOIST HOOKS, SHEAVES, DRUMS, HOIST FRAME AND STEEL FOUNDATION AND STRUCTURE FOR DAMAGE, MISSING PARTS, DEFORMATIONS, CRACKS, ETC. PER OMI Q3437.
	OR			
	G6 HOIST GEAR REDUCER/ BAND BRAKE FAILURE		G6 DEVELOPED UNDER HAZARDOUS COLUMN G6.	G6 DEVELOPED UNDER HAZARDOUS COLUMN G6.
G2 LOAD CON-TACTS PER-SONNEL	G1 LOAD DROPS	G0 PERSONNEL INJURY/LOSS OF LIFE AND/OR FLIGHT HARD-WARE DAMAGE.	G1 DEVELOPED UNDER HAZARDOUS COLUMN G1.	G1 DEVELOPED UNDER HAZARDOUS COLUMN G1.

Table 6 (Page 2 of 6). **HAZARD ANALYSIS WORKSHEETS**

Phase/Mode Function 90-TON HOIST

Task/Operation or Facility PAD B PCR

Date DECEMBER 1993

Prepared by G. WHITMORE, LSOC 52-11

HAZARDOUS CONDITION	HAZARD CAUSE	HAZARD EFFECT	SAFETY/ENGINEERING REQUIREMENTS	HAZARD ELIMINATION/CONTROL PROVISIONS
	AND E1 PERSONNEL REQUIRED TO PERFORM WORK WHILE BENEATH A SUSPENDED LOAD.		E1 NSS/GO 1740.9B, SECTION 406 (6), LOADS SHALL NOT BE MOVED OVER PEOPLE. GP1098F, 2.36, A LOAD SHALL NOT BE LIFTED, SUSPENDED, OR TRANSPORTED OVER PERSONNEL, FLIGHT HARDWARE OR CRITICAL GSE.	E1 PERSONNEL WARNED AGAINST REQUIREMENTS FOR PERFORMING WORK BENEATH A SUSPENDED LOAD. ONLY MOVE CRITICAL PERSONNEL ALLOWED UNDER A SUSPENDED LOAD. PERSONNEL ARE BENEATH SUSPENDED LOAD ONLY FOR AMOUNT OF TIME NEEDED TO COMPLETE TASK. PRE-OPERATIONAL INSPECTION AND TEST PERFORMED PRIOR TO LIFT PER OMI Q3437. PERIODIC INSPECTION AND MAINTENANCE INCLUDING OPERATIONAL TEST AND ANNUAL LOAD TEST PERFORMED PER Q6325. REFERENCE HAZARD REPORT RT-ENG-1019.
G4 FAILURE OF HOIST BRAKING SYSTEM	E5 FAILURE OF GEAR REDUCER BRAKE	G1 LOAD DROPS	E5, E6, E7 NSS/GO 1740.9B, SECTION 404 (f)(3) , FOR CRITICAL CRANES, TWO MEANS OF BRAKING, EACH CAPABLE OF BRINGING A RATED LOAD TO ZERO SPEED AND HOLDING IT, SHALL BE PROVIDED; SECTION 402 (5) OPERATIONAL TEST OF BRAKES REQUIRED; SECTION 403, FORMAL PERIODIC INSPECTION OF BRAKING SYSTEMS REQUIRED.	E5, E6, E7 OMI Q6325 ANNUALLY INSPECTS THE GEAR REDUCER FOR PITTING, UNEVEN WEAR, AND UNIFORM DISTRIBUTION OF LUBRICANT. OMI Q6325 QUARTERLY INSPECTS THE GEAR REDUCER FOR CORROSION, DAMAGE, AND OIL LEAKAGE.
	AND E6 FAILURE OF BAND BRAKE		FILE VI OMRSD GRWFHTRAO.005, STATES TO PERFORM A BRAKE LOAD TEST FOR TWO HOLDING BRAKES AND ONE DRUM BRAKE TO PROVIDE ASSURANCE THAT EACH BRAKE INDEPENDENTLY HOLDS THE RATED LOAD FOR THE 90-TON HOIST.	OMI Q3437 INSPECTS THE BAND BRAKE ASSEMBLY FOR EVIDENCE OF DISTORTION, CRACKED WELDS, AND LOOSE BOLTED CONNECTIONS WITHIN 30 DAYS OF A CANISTER HOISTING OPERATION. OMI Q6325 PERFORMS AN ANNUAL LOAD TEST WHICH INDEPENDENTLY TESTS ALL THREE BRAKES AT RATED LOAD. OMI Q6325 ANNUALLY CHECKS THE BRAKE LININGS FOR WEAR AND VERIFIES PROPER BRAKE LINING CLEARANCE.
	AND E7 FAILURE OF MOTOR BRAKE			

Table 6 (Page 3 of 6). **HAZARD ANALYSIS WORKSHEETS**

Phase/Mode Function 90-TON HOIST

Task/Operation or Facility PAD B PCR

Date DECEMBER 1993

Prepared by G. WHITMORE, LSOC 52-11

HAZARDOUS CONDITION	HAZARD CAUSE	HAZARD EFFECT	SAFETY/ENGINEERING REQUIREMENTS	HAZARD ELIMINATION/CONTROL PROVISIONS
G5 FAILURE OF WIRE ROPE	E3 INSUFFICIENT MAINTENANCE	G1 LOAD DROPS	E3 NSS/GO 1740.9B, SECTION 403(a), STATES TO INSPECT THE WIRE ROPE PERIODICALLY PAYING PARTICULAR ATTENTION TO SIGNS OF DETERIORATION AND DAMAGE.	E3 OMI Q3437 PERFORMS A WIRE ROPE INSPECTION/LUBRICATION PRIOR TO CANISTER HOISTING OPERATION. THIS INSPECTION IS PERFORMED WITHIN 30 DAYS OF A CANISTER HOIST OPERATION.
	OR			
	E4 UNEVEN SPOOLING		E4 NSS/GO 1740.9B, SECTION 406(a), STATES THAT ONLY CERTIFIED OPERATORS SHALL BE AUTHORIZED TO USE/OPERATE LIFTING DEVICES, INCLUDING HOIST OPERATIONS WHERE PROCEDURAL CONTROLS CAN BE PROVIDED IN A TECHNICAL OPERATING PROCEDURE.	E4 OMI M3160 REQUIRES OIS COMMUNICATIONS BE MAINTAINED BETWEEN ALL OBSERVERS DURING HOISTING OPERATIONS. EMERGENCY PROCEDURES OBSERVERS TO COMMAND "EMERGENCY STOP" OVER OIS CHANNEL, IF THEY ARE ABOUT TO WITNESS ANY ANOMALIES.
	OR		G7 DEVELOPED UNDER HAZARDOUS COLUMN G7.	G7 DEVELOPED UNDER HAZARDOUS COLUMN G7.
	G7 TWO-BLOCKING			
G6 HOIST GEAR REDUCER/ BAND BRAKE FAILURE	E8 STRUCTURAL FAILURE OF GEAR REDUCER	G1 LOAD DROPS	E8, E6 NSS/GO 1740.9B, SECTION 403(d), STATES THAT FORMAL INSPECTIONS SHALL BE PERFORMED AT VARYING INTERVALS, DEPENDING ON ACTIVITY, SEVERITY OF SERVICE, ENVIRONMENT, AND CRITICALITY.	E8 OMI Q6325 ANNUALLY INSPECTS THE GEAR REDUCER FOR PITTING, UNEVEN WEAR, AND UNIFORM DISTRIBUTION OF LUBRICANT. OMI Q6325 QUARTERLY INSPECTS THE GEAR REDUCER FOR CORROSION, DAMAGE, AND OIL LEAKAGE.
	AND			
	E6 FAILURE OF BAND BRAKE			E6 OMI Q3437 INSPECTS THE BAND BRAKE ASSEMBLY FOR EVIDENCE OF DISTORTION, CRACKED WELDS, AND LOOSE BOLTED CONNECTIONS WITHIN 30 DAYS OF A CANISTER HOISTING OPERATION. OMI Q6325 PERFORMS AN ANNUAL LOAD TEST WHICH INDEPENDENTLY TESTS ALL THREE BRAKES AT RATED LOAD. OMI Q6325 ANNUALLY CHECKS THE BRAKE LININGS FOR WEAR AND VERIFIES PROPER BRAKE LINING CLEARANCE.

Table 6 (Page 4 of 6). **HAZARD ANALYSIS WORKSHEETS**

Phase/Mode Function 90-TON HOIST

Task/Operation or Facility PAD B PCR

Date DECEMBER 1993

Prepared by G. WHITMORE, LSOC 52-11

HAZARDOUS CONDITION	HAZARD CAUSE	HAZARD EFFECT	SAFETY/ENGINEERING REQUIREMENTS	HAZARD ELIMINATION/CONTROL PROVISIONS
G7 TWO-BLOCKING	G8 HOIST CONTINUES TO OPERATE IN UPWARD DIRECTION	G5 FAILURE OF WIRE ROPE	DEVELOPED UNDER HAZARDOUS COLUMN G8.	DEVELOPED UNDER HAZARDOUS COLUMN G8.
	AND			
	E9 FAILURE OF UPPER LIMIT SWITCH		E9, E10 NSS/GO 1740.9B, SECTION 401 (7), FOR CRITICAL CRANES, DUAL UPPER LIMIT SWITCHES ARE REQUIRED; SECTION 402 (e)(3), OPERATIONAL TEST OF LIMIT SWITCHES REQUIRED.	E9, E10 PRE-OPERATION INSPECTION AND OPERATIONAL CHECK OF HOIST LIMIT SWITCH PRIOR TO EACH USE PER OMI Q3437. OPERATOR AND OBSERVERS PROVIDED WITH EMERGENCY STOP CAPABILITY AND INSTRUCTED TO HALT HOISTING OPERATIONS SHOULD ANOMALY OCCUR PER OMI M3160.
	AND			
	E10 FAILURE OF FINAL UPPER LIMIT SWITCH			
G8 HOIST CONTINUES TO OPERATE IN UPWARD DIRECTION	E11 OPERATOR ERROR	G7 TWO-BLOCKING	E11 NSS/GO 1740.9B, SECTION 403(a) STATES THAT ONLY CERTIFIED OPERATORS SHALL BE AUTHORIZED TO USE/OPERATE LIFTING DEVICES, INCLUDING HOIST OPERATIONS WHERE PROCEDURAL CONTROLS CAN BE PROVIDED IN A TECHNICAL OPERATING PROCEDURE.	E11 OMI M3160 REQUIRES HOIST OPERATORS TO HAVE CERTS 019-1 "FIXED CRANES/HOIST CONTROL," 091-1 "FIXED CRANES/HOIST E-STOP OBSERVERS," 093 "PENDANT CONTROLLED/USER-OPERATED CRANES/HOISTS OPERATOR" AND 094-1 "FIXED CRANES/HOISTS OPERATOR" TO OPERATE THE 90-TON HOIST.
	OR			
	G9 MOTION FAILS TO STOP WHEN COMMANDED		DEVELOPED UNDER HAZARDOUS COLUMN G9.	DEVELOPED UNDER HAZARDOUS COLUMN G9.

Table 6 (Page 5 of 6). **HAZARD ANALYSIS WORKSHEETS**

Phase/Mode Function 90-TON HOIST

Task/Operation or Facility PAD B PCR

Date DECEMBER 1993

Prepared by G. WHITMORE, LSOC 52-11

HAZARDOUS CONDITION	HAZARD CAUSE	HAZARD EFFECT	SAFETY/ENGINEERING REQUIREMENTS	HAZARD ELIMINATION/CONTROL PROVISIONS
G9 MOTION FAILS TO STOP WHEN COMMANDED	E12 CONTROL FAILURE	G8 HOIST CONTINUES TO OPERATE IN UPWARD DIRECTION		E12 PRE-OPERATION INSPECTION AND OPERATIONAL TEST OF HOIST CONTROLS PRIOR TO EACH USE PER OMI Q3437. ANNUAL INSPECTION OF HOIST CONTROL CONSOLE PER OMI Q6325. OPERATOR AND OBSERVERS PROVIDED WITH EMERGENCY STOP CAPABILITY AND INSTRUCTED TO HALT HOIST MOVEMENT SHOULD AN ANOMALY OCCUR PER OMI M3160.
		OR		
		G11 HOIST CONTINUES TO OPERATE IN DOWNWARD DIRECTION	DEVELOPED UNDER HAZARDOUS COLUMN G10.	
	AND			
	G10 LOSS OF EMERGENCY STOP CAPABILITY			
G10 LOSS OF EMERGENCY STOP CAPABILITY	E11 OPERATOR ERROR	G9 MOTION FAILS TO STOP WHEN COMMANDED	E11 NSS/GO 1740.9B, SECTION 403(a), STATES THAT ONLY CERTIFIED OPERATORS SHALL BE AUTHORIZED TO USE/OPERATE LIFTING DEVICES, INCLUDING HOIST OPERATIONS WHERE PROCEDURAL CONTROLS CAN BE PROVIDED IN A TECHNICAL OPERATING PROCEDURE.	E11 OMI M3160 REQUIRES HOIST OPERATORS TO HAVE CERTS 019-1 "FIXED CRANES/HOIST CONTROL," 091-1 "FIXED CRANES/HOIST E-STOP OBSERVERS," 093 "PENDANT CONTROLLED/USER-OPERATED CRANES/HOISTS OPERATOR" AND 094-1 "FIXED CRANES/HOISTS OPERATOR" TO OPERATE THE 90-TON HOIST.
	OR			
	E14 INSUFFICIENT REACTION TIME		E14 NSS/GO 1740.9B, SECTION 401 (g)(5) , REMOTE EMERGENCY STOP SHALL BE PROVIDED WHEN NEEDED.	E14 OBSERVERS PROVIDED WITH REMOTE EMERGENCY STOP AND INSTRUCTED PER OMI Q3437 TO HALT HOIST MOVEMENT SHOULD AN ANOMALY OCCUR.

Table 6 (Page 6 of 6). **HAZARD ANALYSIS WORKSHEETS**

Phase/Mode Function 90-TON HOIST

Task/Operation or Facility PAD B PCR

Date DECEMBER 1993

Prepared by G. WHITMORE, LSOC 52-11

HAZARDOUS CONDITION	HAZARD CAUSE	HAZARD EFFECT	SAFETY/ENGINEERING REQUIREMENTS	HAZARD ELIMINATION/CONTROL PROVISIONS
	OR			
	E13 FAILURE OF EMERGENCY STOP		E13 NSS/GO 1740.9B, SECTION 401 (g)(5) , REMOTE EMERGENCY STOPS SHALL BE PROVIDED WHEN NEEDED; SECTION 402 (c)(3), OPERATIONAL TEST OF EMERGENCY STOPS REQUIRED.	E13 OPERATIONAL CHECK AND INSPECTION OF EMERGENCY STOP PERFORMED SEMI-ANNUALLY PER OMI Q3437. PRE-OPERATION INSPECTION AND OPERATIONAL CHECK PERFORMED PRIOR TO EACH USE PER OMI Q3437.
G3 LOAD COLLISION DUE TO DOWNWARD OVERTRAVEL	E15 FAILURE OF LOWER LIMIT SWITCH	G0 PERSONNEL INJURY/LOSS OF LIFE AND/OR FLIGHT HARDWARE DAMAGE	E15 NSS/GO 1740.9B, SECTION 401 (7), FOR CRITICAL CRANES, DUAL UPPER LIMIT SWITCHES ARE REQUIRED; SECTION 402 (c)(3), OPERATIONAL TEST OF LIMIT SWITCHES REQUIRED.	E15 PRE-OPERATION INSPECTION AND OPERATIONAL CHECK OF HOIST LIMIT SWITCH PRIOR TO EACH USE PER OMI Q3437. OPERATOR AND OBSERVERS PROVIDED WITH EMERGENCY STOP CAPABILITY AND INSTRUCTED TO HALT HOISTING OPERATIONS SHOULD ANOMALY OCCUR PER OMI M3160.
	AND			
	G11 HOIST CONTINUES TO OPERATE IN DOWNWARD DIRECTION		DEVELOPED UNDER HAZARDOUS COLUMN G11.	DEVELOPED UNDER HAZARDOUS COLUMN G11.
G11 HOIST CONTINUES TO OPERATE IN DOWNWARD DIRECTION	G9 MOTION FAILS TO STOP WHEN COMMANDED	G3 LOAD COLLISION DUE TO DOWNWARD OVERTRAVEL	DEVELOPED UNDER HAZARDOUS COLUMN G9.	DEVELOPED UNDER HAZARDOUS COLUMN G9.
	OR			
	E11 OPERATOR ERROR		E11 NSS/GO 1740.9B, SECTION 403(a), STATES THAT ONLY CERTIFIED OPERATORS SHALL BE AUTHORIZED TO USE/OPERATE LIFTING DEVICES, INCLUDING HOIST OPERATIONS WHERE PROCEDURAL CONTROLS CAN BE PROVIDED IN A TECHNICAL OPERATING PROCEDURE.	E11 OMI M3160 REQUIRES HOIST OPERATORS TO HAVE CERTS 019-1 "FIXED CRANES/HOIST CONTROL," 091-1 "FIXED CRANES/HOIST E-STOP OBSERVERS," 093 "PENDANT CONTROLLED/USER-OPERATED CRANES/HOISTS OPERATOR" AND 094-1 "FIXED CRANES/HOISTS OPERATOR" TO OPERATE THE 90-TON HOIST.

8.0 LPS CONTROL/MONITOR FUNCTIONS REVIEW

There are no LPS control/monitor functions associated with this system.

9.0 END-TO-END ANALYSIS

This system interfaces with and requires the support of the systems depicted in Figure 9 on page 79. An assessment of the loss of each interfacing system follows.

Table 7. **INTERFACING SYSTEM LOSS ASSESSMENT**

Interfacing System Title	Effect of Loss	SAA Number	Concurrence in Other SAA Comments
60 Hz Power Pad-B	Hoist will stop and the brakes will set. Non-critical.	SAA09ELB2-001	Yes.

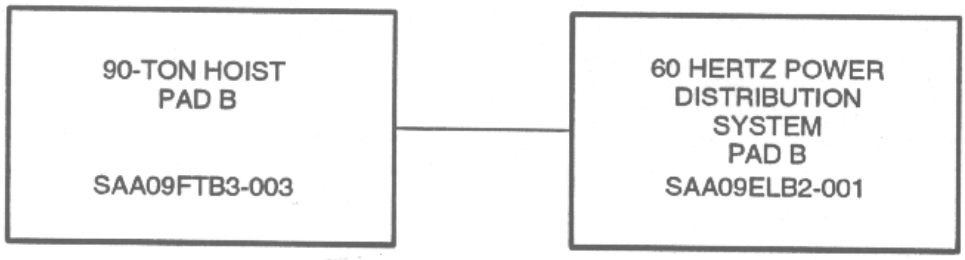


FIGURE 9. END-TO-END BLOCK DIAGRAM

10.0 SNEAK CIRCUIT ANALYSIS

There was no Sneak Circuit Analysis performed on this system.

11.0 EMERGENCY SAFING ANALYSIS

There are no Emergency Safing Circuits associated with this system.

12.0 AREAS OF CONCERN

There were no Areas of Concern identified during this analysis.

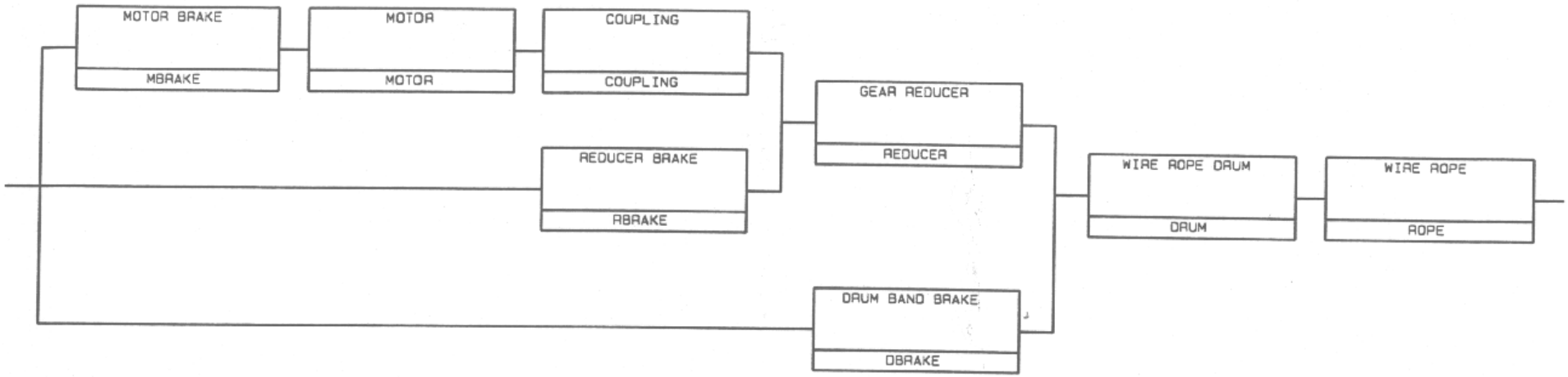
13.0 CRITICALITY CATEGORY 1R ANALYSIS

Improper performance of this system could result in loss of life or vehicle; therefore, the components used in the critical functions are analyzed in the following reliability block diagram.

13.1 RELIABILITY BLOCK DIAGRAM

The components of this system are described in the following reliability block diagram. The reliability block diagram depicts the logical relationship of system components in series and parallel paths that lead to the desired event. Those items identified as criticality category 1R are summarized in section 13.2.

Description : <Gate not found>



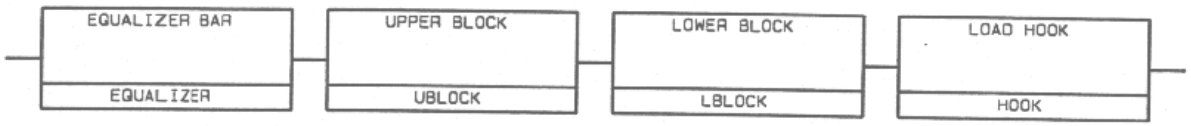


FIGURE 10. RELIABILITY BLOCK DIAGRAM

13.2 CRITICALITY CATEGORY 1R ITEMS

There were two criticality category 1R items identified. See section 13.1 for additional information. The 1R items are summarized on the following Criticality Category 1R Items Summary Sheets (Worksheet 5312-015).

Table 8. CRITICALITY CATEGORY 1R ITEMS SUMMARY

System 90-TON HOIST RSS
Baseline 422.00

Program SPACE SHUTTLE

Station Set/Facility Code RW
Date DECEMBER 1993

Prepared By B. KALLE, LSOC 52-11

FIND NO. NASA PART NO. MFG NAME MFG PART NO.	PART NAME PROGRAM MODEL NO. DRAWING/SHEET NO.	a. FAILURE MODE b. CAUSE c. FMN	FAILURE EFFECT ON SYSTEM PERFORMANCE/VEHICLE SYSTEMS AND/OR PERSONNEL SAFETY	REDUNDANCY SCREENS PASS - FAIL		CONFORMS TO JSCM 8080	OMRS FILE VI VOLUME I TEST AND INSPECTION REQUIREMENT(S)	TEAR DOWN ANALYSIS REQUIRED
1 NONE B-16497 1603HLE 4-F-375	GEAR REDUCER K61-0168 B-16497/1	a. GEAR DISENGAGEMENT b. STRUCTURAL FAILURE c. 09FTB3-003.001	NOISY AND/OR JERKY OPERATION TO DROPPING OF LOAD DEPENDING ON SEVERITY OF FAILURE. OVERSPEED SENSOR AUTOMATICALLY SETS BAND BRAKE. SUBSEQUENT FAILURE OF BAND BRAKE TO SET COULD RESULT IN A DROPPED PAYLOAD CONTAINING SOLID PROPELLANT AND HYPERGOLS. POSSIBLE LOSS OF LIFE.	A B C		NA	ANNUAL VERIFICATION OF RATED LOAD TEST.	NO
9 NONE A-13190	BAND BRAKE ASSEMBLY K61-0168 A-13190/1	a. BRAKE SLIPS OR FAILS TO SET b. SOLENOID VALVE FAILS CLOSED, HYDRAULIC CYLINDER FAILS TO ACTUATE, ACTUATOR SPRING FAILURE, OVERSPEED SWITCH FAILS TO ACTIVATE BRAKE c. 09FTB3-003.002	UNABLE TO SET BAND BRAKE. TWO REDUNDANT BRAKES CAN HOLD LOAD. SUBSEQUENT FAILURE OF GEAR REDUCER COULD RESULT IN A DROPPED PAYLOAD CONTAINING SOLID PROPELLANT AND HYPERGOLS. POSSIBLE LOSS OF LIFE.	A B C		NA	ANNUAL VERIFICATION OF RATED LOAD TEST.	NO