30

MCDONNELL DOUGLAS

SPACE TUG SYSTEMS STUDY (CRYOGENIC)
SEPTEMBER DATA DUMP

VOLUME 7 Safety
Book 1 Option 1

SEPTEMBER 1973

PREPARED BY: SPACE TUG STUDY TEAM

APPROVED BY: L. Q. Westmoreland

L. Q. WESTMORELAND
STUDY MANAGER

(NASA-CR-179113) SPACE TUG SYSTEMS STUDY (CRYOGENIC). VOLUME 7: SAFETY, BOOK 1, OPTION 1 Data Dump, Sep. 1973 (McDonnell-Douglas Astronautics Co.) 180 p Avail: NTIS

N87-70406

Unclas

00/18 0074245

PREPARED FOR NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
MARSHALL SPACE FLIGHT CENTER
UNDER CONTRACT NO. NAS8-29677

MCDONNELL DOUGLAS ASTRONAUTICS COMPANY-WEST

5301 Bolsa Avenue, Huntington Beach, CA 92647

PREFACE

This study report for the Tug Program is submitted by the McDonnell Douglas Astronautics Company (MDAC) to the Government in partial response to Contract Number NAS8-29677.

The current results of this study contract are reported in eight volumes:

Volume 1 — Summary, Program Option 1
Volume 2 — Summary, Program Option 2
Volume 3 — Summary, Program Option 3

These three summary volumes present the highlights of the comprehensive data base generated by MDAC for evaluating each of the three program options. Each volume summarizes the applicable option configuration definition, Tug performance and capabilities, orbital and ground operations, programmatic and cost considerations, and sensitivity studies. The material contained in these three volumes is further summarized in the Data Dump Overview Briefing Manual.

Volume 4 — Mission Accomplishment. (3 Books and 1 Supplement Bound Together)

This volume contains mission accomplishment analysis for each of the three program options and includes the tug system performance, mission capture, and fleet size analysis.

Volume 5 — Systems (3 Books)

This volume presents the indepth design, analysis, trade study, and sensitivity technical data for each of the configuration options and each of the Tug systems i.e., structures, thermal, avionics, and propulsion. Interface with the Shuttle and Tug payloads for each of the three options is defined.

Volume 6 — Operations (3 Books)

This volume presents the results of orbital and ground operations trades and optimization studies for each option in the form of operations descriptions, time lines, support requirements (GSE, manpower, networks, etc.), and resultant costs.

Volume 7 — Safety (3 Books)

This volume contains safety information and data for the Tug Program. Specific safety design criteria applicable to each option are determined and potential safety hazards common to all options are identified.

Volume 8 — Programmatics and Cost (3 Books)

This volume contains summary material on Tug Program manufacture, facilities, vehicle test, schedules, cost, project management SR&T, and risk assessment for each option studied.

These volumes contain the data required for the three options which were selected by the Government for this part of the study and are defined as:

A. Option 1 is a direct development program (I.O.C.: Dec 1979). It emphasizes low DDT&E cost; the deployment requirement is 3500 pounds into geosynchronous orbit, it does not have retrieval capability, and it is designed for a 36-hour mission. MDAC has also prepared data for an alternative to Option 1 which deviates from certain requirements to achieve the lowest practicable DDT&E cost.

B. Option 2 is also a direct development program (I.O.C.: 1983). It emphasizes total program cost effectiveness in addition to low DDT&E cost. The deployment requirement is 3500 pounds minimum into geosynchronous orbit and 3500 pounds minimum retrieval from geosynchronous orbit.

C. Option 3 is a phased development program (I.O.C.: 1979 phased to I.O.C. 1983). It emphasizes minimum initial DDT&E cost and low total program cost. The initial Tug capability will deploy a minimum of

3500 pounds into geosynchronous orbit without retrieval capability, however, through phased development, it will acquire the added capability to retrieve 2200 pounds from geosynchronous orbit. The impact of increasing the retrieval capability to 3500 pounds is also provided.

INTRODUCTION AND SUMMARY

This Tug, when designed, produced, and operated under the constraints of the criteria and requirements shown in this volume, will, from a safety standpoint, be a vehicle well within an acceptable risk level for the Space Shuttle Program.

Safety information and data for Option No. 1 of the Tug Program are contained herein. The intent has been to identify specific safety design criteria applicable to Option 1, in addition to potential hazards common to all options. Most of the potential hazards identified are common to all options, and should not affect the final selection from a safety standpoint.

The Option No. 1 Design Freeze, dated 27 August 1973, as shown in Volume 5, was used as the basis for this analyses.

The potential hazards unique to this option are the use of hydrazine in the ACPS and potassium hydroxide in the batteries.

A special safety analysis of the tug/orbiter capture and docking characteristics was performed and the results are shown in Appendix 1.

The analyses for Option 2 are shown in Book 2 of the Safety Volume and Option 3 in Book 3.

CONTENTS

Section 1	LISTING OF HAZARDS	1-1
Section 2	OPERATIONAL EVENTS	2-1
Section 3	HAZARD SEVERITY AND LIKELIHOOD OF OCCURRENCE	3-1
Section 4	PROPOSED HAZARD CONTROL ACTIONS	4-1
Section 5	SAFETY IMPACT	5-1
	5.1 Design	5-1
	5.2 Production	5-1
	5.3 Operations	5-2
Section 6	RESIDUAL HAZARDS AND RATIONALE FOR ACCEPTANCE	6-1
Section 7	SAFETY CRITERIA AND REQUIREMENTS	7-1
Section 8	EXCEPTIONS/DEVIATIONS	8-1
Appendix 1	CAPTURE AND DOCKIN G ANALYSIS	A1-1
Appendix 2	PRELIMINARY SYSTEM SAFETY PROGRAM PLAN	A2-1
Appendix 3	HAZARD REVIEW CHECKLIST	A3-1
Appendix 4	SAFETY CRITERIA AND REQUIREMENTS	A4-1

Section 1
LISTING OF HAZARDS

A composite listing of the hazards identified through performing design, operational, and interface hazard analyses are shown by Preliminary Hazards Analysis and the Operational Hazards Analyses which follow in Section 4.

The Preliminary System Safety Program Plan, Appendix 2, provides the hazard classifications as applied to the analyses. In addition, interpretation of the Preliminary Hazard Analyses, Section 4 and the Operational Hazard Analyses, Section 4 are provided so that correct information could be assigned to the format categories.

The Operational Hazard Analyses were predicated upon a hazard review checklist[1] shown as Appendix 3. Each hazard was applied to the subsystem reviewed to determine its application. In some cases, a specific condition may be listed as a hazard; in others as a cause or effect.

1. Progressive Qualitative Hazard Analyses, Willie Hammer, AIAA Paper No. 67-935.

Section 2
OPERATIONAL EVENTS

Identification of hazards is intimately related to the hardware that may create or be affected by a hazard. It is therefore necessary that the various subsystems be reviewed to determine whether a hazard will exist and the time that its adverse effects may be critical.

The operational events considered for the Operating Hazards Analyses covered the full spectrum of the Tug Program from Preflight Operations through Postflight Flow and Refurbishment and addressed themselves to the level deemed most hazardous.

The events determined to be affected by the identified hazard are noted in the "Planned Operation" column of the Operating Hazards Analysis, Section 4 for each subsystem analyzed.

Section 3

HAZARD SEVERITY AND LIKELIHOOD OF OCCURRENCE

The hazard severity was based upon the hazard classification definitions as noted in the Preliminary System Safety Program Plan in Appendix 2 and is shown in the third column of the OHA's, Section 4.

The likelihood of occurrence of the identified hazards requires a quantitative evaluation of the hazard. The quantitative analysis depends on the qualitative hazard identification so that probabilities of occurrence or damage may be assigned. The subject of probability of occurrence of some of the hazards identified the Operating Hazard Analyses (OHA) were addressed in the Reliability studies performed. These are included following the OHA's, Section 4.

An estimate of the likelihood of occurrence of hazards can be made by assessing the driving factor in a probability analyses, that is the unreliability for the various components. This was determined during the Reliability Analysis and is shown in Column 10 of the Reliability Analysis Tables shown in Section 4 of this document.

Actual probabilities of occurrence of hazardous events for subsystems must be determined through a comprehensive Fault Tree Analysis where these cursory estimates can be combined with system complexity and operational characteristics.

Since a detailed Fault Tree analysis could not be performed as part of this study, only a qualitative assessment using the terms likely, unlikely, and very unlikely has been performed and is shown in the "Source" column of the OHA's.

Section 4
PROPOSED HAZARD CONTROL ACTIONS

The end result of the OHA is to provide information leading to possible control action for the identified hazard. As the source/result of the hazard in its planned operation was identified, the possible control was established. These are shown in the last column of the OHA's.

These controls are formally transmitted to the cognizant designer for his inclusion in the engineering drawings, specifications, and procedures.

The incorporation of these controls and conformance to the criteria and requirements is verified by System Safety Engineering through the System Hazard Analysis. This analysis used the various techniques available as deemed best for the analysis, i.e., checklists, Logic Study Approach, Logic Diagrams, Design Reviews, Special Safety Reviews, Mathematical Analysis, Fault Hazard Analysis and Fault Tree Analysis.

The System Hazard Analysis results in either the hazard being closed or being identified as a residual hazard. A hazard shall be considered closed only if:

A. The hazard has been eliminated through design and design accomplishment verified, or
B. The hazard has been reduced to an acceptable level (marginal or less) and reduction has been verified by test, analysis, or suitable training, or
C. The hazard has been assessed and accepted by NASA by separate submittal of the Safety Analysis Report.

The residual catastrophic and critical hazards that cannot be reduced by the measures identified will be presented to program management. Design changes, new technology, and devices will continually be evaluated during the program toward reduction of these hazards.

TUG
PRELIMINARY HAZARD ANALYSIS

SUBSYSTEM	HAZARDOUS MATERIAL/OPERATION/ CONDITION	POSSIBLE INCIDENT	WORST PROBABLE CONSEQUENCE	HAZARD CATEGORY
1.0 Guidance				
1.1 Laser System	1. Laser Beam	1. Impact on orbiter cockpit	1. Injury to crew member - loss of sight.	Safety Critical
		2. Impact on ordnance device in payload	1. Initiation of ordnance device - loss of all stages.	Safety Catastrophic

TUG
PRELIMINARY HAZARD ANALYSIS

SUBSYSTEM	HAZARDOUS MATERIAL/OPERATION/ CONDITION	POSSIBLE INCIDENT	WORST PROBABLE CONSEQUENCE	HAZARD CATEGORY
2.0 Propulsion				
2.1 Main	1. Hydrogen	Gas Leak	1. Fire/explosion - destruction of orbiter.	Safety Catastrophic
			2. Overpressurization of cargo bay - rupture of structure.	Safety Critical
		Liquid Leak	1. Fire/explosion - destruction of orbiter.	Safety Catastrophic
			2. Spill on adjacent equipment.	Safety Marginal
			3. Spill on personnel.	Safety Marginal
		Vent	1. Fire - injury to personnel.	Safety Marginal
	2. Oxygen	Gas Leak	1. Overpressurization of cargo bay - rupture of structure.	Safety Critical
		Liquid Leak	1. Spill on adjacent equipment.	Safety Marginal
			2. Spill on personnel causing injury.	Safety Marginal
			3. Explosion - may form shock sensitive gels with hydrocarbons.	Safety Critical

TUG
PRELIMINARY HAZARD ANALYSIS

SUBSYSTEM	HAZARDOUS MATERIAL/OPERATION/ CONDITION	POSSIBLE INCIDENT	WORST PROBABLE CONSEQUENCE	HAZARD CATEGORY
2.2 Auxiliary				
2.2.1 Monopropellant	1. Hydrazine	Leak/Spill	1. Fire/explosion - destruction of orbiter.	Safety Catastrophic
			2. Personnel injury - toxic vapor inhalation.	Safety Critical
		Tank Rupture	1. Shrapnel from tank penetrates LOX tank & LH_2 tank with ignition source. Fire and/or explosion.	Safety Catastrophic
	2. Helium Pressurant	Leak	1. Overpressurization of orbiter bay - rupture of structure.	Safety Critical
			2. He depletion - mission scrub.	Safety Marginal
		Tank Rupture	1. Shrapnel from tank penetrates LOX tank & LH_2 tank with ignition source. Fire and/or explosion.	Safety Catastrophic

TUG
PRELIMINARY HAZARD ANALYSIS

SUBSYSTEM	HAZARDOUS MATERIAL/OPERATION/ CONDITION	POSSIBLE INCIDENT	WORST PROBABLE CONSEQUENCE	HAZARD CATEGORY
2.2 Auxiliary				
2.2.2 Bi-Propellant	1. Monomethyl-hydrazine	Leak/Spill	1. Fire/explosion - destruction of orbiter.	Safety Catastrophic
			2. Personnel injury - toxic vapor.	Safety Critical
		Tank Rupture	1. Shrapnel from tank penetrates LOX tank & LH_2 tank. Fire and/or explosion.	Safety Catastrophic
	2. Nitrogen Tetroxide	Leak/Spill	1. May combine with a fuel to cause fire and/or explosion.	Safety Catastrophic
			2. Personnel injury - toxic vapor.	Safety Critical
			3. Corrosive liquid.	Safety Critical
		Tank Rupture	1. Shrapnel from tank penetrates LOX tank & LH_2 tank with source of ignition. Fire and/or explosion.	Safety Catastrophic

TUG
PRELIMINARY HAZARD ANALYSIS

SUBSYSTEM	HAZARDOUS MATERIAL/OPERATION/ CONDITION	POSSIBLE INCIDENT	WORST PROBABLE CONSEQUENCE	HAZARD CATEGORY
2.2 Auxiliary				
2.2.2 Bi-propellant (Continued)	3. Helium Storage and Supply System	Leak	1. Overpressurization of orbiter bay - rupture of structure.	Safety Critical
			2. He depletion - mission scrub.	Safety Marginal
		Tank Rupture	1. Shrapnel from tank penetrates LOX tank & LH_2 tank with ignition source. Fire and/or explosion.	Safety Catastrophic
		Mix of MMH & N_2O_4 in pressurizing system due to "back-flow" of propellants	1. Explosion and/or fire - destruction of orbiter.	Safety Catastrophic

TUG
PRELIMINARY HAZARD ANALYSIS

SUBSYSTEM	HAZARDOUS MATERIAL/OPERATION/ CONDITION	POSSIBLE INCIDENT	WORST PROBABLE CONSEQUENCE	HAZARD CATEGORY
3.0 Electrical				
3.1 Fuel Cell	Hydrogen	Gas Leak	1. Fire/explosion - destruction of orbiter.	Safety Catastrophic
			2. Overpressurization of cargo bay - rupture of structure	Safety Critical
		Liquid Leak	1. Fire/explosion - destruction of orbiter.	Safety Catastrophic
			2. Spill on adjacent equipment.	Safety Marginal
			3. Spill on personnel.	Safety Marginal
	Oxygen	Gas Leak	1. Overpressurization of cargo bay - rupture of structure.	Safety Critical
		Liquid Leak	1. Spill on adjacent equipment.	Safety Marginal
			2. Spill on personnel causing injury.	Safety Marginal
			3. Explosion - may form shock sensitive gels with hydrocarbons.	Safety Critical

TUG
PRELIMINARY HAZARD ANALYSIS

SUBSYSTEM	HAZARDOUS MATERIAL/OPERATION/ CONDITION	POSSIBLE INCIDENT	WORST PROBABLE CONSEQUENCE	HAZARD CATEGORY
3.0 Electrical				
3.1 Fuel Cell (Continued)	Helium Pressurant Tank	Leak	1. Overpressurization of orbiter bay. Rupture of structure.	Safety Critical
			2. He depletion - mission scrub.	Safety Marginal
		Tank Rupture	1. Shrapnel from tank penetrates LOX tank & LH_2 tank with ignition source. Fire and/or explosion.	Safety Catastrophic

TUG
PRELIMINARY HAZARD ANALYSIS

SUBSYSTEM	HAZARDOUS MATERIAL/OPERATION/ CONDITION	POSSIBLE INCIDENT	WORST PROBABLE CONSEQUENCE	HAZARD CATEGORY
3.0 Electrical				
3.2 Battery	Hydrogen gas released from electrolyte	Battery Case ruptures explosively	1. Shrapnel from case penetrates LOX tank & LH_2 tank with ignition source. Fire and/or explosion.	Safety Catastrophic
			2. Electrolyte spills on adjacent equipment causing corrosion.	Safety Marginal

TUG
PRELIMINARY HAZARD ANALYSIS

SUBSYSTEM	HAZARDOUS MATERIAL/OPERATION/ CONDITION	POSSIBLE INCIDENT	WORST PROBABLE CONSEQUENCE	HAZARD CATEGORY
4.0 Ordnance				
4.1 LOX Dump	V-Band Explosive Bolt	Inadvertent Initiation	LOX spill in bay during dump - overpressurization of orbiter bay - rupture of structure.	Safety Critical

OPERATING HAZARDS ANALYSIS

PROPULSION SYSTEM - MAIN

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT (PROPELLANT LOADING)	ACCELERATION	SAFETY CRITICAL	RAPID FLOW CUT-OFF OR FLOW START CAUSES HIGH PRESSURE SURGES IN FILL AND DRAIN SYSTEM. (LIKELY)	4:1 SAFETY FACTOR ON PLUMBING. PROVIDE FLEXIBILITY IN PLUMBING SUPPORT. SELECT VALVE OPERATING TIMES TO PRECLUDE HIGH SURGES. REDUCE FILL VELOCITY. IDENTIFY SURGE PEAK PRESSURE AND USE FOR MAXIMUM OPERATING PRESSURE FOR DESIGN.
FLIGHT (LAUNCH AND DEPLOYMENT)	ACCELERATION	SAFETY CRITICAL	RAPID MOVEMENT OF PROPELLANTS IN TANKS. (LIKELY)	PROVIDE BAFFLING TO PRECLUDE RAPID MOVEMENT OR ASSURE ALL MOVEMENT WILL NOT CAUSE RAPID PROPELLANT MOVEMENT. PROVIDE SETTLING CAPABILITY.
			PROPULSIVE VENTING (LIKELY)	DETERMINE IF ACCELERATION IS DETRIMENTAL.

OPERATING HAZARDS ANALYSIS

PROPULSION SYSTEM - MAIN

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT	CONTAMINATION	SAFETY MARGINAL	INGESTION OF CONTAMINANTS INTO PROPELLANT TANKS (CAUSES LOW PROPELLANT FLOW RATES). (LIKELY)	PERFORM OPERATIONS IN CONTROLLED AREA. PROVIDE CONTROLS FOR CLOTHING AND EQUIPMENT. PROVIDE POSITIVE PRESSURE INSIDE TANKS. DESIGN FOR MINIMUM ACCESS REQUIREMENTS. PROVIDE PROPELLANT FILTERING DEVICES
REFURBISHMENT	CONTAMINATION	SAFETY MARGINAL	INGESTION OF CONTAMINANTS INTO PROPELLANT TANKS, ENGINE SYSTEM, VENT SYSTEM OR FILL AND DRAIN SYSTEM (CAUSES LOW PROPELLANT FLOW RATES AND VALVE LEAKAGE OR BINDING). (LIKELY)	SAME AS PREFLIGHT.
		SAFETY MARGINAL	DEPOSIT OF ACPS EXHAUST ON TANKS/SHELL (LIKELY)	ASSURE PROTECTIVE COATINGS WILL NOT REACT WITH ACPS EXHAUST PRODUCTS.

OPERATING HAZARDS ANALYSIS

PROPULSION SYSTEM - MAIN

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT (ALL SUBSYSTEMS AND HARDWARE)	CORROSION	SAFETY MARGINAL	EXPOSURE TO CORROSIVE ATMOSPHERES AND/OR FLUIDS. (LIKELY)	PERFORM OPERATIONS IN CONTROLLED AREA. ASSURE COMPATIBILITY OF MATERIALS AND FLUIDS. DO NOT USE TRICHLOR PRODUCTS TO CLEAN TITANIUM PARTS. ASSURE LEAK TEST SOLUTIONS ARE CORRECTLY REMOVED. USE GALVANIC CHART WHEN SELECTING MATERIALS. PROVIDE PROTECTIVE COATINGS.
REFURBISHMENT	CORROSION	SAFETY MARGINAL	EXPOSURE TO CORROSIVE ATMOSPHERES AND/OR FLUIDS (LIKELY)	SAME AS PREFLIGHT

OPERATING HAZARDS ANALYSIS

PROPULSION SYSTEM - MAIN

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT (VENT SYSTEM, FILL AND DRAIN, ENGINE, QUANTITY MEASURING)	ELECTRICAL A. INADVERTANT ACTIVATION	SAFETY MARGINAL	ACTIVATION OF THE PRE-VALVE(S) IN THE ENGINE FEED SYSTEM WILL ALLOW PROPELLANTS TO REACH ENGINE SHUT-OFF VALVES. POSSIBLE LEAKAGE INTO BAY. (UNLIKELY)	PROVIDE ELECTRICAL INTERLOCKS TO PREVENT INADVERTANT ACTIVATION.
	B. POWER SOURCE FAILURE	SAFETY MARGINAL	1. POWER SOURCE FAILURE MAY CAUSE RAPID SHUT-DOWN DURING FILL WITH RESULTING SURGES. (LIKELY) 2. POWER SOURCE FAILURE MAY CAUSE QUANTITY MEASURING SYSTEM TO BE INOPERATIVE ALLOWING OVERFILL. (LIKELY)	PROVIDE DUAL POWER SOURCE. DESIGN PROPELLANT FILL VALVES "FAIL CLOSED". DESIGN VENT VALVES TO FAIL "OPERATIONAL". PROVIDE REDUNDANT QUANTITY MEASURING SYSTEM WITH SEPARATE POWER SOURCES.
	C. STATIC ELECTRICITY	SAFETY MARGINAL	PROPELLANT FLOW CREATES STATIC ELECTRICITY ON PLUMBING. (LIKELY)	DESIGN SYSTEM WITH GOOD GROUND PATHS. APPLY MIL-STD- FOR GROUNDING. PROVIDE GROUNDING GRIDS AS REQUIRED. PROVIDE LIGHTNING PROTECTION. GROUNDING PATHS FOR INSULATED SYSTEMS MUST EQUAL THAT OF UNINSULATED SYSTEMS.

OPERATING HAZARDS ANALYSIS

PROPULSION SYSTEM - MAIN

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
FLIGHT	ELECTRICAL			
	A. INADVERTENT ACTIVATION	SAFETY CATASTROPHIC	ACTIVATION OF THE TUG ENGINE WHILE IN THE ORBITER BAY OR IN CLOSE PROXIMITY. (UNLIKELY)	PROVIDE ELECTRICAL INTERLOCKS TO PREVENT INADVERTENT ACTIVATION. DESIGN SYSTEM SUCH THAT POSITIVE CREW ACTION IS REQUIRED TO ACTIVATE THE ENGINE SYSTEM. PROVIDE SAFETY INTERLOCK WHILE TUG IS ATTACHED TO ORBITER BY MEANS OF AN ELECTROMECHANICAL DEVICE. ASSURE INSULATION WILL NOT ALLOW INADVERTENT ACTIVATION. ASSURE CONNECTOR AND PIN SELECTION WILL PRECLUDE INADVERTENT ACTIVATION. PROVIDE MONITORS TO INDICATE SAFING STATUS.
	B. POWER SOURCE FAILURE	SAFETY MARGINAL	POWER SOURCE FAILURE MAY CAUSE ENGINE SHUTDOWN. (LIKELY)	PROVIDE SECONDARY POWER SOURCE.
LANDING	C. ARCING	SAFETY CRITICAL	ARCING CREATES SOURCE OF IGNITION ON CRASH LANDING (LIKELY)	ASSURE PROVISIONS ARE MADE TO DEACTIVATE SYSTEMS WHICH CAN PROVIDE AN IGNITION SOURCE ON CRASH IMPACT.

OPERATING HAZARDS ANALYSIS

PROPULSION SYSTEM - MAIN

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
FLIGHT (REENTRY AND LANDING)	EXPLOSION	SAFETY CRITICAL	CRYOGENICS LOCKED-UP BETWEEN VALVES (UNLIKELY)	PROVIDE PRESSURE RELIEF DESIGN TO PRECLUDE TRAPPED CRYOGENICS. PROVIDE INSULATION TO PRECLUDE HEAT RISE EFFECT.
		SAFETY CATASTROPHIC	CRYOGENICS LOCKED-UP IN TANKS (UNLIKELY)	ASSURE VENT TO VACUUM DOES NOT ALLOW RETENTION OF CRYOGENICS AS SOLIDS. PROVIDE RELIEF VALVE OVERRIDE.

OPERATING HAZARDS ANALYSIS

PROPULSION SYSTEM - MAIN

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT	FIRE	SAFETY CATASTROPHIC	HYDROGEN LEAK/SPILL INTO ORBITER BAY THROUGH A SYSTEM JOINT. (UNLIKELY)	LEAK CHECK SYSTEM PRIOR TO FILLING. INERT ORBITER BAY PRIOR TO FILLING. DOUBLE SEAL OR WELD ALL CONNECTIONS. LEAKAGE NOT TO EXCEED TBD SCCS PLUMBING TBD SCCS TANK TBD SCCS FITTINGS DESIGN TO PRECLUDE LOW THERMAL EFFECTS. DESIGN TO ELIMINATE ALL SOURCES OF IGNITION. CONSIDER FRICTION SPARKS, IMPACT SPARKS, ELECTRICAL SPARKS AND HOT OBJECTS. PURGE BAY AND ASSURE ALL CONFINED AREAS ARE ALSO PURGED. LEAK CHECK SYSTEM AFTER CHILLDOWN. DESIGN SYSTEM TO MINIMIZE POINTS OF POTENTIAL LEAKAGE. PROVIDE PRESSURE RELIEF AND BLEED TO ALLOW FOR CRYOGENIC EXPANSION. LOCATE ELECTRICAL WIRING OR OTHER POTENTIAL IGNITION SOURCES SO THAT NO CONTACT CAN BE MADE WITH THE LEAKING FLUID.
	FIRE	SAFETY CRITICAL	HYDROGEN VENT SYSTEM (LIKELY)	PROVIDE DISPOSITION BY A BURNER SYSTEM.

OPERATING HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT	FIRE	SAFETY CATASTROPHIC	IGNITION OF INSULATION (UNLIKELY)	SELECT INSULATION THAT WILL NOT IGNITE OR REACT WITH SYSTEM FLUIDS. SELECT INSULATION OF A NON ABSORBENT MATERIAL SO FLUID CANNOT BE RETAINED IN OR UNDER IT. SELECT MATERIALS WITH LOW FLAME PROPAGATION RATES, HIGH IGNITION TEMPERATURES, AND A LOW LEVEL OF TOXIC PRODUCTS OF COMBUSTION.

OPERATING HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
FLIGHT (LAUNCH AND DEPLOYMENT)	FIRE	SAFETY CATASTROPHIC	INADVERTENT ACTIVATION OF MAIN ENGINE IN ORBITER BAY. (VERY UNLIKELY)	PROVIDE MECHANICAL INTERRUPT FOR MAIN PROPULSION IGNITION SYSTEM WHEN INSTALLED IN ORBITER. DESIGN IGNITION SYSTEM TO REQUIRE POSITIVE CREW ACTION FOR ACTIVATION.
		SAFETY CRITICAL	INADVERTENT ACTIVATION OF MAIN ENGINE IN TBD FEET OF THE ORBITER. (UNLIKELY)	DESIGN IGNITION SYSTEM TO REQUIRE POSITIVE CREW ACTION FOR ACTIVATION.

OPERATING HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
FLIGHT (RETRIEVAL)	FIRE	SAFETY CATASTROPHIC	LEAKAGE OF GH_2 INTO THE ORBITER BAY AFTER RETRIEVAL. IGNITION ON REENTRY. (UNLIKELY)	VENT H_2 TO TBD PSI AND PURGE WITH GHe, VENT TO TBD PSI AND PRESSURIZE TO TBD PSI WITH GHe.
(LANDING)		SAFETY CRITICAL	VENTING OF GH_2 OUT ORBITER VENT. (LIKELY)	PUT TANK UNDER GHe BLANKET. PROVIDE DISPOSITION BY A BURNER SYSTEM.

OPERATING HAZARDS ANALYSIS

PROPULSION SYSTEM - MAIN

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
FLIGHT (DEPLOYMENT AND RETURN)	HEAT AND TEMPERATURE (HIGH)	SAFETY CATASTROPHIC	BURN THROUGH OF SHELL AND TANK BY ACPS ROCKET EXHAUST. (LIKELY)	PROVIDE THERMAL PROTECTION PADS AT ACPS ROCKET PLUMES.
(REENTRY AND LANDING)		SAFETY MARGINAL	ORBITER BAY UPPER TEMPERATURE LIMIT IS 200°F. (LIKELY)	DESIGN TO PRECLUDE THERMAL SHOCK. AVOID LOCKED-UP CRYOGENICS IN LINES. PROVIDE TANK PRESSURE RELIEF WITH OVERRID. MONITOR PRESSURES.

OPERATING HAZARDS ANALYSIS

PROPULSION SYSTEM - MAIN

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT	HEAT AND TEMPERATURE (LOW)	SAFETY CATASTROPHIC	CRYOGENIC FLUIDS CAUSE RAPID CONTRACTION OF MATERIALS, UNEVENLY, CAUSING PART FAILURE AND LH_2 SPILL. (LIKELY)	SELECT MATERIALS WHICH ARE SATISFACTORY FOR CRYOGENICS. PRE-COOL THE SYSTEM TO PRECLUDE CRYOGENIC SHOCK. PROVIDE FLEXIBLE SECTIONS TO ALLOW CONTRACTION AND EXPANSION OF TUBING RUNS. PROVIDE VIBRATION DAMPING SLIDING SUPPORTS FOR PLUMBING. SELECT SEALS WHICH DO NOT LOSE SEALING ABILITY AT CRYOGENIC TEMPERATURES.
		SAFETY MARGINAL	CRYOGENIC BURNS (LIKELY)	PROTECTIVE CLOTHING MUST BE REQUIRED. INSULATE AREAS WHICH ARE CRITICAL.
		SAFETY MARGINAL	CONDENSATION OF MOISTURE (LIKELY)	PURGE AREAS WITH DRY GN_2 TO REDUCE MOISTURE LEVEL. INSULATE AREAS WHERE MOISTURE COULD CONDENSE.

OPERATING HAZARDS ANALYSIS

PROPULSION SYSTEM - MAIN

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
FLIGHT (LAUNCH)	HEAT AND TEMPERATURE (LOW)	SAFETY CATASTROPHIC	VENT AND RELIEF VALVE FREEZES CLOSED AND TANK RUPTURES DUE TO OVER-PRESSURE. (LIKELY)	DESIGN SYSTEM WITH PARALLEL-DUAL VENT AND RELIEF VALVES. SELECT MATERIALS TO PRECLUDE FREEZING. DESIGN TO PREVENT MOISTURE ACCUMULATION. DESIGN TO PREVENT STICKING VALVE STEMS.
(RECOVERY)		SAFETY MARGINAL	FAILURE OF DISCONNECTS TO MATE DUE TO TEMPERATURE DIFFERENTIALS. (LIKELY)	ASSURE CORRECT SELECTION OF MATERIALS. PROVIDE HEATERS AS REQUIRED.

OPERATING HAZARDS ANALYSIS

PROPULSION SYSTEM - MAIN

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT (PRESSURE TESTS)	LEAKAGE	SAFETY MARGINAL	LEAKAGE OF GN_2 DURING PRESSURE TEST IN CLOSED AREA CREATES HAZARDOUS CONDITION. (LIKELY)	PROVIDE SUFFICIENT VENTILATION TO CLEAR LEAKED TEST MEDIUM FROM AREA. PROVIDE GAS DETECTORS TO SIGNAL HAZARDOUS CONDITIONS. PERFORM ADEQUATE LEAK TESTS PRIOR TO PRESSURE TESTS.
(PROPELLANT LOADING)	LEAKAGE	SAFETY MARGINAL	LEAKAGE OF LH_2 INTO CENTER SHELL SECTION 1. IMPINGES ON ELECTRONIC EQUIPMENT CAUSING IT TO BE INOPERATIVE. (UNLIKELY) 2. IMPINGES ON INSULATION CAUSING HAZARDOUS CONDITION. (UNLIKELY) 3. IMPINGES ON PURGE BAG-EMBRITTLEMENT AND BAG RUPTURE. (UNLIKELY) 4. CREATES CONDENSATION OF MOISTURE AND LIQUEFACTION OF AIR. (UNLIKELY) 5. GASIFIES AND CREATES HAZARDOUS ATMOSPHERE. (UNLIKELY) 6. GASIFIES AND CREATES OVERPRESSURE. (UNLIKELY)	1. INSURE THAT ELECTRICAL SYSTEMS WILL OPERATE WHEN EXPOSED TO LOW TEMPERATURE PROPELLANTS. INSURE ELECTRONIC EQUIPMENT IS VAPOR TIGHT TO PRECLUDE ENTRY OF LH_2 OR VAPORS. PURGE CENTER SHELL SECTION. LOCATE EQUIPMENT SO THAT LH_2 WILL NOT IMPINGE. 2. INSURE INSULATION IS A NON ABSORBENT MATERIAL AND CANNOT REACT CHEMICALLY WITH THE LH_2. 3. INSURE BAG MATERIAL WILL NOT RUPTURE WHEN EXPOSED TO CRYOGENIC LIQUIDS. 4. PROVIDE PURGE TO CREATE INERT ATMOSPHERE AND MAINTAIN THERMAL AND HUMIDITY REQUIREMENTS. 5. PROVIDE PURGE TO MAINTAIN INERT ATMOSPHERE AND CLEAR GASEOUS H_2 FROM CENTER SHELL SECTION. PROVIDE PORTING AND PURGING SYSTEM TO ASSURE COMPLETE PURGE. 6. PROVIDE PORTING TO PRECLUDE OVERPRESSURE.

OPERATING HAZARDS ANALYSIS

PROPULSION SYSTEM - MAIN

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT (PROPELLANT LOADING)	LEAKAGE	SAFETY MARGINAL	LEAKAGE OF LO_2 INTO CENTER SHELL SECTION 1. IMPINGES ON ELECTRONIC EQUIPMENT CAUSING IT TO BE INOPERATIVE. (UNLIKELY) 2. IMPINGES ON INSULATION CAUSING HAZARDOUS CONDITION. (UNLIKELY) 3. IMPINGES ON PURGE BAG CAUSING BAG EMBRITTLEMENT AND BAG RUPTURE. (UNLIKELY) 4. CREATES CONDENSATION OF MOISTURE. (UNLIKELY) 5. GASIFIES AND CREATES OVERPRESSURE. (UNLIKELY)	1. INSURE THAT ELECTRICAL SYSTEMS WILL OPERATE WHEN EXPOSED TO LOW TEMPERATURE PROPELLANTS. INSURE ELECTRONIC EQUIPMENT IS VAPOR TIGHT TO PRECLUDE ENTRY OF LO_2 OR VAPORS. PURGE CENTER SHELL SECTION. LOCATE EQUIPMENT SO THAT LO_2 WILL NOT IMPINGE. 2. INSURE INSULATION IS A NON ABSORBENT MATERIAL AND CANNOT REACT CHEMICALLY WITH LO_2. 3. INSURE BAG MATERIAL WILL NOT RUPTURE WHEN EXPOSED TO CRYOGENIC LIQUIDS. 4. PROVIDE PURGE TO CREATE INERT ATMOSPHERE AND MAINTAIN THERMAL AND HUMIDITY REQUIREMENTS. 5. PROVIDE PORTING TO PRECLUDE OVERPRESSURE.

OPERATING HAZARDS ANALYSIS

PROPULSION SYSTEM - MAIN

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT (PROPELLANT LOADING)	LEAKAGE	SAFETY MARGINAL	LEAKAGE OF LH_2 INTO ORBITER BAY CREATES HAZARDOUS CONDITION. CREATES CONDENSATION AND LIQUEFACTION OF AIR. (UNLIKELY)	PROVIDE PURGE TO CREATE INERT ATMOSPHERE. PROVIDE DETECTORS TO SIGNAL H_2 PRESENCE. PERFORM ADEQUATE LEAK TESTS PRIOR TO LOADING OF LH_2.

OPERATING HAZARDS ANALYSIS

PROPULSION SYSTEM - MAIN

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
FLIGHT (DEPLOYMENT)	LEAKAGE	SAFETY MARGINAL	FLUID LEAKAGE THROUGH DISCONNECT (LIKELY)	PROVIDE POSITIVE SHUT-OFF ON TUG SIDE OF DISCONNECT.

OPERATING HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
FLIGHT (RETRIEVAL AND REENTRY)	LEAKAGE	SAFETY CATASTROPHIC	LEAKAGE OF LH_2 INTO ORBITER BAY CREATES HAZARDOUS ATMOSPHERE AT REENTRY. (UNLIKELY)	AFTER RETRIEVAL TO ORBITER BAY, DUMP LH_2 REMAINING TO SPACE AND VENT TANK TO TBD PSI. CLOSE DUMP AND VENT SYSTEM AND ALLOW TANK TO WARM. VENT TO TBD PSIA MAX. CLOSE VENT AND FILL WITH GHe. BLOWDOWN AND REFILL WITH GHe TO TBD PSIA.

OPERATING HAZARDS ANALYSIS

PROPULSION SYSTEM - MAIN

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT (LOADING)	MOISTURE	SAFETY MARGINAL	CONDENSATION AND FREEZING OF MOISTURE ON CRYOGENIC TANKS AND LINES DURING PROPELLANT LOADING. (LIKELY)	PROVIDE PURGE TO ESTABLISH AND MAINTAIN HUMIDITY REQUIREMENTS. PROVIDE INSULATION TO MEET EXPOSURE TIMES.
ALL PHASES	OXIDATION	SAFETY CRITICAL	DETERIORATION OF OXYGEN COMPONENTS WITH SUB-SEQUENT FAILURE. (LIKELY)	PROVIDE FOR LONG TERM EXPOSURE AND SELECT MATERIALS COMPATIBLE WITH OXYGEN. PROVIDE PROTECTIVE COATINGS TO AID IN OXIDATION REDUCTION.
PREFLIGHT (PRESSURE TESTS)	PRESSURE	SAFETY CRITICAL	TANK RUPTURES DUE TO OVERPRESSURE. (VERY UNLIKELY)	PROVIDE PRESSURE LIMITING DEVICES IN GSE. PRESSURE TEST AT NO GREATER THAN 1/4 MAX. OPERATING PRESSURE. PROVIDE PRESSURE RELIEF DEVICES. DESIGN WITH ADEQUATE SAFETY FACTOR. APPLY FRACTURE CONTROL PROGRAM. PROVIDE PROCEDURAL CONTROLS. PROVIDE REDUNDANT PRESSURE RELIEF DEVICES. PROVIDE TUG RETENTION TO PRECLUDE TUG MOVEMENT. ASSURE NO SINGLE FAILURE CAUSES HAZARDOUS CONDITION.
(PROPELLANT LOADING)	PRESSURE	SAFETY CATASTROPHIC	TANK RUPTURES DUE TO OVERPRESSURE. (VERY UNLIKELY)	PROVIDE REDUNDANT PRESSURE RELIEF DEVICES. MONITOR TANK PRESSURES AND PROVIDE VENT AND RELIEF OVERRIDE. SIZE VENTS FOR MAX. LOADING RATE.
		SAFETY CRITICAL	PRESSURE SURGES CAUSE RUPTURE OF FILL AND DRAIN SYSTEM. (UNLIKELY)	4:1 SAFETY FACTOR ON PLUMBING. PROVIDE FLEXI-BILITY IN PLUMBING SUPPORT. SELECT VALVE OPERATING TIMES TO PRECLUDE HIGH SURGES. REDUCE FILL VELOCITY.
(LAUNCH)	PRESSURE	SAFETY CATASTROPHIC	TANK RUPTURES DUE TO OVERPRESSURE. (VERY UNLIKELY)	ASSURE TANKS HAVE ADEQUATE SAFETY FACTOR WHEN VENTING RESTRICTIONS ARE CONSIDERED.
(DEPLOYMENT)	PRESSURE	SAFETY CRITICAL	TANK RUPTURES DUE TO OVERPRESSURE. (VERY UNLIKELY)	MONITOR TANK PRESSURES DURING PRESSURIZATION. PROVIDE PRESSURE LIMITING DEVICES IN PRESSURI-ZATION SYSTEM. PROVIDE VENT AND RELIEF OVER-RIDE.

OPERATING HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
(RETRIEVAL)	PRESSURE	SAFETY MARGINAL	PRESSURE BUILDUP IN ORBITER BAY DUE TO VENT DISCONNECT LEAKAGE. (VERY UNLIKELY)	ASSURE DISCONNECT IS DESIGNED TO PRECLUDE LEAKAGE ON REMATE. SHROUD DISCONNECT AND BLEED REMOTE OF ORBITER BAY.
(POSTFLIGHT)	PRESSURE	SAFETY MARGINAL	INSUFFICIENT INTERNAL TANK PRESSURE-TANK COLLAPSE. (UNLIKELY)	PROVIDE SUFFICIENT PRESSURE TO PRECLUDE COLLAPSE.
(POSTFLIGHT)	PRESSURE	SAFETY CRITICAL	PRESSURE BUILDUP IN HYDROGEN TANK AFTER LANDING AND PRIOR TO VENTING (LIKELY)	START REENTRY WITH TBD POUNDS GHe IN TANK. PROVIDE SUFFICIENT GHe TO ESTABLISH GH_2 VOLUME BELOW 4 PERCENT LEL. VENT TANK AS REQUIRED.
(REFURBISHMENT)	PRESSURE	SAFETY CRITICAL	RETAINED PRESSURE CAUSES COMPONENTS TO BE PROPULSIVE DURING REMOVAL. (LIKELY)	ASSURE PRESSURE BLEED DOWN PRIOR TO REFURBISHMENT. PROVIDE PROCEDURAL CONTROLS.

OPERATING HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT (PRESSURE TESTS AND PROPELLANT LOADING)	STRESS REVERSALS	SAFETY CRITICAL	PRESSURE - BLEED CYCLES AND CRYOGENIC LOAD - OFFLOAD RESULT IN STRUCTURAL FAILURE. (UNLIKELY)	MINIMIZE PRESSURE-BLEED CYCLES. APPLY FRACTURE MECHANICS PROGRAM. SELECT MATERIALS COMPATIBLE FOR CRYOGENIC CYCLING. DESIGN WITH SUFFICIENT SAFETY FACTORS TO ALLOW FOR STRESS REVERSALS.
ALL PHASES	STRUCTURAL DAMAGE	SAFETY MARGINAL	FAILURE OF TANK. (VERY UNLIKELY)	ASSURE ADEQUATE DESIGN STRENGTH. PREVENT OVER-PRESSURE. DESIGN FOR CRYOGENICS. ASSURE ADEQUATE DESIGN FOR VIBRATION. CONSIDER ACCELERATION. PROVIDE CORRECT GROUND HANDLING EQUIPMENT.
REFURBISHMENT	TOXICITY	SAFETY MARGINAL	HIGH GHe OR GN_2 CONCENTRATION IN TANK WITH ACCESS REQUIRED. (LIKELY)	PROVIDE FRESH AIR PURGE. SAMPLE ATMOSPHERE AND PROVIDE CONTINUOUS MONITORING. PROVIDE RESPIRATION EQUIPMENT.

OPERATING HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
FLIGHT	VIBRATION	SAFETY MARGINAL	ENGINE CREATED VIBRATION CAUSES METAL FATIGUE LEADING TO STRUCTURAL FAILURE. (LIKELY)	DESIGN TO MEET ANTICIPATED VIBRATION ENVIRONMENT.

OPERATING HAZARDS ANALYSIS PURGE, EVACUATION, & REPRESSURIZATION SYSTEM

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT	CONTAMINATION	SAFETY MARGINAL	INGESTION OF CONTAMINANTS INTO TANK. (LIKELY)	PERFORM OPERATIONS IN CONTROLLED AREA. PROVIDE FILTERING DEVICES. SAMPLE AND TEST FOR CLEANLINESS.
FLIGHT	CONTAMINATION	SAFETY MARGINAL	CLOGS FILTER AND CAUSES LOW FLOW RATE. (LIKELY)	PROVIDE FILTER DEVICES WITH SUFFICIENT CAPACITY AND BYPASS CAPABILITY.
	CONTAMINATION	SAFETY CRITICAL	VALVE FAILS TO CLOSE AND CONTINUES PRESSURIZATION. (UNLIKELY)	PROVIDE FILTER DEVICE. PROVIDE VENT SYSTEM FOR BAGS. PROVIDE REDUNDANT SYSTEM SHUTOFF VALVE.
	CONTAMINATION	SAFETY CRITICAL	LH_2 LEAKAGE CROSS FLOWS TO LO_2 PURGE BAG. CREATES HAZARD POTENTIAL. (UNLIKELY)	PROVIDE POSITIVE MEANS TO PRECLUDE LEAKAGE CROSS FLOW BETWEEN PURGE BAGS.
	CONTAMINATION	SAFETY MARGINAL	BAG RUPTURES AND ALLOWS GHe TO FLOW INTO ORBITER BAY. (LIKELY)	PROVIDE FLOW SENSITIVE SHUTOFF CAPABILITY OR MONITOR WITH CREW OVERRIDE ON SHUTOFF VALVES.

OPERATING HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
REFURBISHMENT	CONTAMINATION	SAFETY MARGINAL	INGESTION OF CONTAMINANTS INTO TANKS AND SYSTEM. (LIKELY)	PERFORM OPERATIONS IN CONTROLLED AREA. PROVIDE CONTROLS FOR CLOTHING AND EQUIPMENT.
PREFLIGHT	CORROSION	SAFETY MARGINAL	EXPOSURE TO CORROSIVE ATMOSPHERE AND/OR FLUIDS. (LIKELY)	PERFORM OPERATIONS IN CONTROLLED AREA. ASSURE COMPATIBILITY OF MATERIALS AND FLUIDS. DO NOT USE TRICHLOR PRODUCTS TO CLEAN TITANIUM PARTS. ASSURE LEAK TEST SOLUTIONS ARE CORRECTLY REMOVED. USE GALVANIC CHART WHEN SELECTING MATERIALS. ASSURE PROTECTIVE COATINGS DO NOT REACT WITH SYSTEM FLUIDS.
REFURBISHMENT	CORROSION	SAFETY MARGINAL	EXPOSURE TO CORROSIVE ATMOSPHERE AND/OR FLUIDS. (LIKELY)	SAME AS PREFLIGHT. ASSURE CLEANING FLUIDS WILL NOT BE TRAPPED IN VALVES AND LINES.

OPERATING HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT	ELECTRICAL A. INADVERTENT ACTIVATION	SAFETY MARGINAL	ACTIVATION OF THE SYSTEM VALVES WILL CAUSE THE BAGS TO BE PRESSURIZED. (UNLIKELY)	PROVIDE ELECTRICAL INTERLOCKS TO PREVENT INADVERTENT ACTIVATION.
	B. STATIC	SAFETY MARGINAL	GAS FLOW CREATES STATIC ELECTRICITY ON BAG. (LIKELY)	DESIGN SYSTEM WITH GOOD GROUND PATHS. APPLY MIL-STD- FOR GROUNDING. PROVIDE GROUNDING GRIDS AS REQUIRED. PROVIDE LIGHTNING PROTECTION. GROUNDING PATHS FOR INSULATED SYSTEMS MUST EQUAL THAT OF UNINSULATED SYSTEMS. PROVIDE BAG OF CONDUCTIVE MATERIAL.

OPERATING HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
FLIGHT	POWER SOURCE FAILURE	SAFETY MARGINAL	POWER SOURCE FAILURE MAY CAUSE VALVE CLOSURE. (LIKELY)	PROVIDE SECONDARY POWER SOURCE.
				ASSURE PROVISIONS ARE MADE TO DEACTIVATE SYSTEMS WHICH CAN PROVIDE AN IGNITION SOURCE ON CRASH IMPACT.

OPERATING HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT (FILL)	EXPLOSION	SAFETY CRITICAL	OVER PRESSURIZATION DURING THE FILL CYCLE AND TANK RUPTURES. (UNLIKELY)	PROVIDE PRESSURE RELIEF IN FILL SYSTEM. MONITOR TANK PRESSURE. PROVIDE PRESSURE RELIEF OF TANK AT 10% ABOVE MAXIMUM OPERATING. RELIEVE TO VENT SYSTEM.

OPERATING HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT (THROUGH PROPELLANT LOADING)	HEAT AND TEMPERATURE (HIGH)	SAFETY MARGINAL	PRESSURE INCREASES AND GHe TANK RUPTURES. (UNLIKELY)	MAINTAIN AMBIENT TEMPERATURE BELOW 110°F. PROVIDE VENT BURST DISC OR MONITOR PRESSURE AND ACTIVATE TO MAIN TANK TO REDUCE PRESSURE.
FLIGHT (REENTRY AND LANDING)	(HIGH)	SAFETY MARGINAL	PRESSURE INCREASES AND GHe TANK RUPTURES. (LIKELY)	(SAME AS ABOVE)
		SAFETY MARGINAL	PURGE BAG RUPTURES DUE TO OVERPRESSURE. (LIKELY)	PROVIDE RELIEF VALVE TO PRECLUDE PURGE BAG OVERPRESSURE. PROVIDE SOLENOID VALVES WITH CREW OVERRID TO CUTOFF SUPPLY GAS.

OPERATING HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT (LOADING)	LEAKAGE	SAFETY CRITICAL	LEAKAGE THROUGH VALVES OR CONNECTIONS. (UNLIKELY)	SYSTEM LEAKAGE RATES NOT TO EXCEED TBD SCCS VALVES TBD SCCS TANK TBD SCCS FITTINGS UPON COMPLETION OF LOADING, SAMPLE ALL FLANGES, ETC. FOR LEAKAGE. CAP ALL PORTS. ASSURE VALVE POSITIONS.

OPERATING HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT (OPERATIONS)	LEAKAGE	SAFETY MARGINAL	LEAKAGE THROUGH VALVES OR CONNECTIONS. (LIKELY)	ASSURE NO OPERATIONAL SIGNALS ARE SENT TO SYSTEM. ASSURE NO INADVERTENT SIGNALS/ OPERATIONS WILL ACTIVATE SYSTEM.
FLIGHT (LAUNCH AND DEPLOYMENT)	LEAKAGE	SAFETY MARGINAL	LEAKAGE THROUGH VALVES. (LIKELY)	ASSURE LAUNCH LOADS DO NOT ALLOW LEAKAGE THROUGH VALVES.

OPERATING HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
REFURBISHMENT	LEAKAGE	SAFETY MARGINAL	LEAKAGE AT SYSTEM REFURBISHMENT. (UNLIKELY)	EVACUATE SYSTEM PRIOR TO REFURBISHMENT.

OPERATING HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT (LOADING)	PRESSURE	SAFETY CATASTROPHIC	EXCESS GHe PRESSURE DURING FILL RUPTURES TANK. (UNLIKELY)	PROVIDE OVERPRESSURE PROTECTION AND CONTROLS ON GSE. ASSURE PROCEDURES PRECLUDE OVERPRESSURE. PROVIDE BURST DISC AND RELIEF DEVICE AT 10% ABOVE MAXIMUM OPERATING. RELIEVE TO CLOSED VENT SYSTEM.
(OPERATIONS)		SAFETY CATASTROPHIC	PRESSURES INCREASE DUE TO UNCONTROLLED THERMAL CONDITIONS RUPTURES TANK. (UNLIKELY)	CONTROL THERMAL CONDITIONS OF TANK TO 100°F MAXIMUM UNDER ALL CONDITIONS. MONITOR TANK PRESSURE. PROVIDE OVERPRESSURE PROTECTION.
FLIGHT (LAUNCH)		SAFETY CATASTROPHIC	PRESSURE INCREASE DUE TO UNCONTROLLED THERMAL CONDITIONS RUPTURES TANK. (UNLIKELY)	CONTROL THERMAL CONDITIONS OF TANK TO 100°F MAXIMUM. MONITOR TANK PRESSURE. PROVIDE TANK OVERPRESSURE PROTECTION.
(REENTRY LANDING)		SAFETY CATASTROPHIC	PRESSURE INCREASE DUE TO UNCONTROLLED THERMAL CONDITIONS RUPTURES TANK. (UNLIKELY)	CONTROL THERMAL CONDITIONS OF TANK TO 100°F MAXIMUM. MONITOR TANK PRESSURE. PROVIDE TANK OVERPRESSURE PROTECTION.

OPERATING HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
POST FLIGHT	PRESSURE	SAFETY CRITICAL	RETAINED PRESSURE IN SYSTEM. (LIKELY)	EVACUATE SYSTEM PRIOR TO REFURBISHMENT. MONITOR FOR PRESSURE.

OPERATING HAZARDS ANALYSIS

PROPULSION - ACPS - BLOWDOWN MONO

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT (PROPELLANT LOADING)	ACCELERATION	SAFETY CRITICAL	RAPID FLOW CUTOFF OR FLOW START CAUSES HIGH PRESSURE SURGES IN FILL AND DRAIN SYSTEM. N_2H_4 SYSTEM . (LIKELY)	4:1 SAFETY FACTOR ON PLUMBING. PROVIDE FLEXIBILITY IN PLUMBING SUPPORT. SELECT VALVE OPERATING TIMES TO PRECLUDE HIGH SURGES. REDUCE FILL VELOCITY. IDENTIFY SURGE PEAK PRESSURE FOR DESIGN.
FLIGHT (LAUNCH AND DEPLOYMENT)	ACCELERATION	SAFETY CRITICAL	RAPID MOVEMENT OF N_2H_4 IN TANK. (UNLIKELY)	ASSURE MOVEMENT WILL NOT CAUSE RAPID PROPELLANT MOVEMENT.

OPERATING HAZARDS ANALYSIS

PROPULSION - ACPS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT	CONTAMINATION	SAFETY MARGINAL	INGESTION OF CONTAMINANTS INTO N_2H_4 TANK. (LIKELY)	PERFORM OPERATIONS IN CONTROLLED AREA. PROVIDE PROPELLANT FILTERING DEVICES. SAMPLE PROPELLANT AND TEST FOR CLEANLINESS. PROVIDE DRAIN AND FLUSH SYSTEM FOR CLEANING.
FLIGHT	CONTAMINATION	SAFETY MARGINAL	CLOGS FILTER AND CAUSES LOW FLOW RATE TO N_2H_4 THRUSTERS. (LIKELY)	PROVIDE FILTER DEVICES WITH SUFFICIENT CAPACITY AND BYPASS CAPABILITY
	CONTAMINATION	SAFETY CRITICAL	ISOLATION VALVE FAILS TO CLOSE AND THRUSTER CONTINUES OPERATION. (UNLIKELY)	PROVIDE FILTER DEVICE. PROVIDE SERIES ISOLATION VALVES.

OPERATING HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT (THROUGH PROPELLANT LOADING)	HEAT AND TEMPERATURE (HIGH)	SAFETY MARGINAL	N_2H_4 DISSOCIATES AT TEMPERATURES OF 228°F TO 234°F. (LIKELY)	MAINTAIN AMBIENT TEMPERATURE BELOW 110°F.
FLIGHT	(LOW)	SAFETY MARGINAL	N_2H_4 FREEZES AT 35°F AND PREVENTS SYSTEM OPERATION. (LIKELY)	PROVIDE SYSTEM THERMAL CONTROL. ASSURE OVER-HEAT PROTECTION.

OPERATING HAZARDS ANALYSIS

PROPULSION - ACPS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT	DISSOCIATION, CHEMICAL	SAFETY CRITICAL	CHEMICAL DISSOCIATION OF N_2H_4 CAUSES RUPTURE OF BLADDER. (LIKELY)	PROVIDE RELIEF DEVICE CONNECTED TO A CLOSED VENT SYSTEM. ASSURE PRESSURE DOES NOT EXCEED MAXIMUM OPERATING PRESSURE +10%.
	DISSOCIATION, CHEMICAL	SAFETY CRITICAL	REVERSE FLOW FROM LEAK TO THRUSTER CATALYST CAUSES HOT GASES TO BE DISCHARGED INTO ORBITER BAY. (UNLIKELY)	PROVIDE SOFT PROTECTIVE CAPS OVER THRUSTER NOZZLES TO PRECLUDE BACK FLOW. CAPS TO BLOW-OFF WHEN THRUSTERS OPERATED.
FLIGHT (REENTRY	DISSOCIATION, CHEMICAL	SAFETY CATASTROPHIC	N_2H_4 WILL DISSOCIATE AT TEMPERATURES OF 228°F TO 234°F. ORBITER BAY TEMPERATURE APPROXIMATELY 200°F. (LIKELY)	REPORT VALVE POSITIONS PRIOR TO RETRIEVAL AND MONITOR WHEN IN ORBITER BAY. MONITOR ORBITER BAY ATMOSPHERE. LEAKAGE NOT TO EXCEED TBD SCCS VALVES TBD SCCS TANK TBD SCCS FITTINGS

OPERATING HAZARDS ANALYSIS

PROPULSION - ACPS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
REFURBISHMENT	CONTAMINATION	SAFETY MARGINAL	INGESTION OF CONTAMINANTS INTO N_2H_4 TANK AND SYSTEM. (LIKELY)	PERFORM OPERATIONS IN CONTROLLED AREA. PROVIDE CONTROLS FOR CLOTHING AND EQUIPMENT
PREFLIGHT	CORROSION	SAFETY MARGINAL	EXPOSURE TO CORROSIVE ATMOSPHERE AND/OR FLUIDS. (LIKELY)	PERFORM OPERATIONS IN CONTROLLED AREA. ASSURE COMPATIBILITY OF MATERIALS AND FLUIDS. DO NOT USE TRICHLOR PRODUCTS TO CLEAN TITANIUM PARTS. ASSURE LEAK TEST SOLUTIONS ARE CORRECTLY REMOVED. USE GALVANIC CHART WHEN SELECTING MATERIALS. ASSURE PROTECTIVE COATINGS DO NOT REACT WITH SYSTEM FLUIDS.
REFURBISHMENT	CORROSION	SAFETY MARGINAL	EXPOSURE TO CORROSIVE ATMOSPHERE AND/OR FLUIDS. (LIKELY)	SAME AS PREFLIGHT. ASSURE CLEANING FLUIDS WILL NOT BE TRAPPED IN VALVES AND LINES.

OPERATING HAZARDS ANALYSIS

PROPULSION - ACPS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT	ELECTRICAL A. INADVERTENT ACTIVATION	SAFETY MARGINAL	ACTIVATION OF THE SYSTEM VALVES WILL CAUSE THE ACPS PROPELLANT SYSTEM TO BE DISPERSED. TOXICITY/FIRE/CONTAMINATION. (UNLIKELY)	PROVIDE ELECTRICAL INTERLOCKS TO PREVENT INADVERTENT ACTIVATION. PROVIDE SERIES ISOLATION AND THRUSTER SHUTOFF VALVES.
(FILL)	B. POWER SOURCE FAILURE	SAFETY MARGINAL	1. POWER SOURCE FAILURE MAY CAUSE RAPID SHUTDOWN DURING FILL WITH RESULTING SURGES. (LIKELY)	PROVIDE DUAL POWER SOURCE. DESIGN PROPELLANT FILL VALVES "FAIL CLOSED". DESIGN VENT VALVES TO "FAIL OPERATIONAL".
			2. POWER SOURCE FAILURE MAY CAUSE QUANTITY MEASURING SYSTEM TO BE INOPERATIVE ALLOWING OVERFILL. (LIKELY)	PROVIDE REDUNDANT QUANTITY MEASURING SYSTEM WITH SEPARATE POWER SOURCES.
	C. STATIC	SAFETY MARGINAL	PROPELLANT FLOW CREATES STATIC ELECTRICITY ON PLUMBING. (LIKELY)	DESIGN SYSTEM WITH GOOD GROUND PATHS. APPLY MIL-STD- FOR GROUNDING. PROVIDE GROUNDING GRIDS AS REQUIRED. PROVIDE LIGHTNING PROTECTION. GROUNDING PATHS FOR INSULATED SYSTEMS MUST EQUAL THAT OF UNINSULATED SYSTEMS.

OPERATING HAZARDS ANALYSIS

PROPULSION SYSTEM - ACPS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
FLIGHT	ELECTRICAL A. INADVERTENT ACTIVATION	SAFETY CATASTROPHIC	ACTIVATION OF THE TUG ACPS WHILE IN THE ORBITER BAY OR IN CLOSE PROXIMITY. (VERY UNLIKELY)	PROVIDE ELECTRICAL INTERLOCKS TO PREVENT INADVERTENT ACTIVATION. DESIGN SYSTEM SUCH THAT POSITIVE CREW ACTION IS REQUIRED TO ACTIVATE THE ACPS. PROVIDE SAFETY INTERLOCK WHILE TUG IS ATTACHED TO ORBITER BY MEANS OF AN ELECTROMECHANICAL DEVICE. ASSURE WIRING INSULATION WILL NOT ALLOW INADVERTENT ACTUATION. ASSURE CONNECTOR AND PIN SELECTION WILL PRECLUDE INADVERTENT ACTUATION. PROVIDE MONITORS TO INDICATE SAFING STATUS.
	B. POWER SOURCE FAILURE	SAFETY MARGINAL	POWER SOURCE FAILURE MAY CAUSE ACPS SHUTDOWN. (LIKELY)	PROVIDE SECONDARY POWER SOURCE.
				ASSURE PROVISIONS ARE MADE TO DEACTIVATE SYSTEMS WHICH CAN PROVIDE AN IGNITION SOURCE ON CRASH IMPACT

OPERATING HAZARDS ANALYSIS

PROPULSION - ACPS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT (PROPELLANT FILL)	EXPLOSION	SAFETY CRITICAL	OVER PRESSURIZATION DURING THE FILL CYCLE AND EXPULSION BLADDER RUPTURES. (UNLIKELY)	PROVIDE PRESSURE RELIEF IN FILL SYSTEM. MONITOR TANK PRESSURE. PROVIDE PRESSURE RELIEF OF TANK AT 10% ABOVE MAXIMUM OPERATING. RELIEVE TO CLOSED VENT SYSTEM.
(GN_2 FILL)	EXPLOSION	SAFETY CRITICAL	OVER PRESSURIZATION DURING FILL CYCLE. (UNLIKELY)	SAME AS PROPELLANT FILL.
(PRIOR TO INSTALLATION)	EXPLOSION	SAFETY CRITICAL	DISSOCIATION OF N_2H_4 CAUSES OVERPRESSURE AND EXPULSION BLADDER RUPTURES. (LIKELY)	VENT TO H_2 VENT LINE. PROVIDE PRESSURE RELIEF AT 10% ABOVE MAXIMUM PRESSURE. MAINTAIN TEMPERATURE BELOW 110°F.
(AFTER INSTALLATION)	EXPLOSION	SAFETY CRITICAL	DISSOCIATION OF N_2H_4 CAUSES OVERPRESSURE AND EXPULSION BLADDER RUPTURES. (LIKELY)	MAINTAIN TEMPERATURE BELOW 110°F.

OPERATING HAZARDS ANALYSIS

PROPULSION - ACPS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT (PROPELLANT LOADING)	FIRE	SAFETY CATASTROPHIC	N_2H_4 LEAK/SPILL WITH IGNITION. (UNLIKELY)	ASSURE SYSTEM INTEGRITY PRIOR TO PROPELLANT LOADING. LEAKAGE NOT TO EXCEED TBD SCCS VALVES TBD SCCS TANK TBD SCCS FITTINGS DESIGN TO ELIMINATE SOURCES OF IGNITION. DESIGN SYSTEM TO MINIMIZE POINTS OF POTENTIAL LEAKAGE. ASSURE CORRECT FIRE PROTECTION EQUIPMENT IS AVAILABLE. ASSURE FUEL CONTAINMENT AND DRAINAGE ARE ADEQUATE. ASSURE SYSTEM INTEGRITY AFTER LOADING.
(INSTALLATION)	FIRE	SAFETY CRITICAL	N_2H_4 LEAK/SPILL WITH IGNITION. (UNLIKELY)	ASSURE PROCEDURAL OPERATIONS DO NOT CREATE HAZARDOUS CONDITIONS. ASSURE INTEGRITY OF "MAKE UP" CONNECTIONS PRIOR TO CREATING A "WET" SYSTEM. ASSURE CORRECT VALVE POSITIONING PRIOR TO CREATING A "WET" SYSTEM. ASSURE SYSTEM INTEGRITY AFTER LOADING AND CREATING A "WET" SYSTEM.
FLIGHT (LAUNCH)	FIRE	SAFETY CATASTROPHIC	N_2H_4 LEAK/SPILL WITH IGNITION (N_2H_4 WILL DISSOCIATE IN A GN_2 OR GHe ATMOSPHERE WITH 38% N_2H_4 AT 228°F TO 234°F. (UNLIKELY)	ASSURE LAUNCH ACCELERATIONS DO NOT AFFECT N_2H_4 SYSTEM. LEAKAGE NOT TO EXCEED TBD SCCS VALVES TBD SCCS TANK TBD SCCS FITTINGS PURGE ORBITER BAY WITH GN_2 PRIOR TO LAUNCH. MONITOR ORBITER BAY ATMOSPHERE. MONITOR VALVE POSITIONS.

OPERATING HAZARDS ANALYSIS

PROPULSION - ACPS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
(REENTRY AND LANDING)	FIRE	SAFETY CATASTROPHIC	N_2H_4 LEAK/SPILL (N_2H_4 WILL DISSOCIATE AT TEMPERATURES OF 228°F TO 234°F) ORBITER BAY TEMPERATURE APPROXIMATELY 200°F. (UNLIKELY)	MONITOR ORBITER BAY ATMOSPHERE. LEAKAGE NOT TO EXCEED TBD SCCS VALVES TBD SCCS TANK TBD SCCS FITTINGS REPORT VALVE POSITIONS PRIOR TO RETRIEVAL AND MONITOR WHEN IN ORBITER BAY.
REFURBISHMENT	FIRE	SAFETY MARGINAL	IGNITION OF TRAPPED N_2H_4. (UNLIKELY)	ASSURE ADEQUATE DRAIN AND FLUSH PROCEDURES.

OPERATING HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT (PROPELLANT LOADING)	LEAKAGE	SAFETY CRITICAL	LEAKAGE THROUGH VALVES OR CONNECTIONS CAUSES TOXICITY/FIRE/CONTAMINATION. (UNLIKELY)	SYSTEM LEAKAGE RATES NOT TO EXCEED TBD SCCS VALVES TBD SCCS TANK TBD SCCS FITTINGS MONITOR AREA FOR LEAKAGE INDICATION. PROTECTIVE CLOTHING TO BE WORN. PERFORM OPERATIONS IN A CONTROLLED AREA. UPON COMPLETION OF LOADING, SAMPLE ALL FLANGES, ETC. FOR LEAKAGE. CAP ALL PORTS.
(INSTALLATION)		SAFETY CRITICAL	LEAKAGE THROUGH VALVES OR CONNECTIONS CAUSES TOXICITY/FIRE/CONTAMINATION. (UNLIKELY)	PROVIDE SERIES VALVES WHOSE OPERATIONAL POSITION PREVENTS LEAKAGE. LEAK CHECK THE SYSTEM PRIOR TO MAKING THE SYSTEM WET. ASSURE VALVE POSITIONS. PROTECTIVE CLOTHING REQUIRED. PERFORM OPERATIONS IN A CONTROLLED AREA. UPON COMPLETION OF OPERATIONS, SAMPLE ALL FLANGES, ETC., FOR LEAKAGE.

OPERATING HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT (OPERATIONS)	LEAKAGE	SAFETY CRITICAL	LEAKAGE THROUGH VALVES OR CONNECTIONS CAUSES TOXICITY/FIRE/CONTAMINATION. (UNLIKELY)	ASSURE NO OPERATIONAL SIGNALS ARE SENT TO SYSTEM. ASSURE NO INADVERTENT SIGNALS/OPERATIONS WILL ACTIVATE SYSTEM. MONITOR AREA FOR LEAKAGE ESTABLISH SAMPLING FREQUENCY REQUIREMENTS.
FLIGHT (LAUNCH AND DEPLOYMENT)	LEAKAGE	SAFETY CRITICAL	LEAKAGE THROUGH VALVES CAUSES TOXICITY/FIRE/CONTAMINATION. (UNLIKELY)	ASSURE LAUNCH LOADS DO NOT ALLOW LEAKAGE THROUGH VALVES. ASSURE LATCHING METHODS WILL WITHSTAND LAUNCH LOADS.
(RECOVERY)	LEAKAGE	SAFETY CRITICAL	LEAKAGE THROUGH VALVES CAUSES UNPROGRAMMED MOTION WITHIN TBD FEET OF ORBITER. (LIKELY)	PROVIDE SERIES VALVES WHOSE OPERATIONAL POSITION PREVENTS LEAKAGE. PROVIDE VALVE POSITION MONITOR INFORMATION TO CREW.

OPERATING HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
FLIGHT (RETRIEVAL AND LANDING)	LEAKAGE	SAFETY CRITICAL	LEAKAGE THROUGH VALVES AND FITTINGS CAUSES TOXICITY/FIRE/CONTAMINATION. (UNLIKELY)	PROVIDE SERIES VALVES WHOSE OPERATIONAL POSITION PREVENTS LEAKAGE. PROVIDE VALVE POSITION MONITOR INFORMATION TO CREW.
POST FLIGHT	LEAKAGE	SAFETY CRITICAL	LEAKAGE AT TUG SEPARATION. (LIKELY)	EVACUATE SYSTEM PRIOR TO SEPARATION. PROTECTIVE CLOTHING REQUIRED. MONITOR FOR LEAKAGE.
PREFLIGHT STORAGE	MOISTURE	SAFETY MARGINAL	DEGRADATION OF CATALYST BED DUE TO MOISTURE ABSORPTION. (LIKELY)	PROVIDE CAPS ON THRUSTER OPENINGS WITH DESSICANTS TO PRECLUDE ENTRANCE OF MOISTURE. ESTABLISH INSPECTION FREQUENCY TO ASSURE DESSICANT INTEGRITY.

OPERATING HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT (PROPELLANT LOADING)	PRESSURE	SAFETY CATASTROPHIC	EXCESS GN_2 PRESSURE DURING FILL RUPTURES TANK. (UNLIKELY)	PROVIDE OVERPRESSURE PROTECTION AND CONTROLS ON GSE. ASSURE PROCEDURES PRECLUDE OVERPRESSURE. PROVIDE BURST DISC AND RELIEF DEVICE AT 10% ABOVE MAXIMUM OPERATING RELIEVE TO CLOSED VENT SYSTEM.
(OPERATIONS)		SAFETY CATASTROPHIC	GN_2/N_2H_4 PRESSURE INCREASE DUE TO UNCONTROLLED THERMAL CONDITIONS RUPTURES TANK. (LIKELY)	CONTROL THERMAL CONDITIONS OF TANK TO 110°F MAXIMUM UNDER ALL CONDITIONS. MONITOR TANK PRESSURE. PROVIDE OVERPRESSURE PROTECTION.
FLIGHT (LAUNCH)		SAFETY CATASTROPHIC	GN_2/N_2H_4 PRESSURE INCREASE DUE TO UNCONTROLLED THERMAL CONDITIONS RUPTURES TANK. (LIKELY)	CONTROL THERMAL CONDITIONS OF TANK TO 110°F MAXIMUM. MONITOR TANK PRESSURE. PROVIDE TANK OVERPRESSURE PROTECTION.
(REENTRY LANDING)		SAFETY CATASTROPHIC	GN_2/N_2H_4 PRESSURE INCREASE DUE TO UNCONTROLLED THERMAL CONDITIONS RUPTURES TANK. (LIKELY)	CONTROL THERMAL CONDITIONS OF TANK TO 110°F MAXIMUM. MONITOR TANK PRESSURE. PROVIDE TANK OVERPRESSURE PROTECTION.

OPERATING HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
POST FLIGHT	PRESSURE	SAFETY CRITICAL	RETAINED PRESSURE IN SYSTEM. (LIKELY)	EVACUATE SYSTEM PRIOR TO SEPARATION. PROTECTIVE CLOTHING REQUIRED. MONITOR FOR PRESSURE.
PREFLIGHT (PROPELLANT LOADING)	TOXICITY	SAFETY CRITICAL	LEAKAGE/SPILL OF N_2H_4 CAUSES TOXIC ATMOSPHERE. OR CLOSED VENT SYSTEM FAILS. (LIKELY)	PROVIDE PROTECTIVE CLOTHING. MONITOR AREA FOR LEAKAGE. UNDERSTAND VAPOR DISPERSION CHARACTERISTICS FOR AREA. ASSURE EMERGENCY EQUIPMENT IS SATISFACTORY. ASSURE EMERGENCY PROCEDURES ARE AVAILABLE. DESIGN TO CONTAIN PTV PROPELLANT PLUS 10%, DIKE AREA. PROVIDE SCRUBBER FOR VENT SYSTEM.
(INSTALLATION)		SAFETY CRITICAL	LEAKAGE/SPILL OF N_2H_4 CAUSES TOXIC ATMOSPHERE. (UNLIKELY)	PROVIDE PROTECTIVE CLOTHING. MONITOR AREA FOR LEAKAGE. UNDERSTAND VAPOR DISPERSION CHARACTERISTICS FOR AREA (INCLUDE A/C OUTLET). ASSURE EMERGENCY PROCEDURES ARE AVAILABLE. ASSURE EMERGENCY EQUIPMENT IS SATISFACTORY.

OPERATING HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT (OPERATIONS)	TOXICITY	SAFETY MARGINAL	LEAKAGE OF N_2H_4 CAUSES TOXIC ATMOSPHERE. (UNLIKELY)	MONITOR AREA FOR LEAKAGE. ASSURE EMERGENCY EQUIPMENT IS SATISFACTORY. ASSURE SYSTEM IS NOT ACTIVATED.
FLIGHT (LAUNCH, RETRIEVAL, REENTRY AND LANDING)	TOXICITY	SAFETY CRITICAL	LEAKAGE OF N_2H_4 CAUSES TOXIC ATMOSPHERE IN BAY. (UNLIKELY)	MONITOR BAY FOR N_2H_4. ASSURE N_2H_4 CANNOT ENTER ORBITER CABIN OR CONTAMINATE ORBITER AIR CONDITIONING.
REFURBISHMENT	TOXICITY	SAFETY MARGINAL	RESIDUAL N_2H_4 CAUSES TOXIC ATMOSPHERE. (LIKELY)	ASSURE DRAIN AND FLUSH OF COMPONENTS. TEST COMPONENTS FOR RESIDUALS PRIOR TO REMOVING PROTECTIVE CLOTHING. ASSURE PROCEDURES COVER ALL SAFETY ASPECTS.

OPERATING HAZARDS ANALYSIS AMBIENT HELIUM PRESSURIZATION

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT	CONTAMINATION	SAFETY MARGINAL	INGESTION OF CONTAMINANTS INTO TANK. (LIKELY)	PERFORM OPERATIONS IN CONTROLLED AREA. PROVIDE FILTERING DEVICES. SAMPLE AND TEST FOR CLEANLINESS.
FLIGHT	CONTAMINATION	SAFETY MARGINAL	CLOGS FILTER AND CAUSES LOW FLOW RATE. (LIKELY)	PROVIDE FILTER DEVICES WITH SUFFICIENT CAPACITY AND BYPASS CAPABILITY.
	CONTAMINATION	SAFETY CRITICAL	VALVE FAILS TO CLOSE AND CONTINUES PRESSURIZATION (UNLIKELY)	PROVIDE FILTER DEVICE. PROVIDE ORIFICE IN SERIES WITH VALVE. PROVIDE VENT SYSTEM FOR TANKS.

OPERATING HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
REFURBISHMENT	CONTAMINATION	SAFETY MARGINAL	INGESTION OF CONTAMINANTS INTO TANKS AND SYSTEM. (LIKELY)	PERFORM OPERATIONS IN CONTROLLED AREA. PROVIDE CONTROLS FOR CLOTHING AND EQUIPMENT.
PREFLIGHT	CORROSION	SAFETY MARGINAL	EXPOSURE TO CORROSIVE ATMOSPHERE AND/OR FLUIDS. (LIKELY)	PERFORM OPERATIONS IN CONTROLLED AREA. ASSURE COMPATIBILITY OF MATERIALS AND FLUIDS. DO NOT USE TRICHLOR PRODUCTS TO CLEAN TITANIUM PARTS. ASSURE LEAK TEST SOLUTIONS ARE CORRECTLY REMOVED. USE GALVANIC CHART WHEN SELECTING MATERIALS. ASSURE PROTECTIVE COATINGS DO NOT REACT WITH SYSTEM FLUIDS.
REFURBISHMENT	CORROSION	SAFETY MARGINAL	EXPOSURE TO CORROSIVE ATMOSPHERE AND/OR FLUIDS. (LIKELY)	SAME AS PREFLIGHT. ASSURE CLEANING FLUIDS WILL NOT BE TRAPPED IN VALVES AND LINES.

OPERATING HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT	ELECTRICAL A. INADVERTENT ACTIVATION	SAFETY MARGINAL	ACTIVATION OF THE SYSTEM VALVES WILL CAUSE THE MAIN TANKS TO BE PRESSURIZED. (VERY UNLIKELY)	PROVIDE ELECTRICAL INTERLOCKS TO PREVENT INADVERTENT ACTIVATION. PROVIDE SERIES ISOLATION AND THRUSTER SHUTOFF VALVES.
	B. STATIC	SAFETY MARGINAL	GAS FLOW CREATES STATIC ELECTRICITY ON PLUMBING. (LIKELY)	DESIGN SYSTEM WITH GOOD GROUND PATHS. APPLY MIL-STD- FOR GROUNDING. PROVIDE GROUNDING GRIDS AS REQUIRED. PROVIDE LIGHTNING PROTECTION. GROUNDING PATHS FOR INSULATED SYSTEMS MUST EQUAL THAT OF UNINSULATED SYSTEMS.

OPERATING HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
FLIGHT	POWER SOURCE FAILURE	SAFETY MARGINAL	POWER SOURCE FAILURE MAY CAUSE SHUTDOWN. (LIKELY)	PROVIDE SECONDARY POWER SOURCE.
				ASSURE PROVISIONS ARE MADE TO DEACTIVATE SYSTEMS WHICH CAN PROVIDE AN IGNITION SOURCE ON CRASH IMPACT.

OPERATING HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT (FILL)	EXPLOSION	SAFETY CRITICAL	OVER PRESSURIZATION DURING THE FILL CYCLE AND TANK RUPTURES. (UNLIKELY)	PROVIDE PRESSURE RELIEF IN FILL SYSTEM. MONITOR TANK PRESSURE. PROVIDE PRESSURE RELIEF OF TANK AT 10% ABOVE MAXIMUM OPERATING. RELIEVE TO VENT SYSTEM.

OPERATING HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT (THROUGH PROPELLANT LOADING)	HEAT AND TEMPERATURE (HIGH)	SAFETY MARGINAL	PRESSURE INCREASES AND GHe TANK RUPTURES. (VERY UNLIKELY)	MAINTAIN AMBIENT TEMPERATURE BELOW 110°F. PROVIDE VENT BURST DISC OR MONITOR PRESSURE AND ACTIVATE TO MAIN TANK TO REDUCE PRESSURE.
FLIGHT (REENTRY AND LANDING)	(HIGH)			(SAME AS ABOVE)

OPERATING HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT (LOADING)	LEAKAGE	SAFETY CRITICAL	LEAKAGE THROUGH VALVES OR CONNECTIONS. (UNLIKELY)	SYSTEM LEAKAGE RATES NOT TO EXCEED TBD SCCS VALVES TBD SCCS TANK TBD SCCS FITTINGS MONITOR AREA FOR LEAKAGE INDICATION. UPON COMPLETION OF LOADING, SAMPLE ALL FLANGES,ETC. FOR LEAKAGE. CAP ALL PORTS. LEAK CHECK THE SYSTEM PRIOR TO MAKING THE SYSTEM WET. ASSURE VALVE POSITIONS.

OPERATING HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT (OPERATIONS)	LEAKAGE	SAFETY MARGINAL	LEAKAGE THROUGH VALVES OR CONNECTIONS. (UNLIKELY)	ASSURE NO OPERATIONAL SIGNALS ARE SENT TO SYSTEM. ASSURE NO INADVERTENT SIGNALS/ OPERATIONS WILL ACTIVATE SYSTEM.
FLIGHT (LAUNCH AND DEPLOYMENT)	LEAKAGE	SAFETY MARGINAL	LEAKAGE THROUGH VALVES. (UNLIKELY)	ASSURE LAUNCH LOADS DO NOT ALLOW LEAKAGE THROUGH VALVES.

OPERATING HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
REFURBISHMENT	LEAKAGE	SAFETY MARGINAL	LEAKAGE AT SYSTEM REFURBISHMENT. (UNLIKELY)	EVACUATE SYSTEM PRIOR TO SEPARATION. PROTECTIVE CLOTHING REQUIRED. MONITOR FOR LEAKAGE.

OPERATING HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
PREFLIGHT (LOADING)	PRESSURE	SAFETY CATASTROPHIC	EXCESS GHe PRESSURE DURING FILL RUPTURES TANK. (VERY UNLIKELY)	PROVIDE OVERPRESSURE PROTECTION AND CONTROLS ON GSE. ASSURE PROCEDURES PRECLUDE OVERPRESSURE. PROVIDE BURST DISC AND RELIEF DEVICE AT 10% ABOVE MAXIMUM OPERATING. RELIEVE TO CLOSED VENT SYSTEM.
(OPERATIONS)		SAFETY CATASTROPHIC	PRESSURES INCREASE DUE TO UNCONTROLLED THERMAL CONDITIONS RUPTURES TANK. (LIKELY)	CONTROL THERMAL CONDITIONS OF TANK TO 110°F MAXIMUM UNDER ALL CONDITIONS. MONITOR TANK PRESSURE. PROVIDE OVERPRESSURE PROTECTION.
FLIGHT (LAUNCH)		SAFETY CATASTROPHIC	PRESSURE INCREASE DUE TO UNCONTROLLED THERMAL CONDITIONS RUPTURES TANK. (LIKELY)	CONTROL THERMAL CONDITIONS OF TANK TO 110°F MAXIMUM. MONITOR TANK PRESSURE. PROVIDE TANK OVERPRESSURE PROTECTION.
(REENTRY LANDING)		SAFETY CATASTROPHIC	PRESSURE INCREASE DUE TO UNCONTROLLED THERMAL CONDITIONS RUPTURES TANK. (LIKELY)	CONTROL THERMAL CONDITIONS OF TANK TO 110°F MAXIMUM. MONITOR TANK PRESSURE. PROVIDE TANK OVERPRESSURE PROTECTION.

OPERATING HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
POST FLIGHT	PRESSURE	SAFETY CRITICAL	RETAINED PRESSURE IN SYSTEM. (LIKELY)	EVACUATE SYSTEM PRIOR TO REFURBISHMENT. MONITOR FOR PRESSURE.

OPERATING HAZARDS ANALYSIS

AVIONICS - BATTERY

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
FLIGHT (LAUNCH AND DEPLOYMENT)	ACCELERATION	SAFETY MARGINAL	LAUNCH AND DEPLOYMENT LOADS CAUSE ELECTROLYTE TO SPILL. (LIKELY)	SELECT BATTERY CELLS TO CONTAIN ELECTROLYTE IN ALL MODES. PROVIDE CONTAINER TO RETAIN SPILLED ELECTROLYTE.
ALL PHASES	CORROSION	SAFETY MARGINAL	ELECTROLYTE LEAK/SPILL. (LIKELY)	SELECT BATTERY CELLS TO CONTAIN ELECTROLYTE IN ALL MODES. PROVIDE CONTAINER TO RETAIN SPILLED ELECTROLYTE AND BE CORROSION RESISTANT.
PREFLIGHT (CHARGING)	CHEMICAL DISSOCIATION	SAFETY MARGINAL	RAPID CHARGING CAUSES H_2 GAS EVOLUTION AND CELL RUPTURE. (LIKELY)	ASSURE CHARGING RATE AND OVERCHARGE LEVEL/TIME ARE CONTROLLED TO PRECLUDE GENERATION OF EXCESS H_2 GAS. PROVIDE CONTAINER TO ACCEPT GAS VOLUME EQUAL TO ALL CELLS.
FLIGHT (LAUNCH, REENTRY, AND LANDING)	CHEMICAL DISSOCIATION	SAFETY MARGINAL	INCREASED HEAT CAUSES EXCESSIVE PRESSURE AND CELL RUPTURE. (LIKELY)	ASSURE CHARGING RATE AND OVERCHARGE LEVEL/TIME ARE CONTROLLED TO PRECLUDE GENERATION OF EXCESS H_2 GAS. PROVIDE CONTAINER TO ACCEPT GAS VOLUME EQUAL TO ALL CELLS.

OPERATING HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
FLIGHT (DEPLOYMENT RETRIEVAL)	ELECTRICAL POWER SOURCE FAILURE	SAFETY MARGINAL	FAULTY CONNECTOR OR CONNECTION (LIKELY)	PROVIDE ALTERNATE BATTERY FOR EMERGENCY CIRCUITS.
PREFLIGHT (CHARGING)	EXPLOSION	SAFETY MARGINAL	RAPID CHARGE OR OVERCHARGE CAUSES H_2 GAS WITH OVERPRESSURE AND CELL RUPTURE. (LIKELY)	SELECT CELLS TO ACCEPT OVERPRESSURE. ASSURE CHARGING RATE AND OVERCHARGE LEVEL/TIME ARE CONTROLLED TO PRECLUDE GENERATION OF EXCESS H_2 GAS. PROVIDE CONTAINER TO ACCEPT GAS VOLUME EQUAL TO ALL CELLS.
PREFLIGHT (CHARGING) (PROPELLANT LOADING)	HEAT AND TEMPERATURE (HIGH)	SAFETY MARGINAL	RAPID CHARGE OR OVERCHARGE CAUSES INCREASED HEAT WITH OVERPRESSURE AND CELL RUPTURE. (LIKELY)	(SAME AS PREFLIGHT - EXPLOSION.) SELECT CELLS WITHIN TEMPERATURE RANGES EXPECTED.
FLIGHT (LAUNCH, DEPLOYMENT, RETRIEVAL, REENTRY, LANDING)	(LOW)	SAFETY MARGINAL	CELLS FREEZE AND RUPTURE WITH ELECTROLYTE SPILL. (LIKELY)	ASSURE THERMAL CONTROL OVER TEMPERATURE RANGES EXPECTED.

OPERATING HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL
ALL	LEAKAGE	SAFETY MARGINAL	LEAKAGE OF ELECTROLYTE OR H_2 GAS. (LIKELY)	PROVIDE CONTAINER TO ACCEPT GAS VOLUME EQUAL TO ALL CELLS AND RETAIN ELECTROLYTE WITHOUT SUBSEQUENT CORROSION.
ALL	PRESSURE	SAFETY MARGINAL	HIGH PRESSURE CAUSES CELL RUPTURE. (LIKELY)	(SAME AS LEAKAGE.) SELECT CELLS WITH CORRECT PRESSURE CHARACTERISTICS.
PREFLIGHT (ALL PHASES) REFURBISHMENT	TOXICITY	SAFETY MARGINAL	LEAKAGE/SPILL OF ELECTROLYTE. (LIKELY)	PROVIDE CONTAINER TO ACCEPT GAS VOLUME. ASSURE BLEED-OFF OF PRESSURE PRIOR TO OPENING CONTAINER. PROVIDE EMERGENCY EQUIPMENT. ASSURE EMERGENCY PROCEDURES ARE PROVIDED.
FLIGHT	NOISE AND VIBRATION	SAFETY MARGINAL	VIBRATION CAUSES PLATES TO SHORT WITH SUBSEQUENT PRESSURE INCREASE AND CELL RUPTURE. (LIKELY)	(SAME AS LEAKAGE.)

TABLE 6.2.2-1

THERMAL CONTROL

OPTION: 1

MISSION TIME: 36

ITEM NO.	NAME	$\lambda x10^{-6}$	α	MODE	β	N	T	ΣQ	$Qx10^{6}$	REMARKS
1.0	Regulator	2.5	.1	Low Press.	1	1	1.7		.4	Active During tug/oss mate only during reentry.
			.9	High Press					0	Redundant to S/O valve - press switch control.
								1		
2.0	S/O Valve, H_2 Tank Purge	1.0	.9	Leakage	.1	1	68.9		6.2	
			.05	Fail to Open	1	1	1.7		.08	T for tug/oss mate only during reentry.
			.05	Fail to Close	1	1	1.7		.08	T for tug/oss mate only during reentry.
								6		
3.0	Press. Switch	1.1	.5	No Output	1	1	1.7		.9	T for tug/oss mate only during reentry.
			.5	Wrong Output	1	1	1.7		.9	T for tug/oss mate only during reentry.
								2		
4.0	Relief Valve	2.6	.9	Leakage	.1	1	1.7		3.9	T for tug/oss mate only during reentry.
			.05	Fail to Open	0	1	0		0	N/A Protective Device.
			.05	Fail to Open	0	1	0		0	N/A Protective Device.
								4		
5.0	S/O Valve Purge Exit	1.0	.9	Leakage	.1	1	1.7		.1	T for tug/oss mate only during reentry.
			.05	Fail to Open	1	1	1		.05	One cycle per flight.
			.05	Fail to Close	1	1	1		.05	
								1		
6.0	Disconnect	1.96	.60	Leakage (INT)	0	1	0		0	N/A Open Q.D.
			.20	Leakage (EXT)	.1	1	1.7		.7	T for tug/oss mate only during reentry.
			.10	Fail to Conn.	1	1	1		.11	One cyc per mission.

TABLE 6.2.2-1 (CONT)

ITEM NO.	NAME	$\lambda x10^{-6}$	α	MODE	β	N	T	ΣQ	$Qx10^{6}$	REMARKS
			.10	Fail to Dis-con	1	1	1	1	.1	One cyc per mission.
7.0	4" Evacuation Valve	3.4	.90	Leakage	.1	1	29.4	9		T for tug/oss mate only.
			.05	Fail to Open	1	1	1		.05	One cyc per mission.
			.05	Fail to Close	1	1	1	9	.05	One cyc per mission.
8.0	Same as 7.0							9		
9.0	Same as 2.0							6		
10.0	Same as 3.0							2		
11.0	Same as 5.0							1		
12.0	Same as 6.0							1		
13.0	Same as 4.0							4		
14.0	Same as 7.0							9		
15.0	Pneu Control Module									
15.1	S/O Valve	1.0	.9	Leakage	.1	6	68.9		37.2	
			.05	Fail to Open	1	6	1		.3	One cyc per mission.
			.05	Fail to Close	1	6	1	38	.3	One cyc per mission.
15.2	Check Valve	.27	.90	Leakage	.1	6	29.4		4.2	T for tug/oss mate only.
			.05	Fail to Open	1	1	1		.05	One cyc per mission.
			.05	Fail to close	1	1	1	4	.05	One cyc per mission.
								98		

R = .999902

TABLE 6.2.4-1

MAIN ENGINE SUPPORT

OPTION: 1

MISSION TIME: 36

ITEM NO.	NAME	$\lambda x10^{-6}$	α	MODE	β	N	T	ΣQ	$Qx10^{6}$	REMARKS
3.1	LH_2 Feed Valve N/O	3.4	.90	Leakage	0				0	Redundant to Eng. S/O Valve.
			.05	Fail to Close	0				0	Redundant to Eng. S/O Valve.
			.05	Fail to Open	1	1	1.0		.170	
	Relief Valve	.27	.90	Leakage	0				0	No effect, internal to sys.
			.05	Fail to Close	0				0	No effect, internal to sys.
			.05	Fail to Open	1	1	1.0		.0135	Possible Ruptured feed line.
								1		
3.2	LO_2 Feed Valve	(SAME AS ABOVE)						1		
4.1	Vent & Relief Valve H_2	5.7	.70	Leakage	.1	2	68.9		55.0	
			.15	Fail to Open	0				0	Pneu. Boost Open
			.15	Fail to Close	0				0	Pneu. Boost Close.
								55.0		
4.2	S/O Valve Module H_2				0	4			0	Quad. redundant.
4.3	Vent VL, Horizontal H_2	3.4	.90	Leakage	0	2			0	Redundant to check Q.D. for flight for OSS/Tug mated redundant to OSS Q.D.
			.05	Fail to Open	0				0	Ground usage only.
			.05	Fail to Close	0				0	Ground usage only.
								0		
4.4	Disconnect H_2	1.96	.60	Leakage (INT)	0				0	No effect: vent gas escape to vaccum. During OSS/Tug mate: valve open

TABLE 6.2.4-1 (CONT)

ITEM NO.	NAME	$\lambda x10^{-6}$	α	MODE	β	N	T	ΣQ	$Qx10^{6}$	REMARKS
			.20	Leakage (EXT)	.1	1			.392	Check safty - volume not critical.
			.10	Fail to Conn.	1	1	1.0		.196	Loss of mission SFP
			.10	Fail to Discon.	1	1	1.0	1	.196	Loss of mission SFP
4.5	Vent & Relief Valve LO_2	(SAME AS 4.1)						55		
4.6	S/O Valve Module LO_2	(SAME AS 4.2)						0		
4.7	Disconnect (Vent) LO_2	(SAME AS 4.4)						1		
5.1	Fill & Drain Valve LH_2	3.4	.90	Leakage	0	1			0	Redundant to 5.3 QD during free Tug. Redundant to OSS QD during OSS/Tug mate.
			.05	Fail to Close	0	1			0	N/A, service prior to launch.
			.05	Fail to Open	0	1		0	0	N/A, service prior to launch.
5.2	Drain (Horizontal)	3.4	.90	Leakage	0	2			0	*(see above).
			.05	Fail to Close	0	2			0	Emergence usage only.
			.05	Fail to Open	0	2		0	0	Emergence usage only.
5.3	Disconnect LH_2 Fill/Drain	1.96	.60	Leakage (INT)	0	1			0	Redundant to S/O 5.1, 5.2 free tug N/A during OSS/Tug mate.

TABLE 6.2.4-1 (CONT)

ITEM NO.	NAME	$\lambda x10^{-6}$	α	MODE	β	N	T	ΣQ	$Qx10^{6}$	REMARKS
			.20	Leakage (EXT)	.1	1	68.9		0	Check safety-volume not critical.
			.10	Fail to Conn.	1	1	1		.2	Loss of mission SFP
			.10	Fail to Dis-con.	1	1	1	3	.2	Loss of mission SFP
5.4	Fill & Drain Valve LO_2	(SAME AS 5.1)						0		
5.5	Abort Dump Valves	3.4	.90	Leakage	.1	2	29.4		18	Redundant to 5.7 QD during free tug, T for OSS/Tug mate.
			.05	Fail to Close	0				0	N/A emergence use only.
			.05	Fail to Open	0			18	0	N/A emergence use only.
5.6	Disconnect LO_2 fill/Drain	(SAME AS 5.3)						3		
5.7	Disconnect LO_2 Abort Dump	1.96	.60	Leakage (INT)	0	1			0	Redundant to 5.5 during free flight for OSS/Tug mate, valve open.
			.20	Leakage (EXT)	0	1			0	N/A emergence condition only.
			.10	Fail to Conn.	1	1	1		.2	Loss of mission SFP
			.10	Fail to Dis-con.	1	1	1	1	.2	Loss of mission SFP
6.0	Pneu. Vl. Module					22				
6.1	S/O Valve (2 req'd)	1.0	.90	Leakage	.1	44	68.9		273	
			.05	Fail to Open	.1	44	68.9		152	
			.05	Fail to Close	.1	44	68.9	577	152	

TABLE 6.2.4-1 (CONT)

ITEM NO.	NAME	$\lambda x10^{-6}$	α	MODE	β	N	T	ΣQ	$Qx10^{6}$	REMARKS
6.2	Check Valve	.27	.90	Leakage	.1	44	29.4		31.4	T for launch/decent only
			.05	Fail to Open	1	44	39.5		23.4	T for tug free flight only.
			.05	Fail to Close	1	44	29.4		17.5	T for launch/decent only
								72		
7.0	P.U. Closed Loop Capacitance	6.2	1.0	All	.01	1	68.9		4.2	
								4		
8.1	Disconnect He Fill	1.96	.60	Leakage (INT)	0	1			0	Redundant to check valve 8.1.1.
			.20	Leakage (EXT)	.1	1	68.9		27	
			.10	Fail to Conn.	1	1	1.0		.2	
			.10	Fail to Dis-con.	1	1	1.0		.2	
								27		
8.1.1	Check Valve He Fill	.27	.90	Leakage	0				0	Redundant to 8.1 Q.D.
			.05	Fail to Open	1	2	13.7		.4	T for purge only.
			.05	Fail to Close	1	2	13.7		.4	T for purge only.
								1		
8.2	Burst Disk/Relief Valve Assy.	.5			0				0	Internal Redundancy.
								0		
8.3	Tank, He Ambient Pressurization	.05	1.0	Leakage	1	5	68.9		17.2	
								17		
8.4	Regulator Module			All	0				0	Internal Redundant.
								0		
8.5	Plenum	.05	1	Leakage	1	1	68.9		3.45	
								4		

TABLE 6.2.4-1 (CONT)

ITEM NO.	NAME	$\lambda x10^{-6}$	α	MODE	β	N	T	ΣQ	$Qx10^{6}$	REMARKS
8.6	LH_2 Repress VL	1.0	.90	Leakage	.1	1	68.9		6.2	
			.05	Fail to Open	1	1	1		.05	T for repress time.
			.05	Fail to Close	1	1	1		.05	T for repress time.
								6		
8.7	LO_2 Repress/Press Module									
8.7.1	Repress S/O Valve	1.0	.90	Leakage	.1	1	68.9		6.2	
			.05	Fail to Open	1	1	1		.05	Repress time only.
			.05	Fail to Close	1	1	1		.05	Repress time only.
								6		
8.7.2	Press S/O Valve	1.0	.90	Leakage	.1	1	68.9		6.2	
			.05	Fail to Open	1	1	3.5		.2	T for engine burn.
			.05	Fail to Close	1	1	3.5		.2	T for engine burn.
								7		
8.8	Check Valve H_2 Eng. Bleed	.27	.90	Leakage	0				0	Redundant check valves.
			.05	Fail to Open	1	1	3.5		.05	T for engine burn.
			.05	Fail to Close	1	1	3.5		.05	T for engine burn.
								1		
8.9	LH_2 Press Module									
8.9.1	S/O Valve	1.0	.90	Leakage	0				0	No effect, parallel to orifice.
			.05	Fail to Open	1	1	3.5		.2	T for engine burn.
			.05	Fail to Close	1	1	3.5		.2	
								1		
								862		
							R = .999138			

TABLE 6.2.4-2

ACPS

OPTION: 1

MISSION TIME: 36

ITEM NO.	NAME	$\lambda x10^{-6}$	α	MODE	β	N	T	ΣQ	$Qx10^{6}$	REMARKS
1	Fill Disconnect GN_2	1.96			0				0	Redundant cap after service ground use only
2	Fill Disconnect N_2H_4	1.96			0				0	Redundant cap after service ground use only
3	S/O Valve, GN_2	1.0			0				0	Redundant cap after service ground use only
4	S/O Valve N_2H_4	1.0			0				0	Redundant cap after service ground use only
5	Burst Disk/Relief Valve				0				0	Internal Redundant
6	Bladder Tank (4 req'd)	.96	1.0	Leakage (INT)	1	3	68.9	198	198	
7	Isolation S/O Valve Module	1.0			0				0	For emergency only. Not used in normal flight
8	Isolation S/O Valve Thruster	1.0	.90	Leakage (INT)	0	16			0	Time in oss bay, redundant to (9) open during flight.
			.05	Fail to Open	1	16	1.0		.80	Loss of one valve not critical open once during mission.
			.05	Fail to Close	1	16	1.0		.80	Time: in oss bay - redundant to (9) closed once during mission.
								2		
9	Thruster S/O Valve	1.0	.90	Leakage (INT)	0				0	Redundant to (8)
			.05	Fail to Open	1	16	39.5		31.6	Time: Free flight. Loss of one value not critical
			.05	Fail to Close	0			32		Redundant to (8)

TABLE 6.2.4-2 (CONT)

ITEM NO.	NAME	$\lambda x10^{-6}$	α	MODE	β	N	T	ΣQ	$Qx10^{6}$	REMARKS
10	Thrust Chamber	.32	1	Cat. Decom-pose	1	16	39.5	202	202	Time: free flight loss of on thruster not critical.
11	Temp. Xducer GN_2	3.03							0	Redundant Units
12	Temp. Xducer N_2H_4	3.03							0	Redundant Units
13	Press. Xducer	8.00							0	Redundant Units
14	Temp. Xducer	3.03							0	Functionally redundant to 15
15	Press. Xducer	8.00							0	Functionally redundant to 14
								636		
						R = .999364				

TABLE 6.2.5-1

LATCH SYSTEM, TUG/PAYLOAD

OPTION: 1

MISSION TIME: 36

ITEM NO.	NAME	$\lambda x10^{-6}$	α	MODE	β	N	T	ΣQ	$Qx10^{6}$	REMARKS
1.1	Pneu. Module	2.0	.90	Leakage	.1	1	38.9		12.4	
			.05	Fail to Open	1	1	1.0		.1	
			.05	Fail to Close	1	1	1.0		.1	
								13		
1.3	Retract Cylinder	3.0	.9	Leakage	.1	4	1.0		.1	
			.1	Jam	1	4	1.0		1.2	
								1		
								14		
							R =	.999985		
	Support Structure						R =	.999999		

TABLE 6.2.5-2

TUG/OSS SEPARATION

OPTION: 1

MISSION TIME: 36

ITEM NO.	NAME	$\lambda x10^{-6}$	α	MODE	β	N	T	ΣQ	$Qx10^{6}$	REMARKS
1.0	Motor Assy	12.8	.3	Low Torque	1	1	2		77	
			.7	Low Speed	.1	1	2		1.8	
								79		
2.0	Gear Drive	2.4	.1	Jam	1	1	2		.48	
			.9	High Friction	.1	1	2		.43	
								1		
3.0	Linkage	1.0	.1	Jam	1	16	2		3.2	
			.9	High Friction	.1	16	2		29	
								32		
4.0	Springs	.01	.1	Break	1	16	2		.03	
								1		
								113		
							R =	.999887		

Section 5
SAFETY IMPACT

As a result of system safety analyses of Tug systems, the design, production, and operations have been impacted by the following.

5.1 DESIGN

A. Burst discs and relief valves in the ACPS, pneumatic supply system, ambient helium system, and the tank purge system. These systems will vent to the tug overboard vent system.

B. Incorporation of relief valves on the insulation purge bags.

C. Incorporation of separate shutoff valves for the GHe supply to the purge bags to preclude cross flow of leaked propellants through the system.

D. Identified single point failure of thruster chamber valve either by leakage or inadvertent operation. Valve design selection changed to provide two series valves, one normally closed and the other capable of latching in either the open or closed position.

E. Identified system inhibit and override functions.

F. Incorporate a container for each battery to retain leaked or spilled electrolyte.

5.2 PRODUCTION

A. Established leak rate levels of GHe for H_2 system tests.

B. Provided cursory analyses of refurbishment concepts to ensure identification of hazardous functions and to reduce exposure to the hazards; i.e., safing of pressurized systems prior to disassembly, monitoring for toxic vapors, and testing pressurized systems at levels acceptable for personal exposure.

C. Cursory analyses of the proposed materials and the fabrication methods show no hazards with which MDAC is not already familiar.

5.3 OPERATIONS

A. Provided curscry analyses of operational concepts to ensure identification of hazardous operations and sequencing those operations to reduce exposure to these hazardous operations; i.e., pressurization of GHe pressure vessels with a 2:1 design ratio to a level not to exceed 4:1 when operational personnel are exposed; restraints in storable propellant loading and detanking, etc.

B. Identified items for crew warning and caution monitoring, hazard potentials at the tilt-table interface, and at the Tug and Orbiter hard points.

C. Determined the quantity of GH_2 to be dumped below 110K feet on reentry.

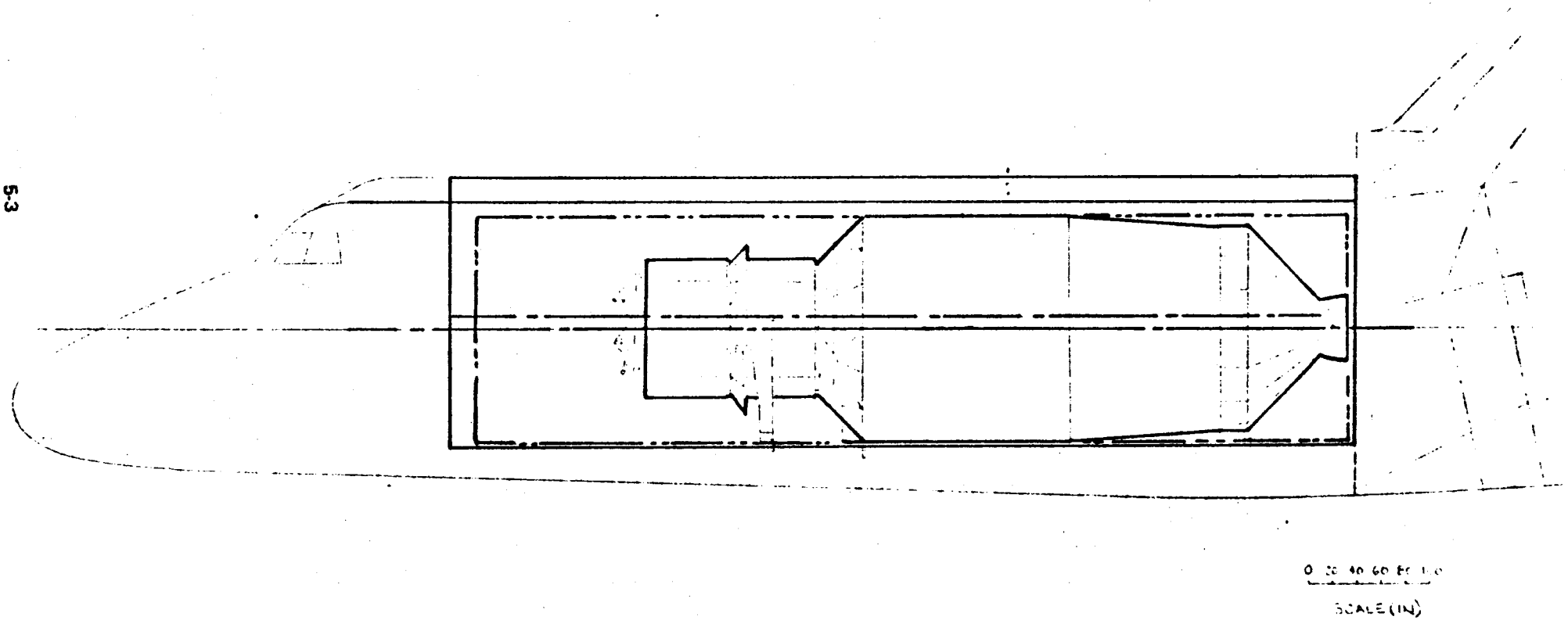
D. Determined toxicity levels for hydrazine and established requirements for monitoring after the monopropellant system is filled.

E. Assisted in analyzing hazards related to abort and post-landing recovery.

F. Performed calculations to determine impact of fluids on the orbiter bay. These calculations are shown in the following tables.

DSCS AND TUG IN ORBITER BAY

TOTAL BAY	$V = 61.5 \text{ ft} \times .7854\ (15.8)^2 =$	$12{,}054 \text{ ft}^3$
OOS	$V = 26.5 \text{ ft} \times .7854\ (15)^2 =$	$-4{,}690 \text{ ft}^3$
DSCS	$V = 11.6 \text{ ft} \times .7854\ (9.2)^2 =$	-766 ft^3
	FREE VOLUME	$6{,}598 \text{ ft}^3$



BAY OVERPRESSURE

Assume 5 lb helium or 39 lb nitrogen

Gas Const R for He = 386.3

GN_2 = 55.16

PV = WRT

P = pressure rise $lb/ft^2/144$ = psi

V = Free bay volume ft^3 = 6598 ft^3

W = Weight in lb

R = Gas constant

T = Temperature °R 530°R (70°F)

1. He Pressure Rise (no venting) (1 bottle)

$$P = \frac{WRT}{V(144)} = \frac{5\ (386.3)(530)}{6598\ (144)} = 1.3 \text{ psi rise}$$

2. GN_2 Pressure Rise (no venting) (4 Bottles)

$$P = \frac{WRT}{V(144)} = \frac{(39)(55.16)(530)}{6598\ (144)} = 1.2 \text{ psi rise}$$

The Safety in Earth Orbit Study, Vol. II, MSC-04477, SD 72-SA-0094-2, page A-36, para. A.10, "Maximum Tolerable Leak Rate Into Shuttle Cargo Bay", NAR states, "The maximum tolerable steady state leakage rate into the cargo bay, with doors closed, is of the order of 2.5 Kg/sec (5.5 lb/sec) for hydrogen and 20 Kg/sec (45 lb/sec) for air, oxygen, or nitrogen".

The results noted in these calculations are well below the values stated in the NAR document.

HYDROGEN LIMITS IN ORBITER BAY

Approximate bay volume = 61.5 ft x .7854 $(15.8)^2$ = 12,054 ft^3
Less Tug volume = 26.5 ft x .7854 $(15)^2$ = -4,690 ft^3

7,364 ft^3

Less DSCS II as typ payload=11.6 ftx.7854$(9.2)^2$ = -766 ft^3

Free Volume = 6,598 ft^3

Hydrogen flammability limit is 4% at S.L. (by volume)

$\therefore$ 6,598 ft^3 x .04 = 263.92 ft^3 of H_2

Hydrogen weighs .0052 lb/ft^3 @ 68°F, S.L.

$\therefore$ .0052
263

1.3676 lb .. leakage of 1.4 lb of GH_2 creates a flammable atmosphere in the Orbiter bay.

The lower explosive limit of H_2 is 18% at S.L. (by volume)

$\therefore$ 6,598 ft^3 x .18 = 1187 ft^3 of H_2

Hydrogen weighs .0052 lb/ft^3 @ 68°F, S.L.

$\therefore$ 1187 ft^3 x .0052 lb/ft^3 = 6.175 lb

$\therefore$ Leakage of 6.2 lb of GH_2 creates an explosive atmosphere in the Orbiter bay

OXYGEN LIMITS IN ORBITER BAY

Assume:

1. It is desired to keep the O_2 level in the orbiter bay at 5% by volume, or less.
2. Orbiter bay free volume is 6598 ft^3.

Use oxygen gas weight of 0.083 lb/ft^3 @ 68°F.

$$\begin{array}{r} 6598 \\ .05 \\ \hline 329.9\ ft^3 \end{array}$$

0.083 lb/ft^3 x 329.9 ft^3 = 27.38 lb to give a 5% by volume O_2 atmosphere in the orbiter bay.

H_2 LEAKAGE

HYDROGEN TANK	1×10^{-6} SCCS/ft GHe[1]
	169 in. dia
	97 in. straight section (assume 3 segments)
TWO CIRCUMFERENCE WELDS:	$2 \times \pi \times D = (2\pi[169])/12 = 88.5$ ft = 90 ft
THREE LINEAR WELDS:	$(3 \times 97)/12 = 24.25$ ft = 25 ft
MISC. WELDS AND ACCESS:	10 ft/125 ft welds

.. 125×10^{-6} SCCS or 1.25×10^{-4} SCCS leakage through welds allowed.

Components	1×10^{-4} SCCS GHe[1]	
Prevalve	1	
Fill and Drain Valve	1	
Pressurization Valve	1	11×10^{4} SCCS
Vent and Relief	2	
Isolation	4	
Interface (Vent)	1	
Dump Valve	1	
	11	

Couplings	1×10^{-5} SCCS GHe[1]
Prevalve	1
Fill and Drain	1
Pressurization	4
Vent and Relief	7
Isolation	10
Interface	1
Prop. Util.	2
Dump Valve	1
	29

TOTAL LEAKAGE:	1.25×10^{-4} SCCS Welds
	11.00×10^{-4} SCCS Components
	2.70×10^{-4} SCCS Couplings
	14.95×10^{-4} SCCS
	1.495×10^{-3} SCCS

TIME: (From NAS9-14000 - Rockwell - SSV73-41 page 84)

Prelaunch through P/L deployment

Disconnect ground purge to open doors 34 min.

34 min x 60 sec/min = 2040 sec

Entry through post landing

From reentry to connect ground purge (TD + 30)

42 + 32 = 72 min.

72 min x 60 sec/min = 4320 sec

.. $1.495 \times 10^{-3} \times 4.320 \times 10^{3} = 6.46$ SCC

CONVERSION: 3.531×10^{-5} ft^3/CC

$3.531 \times 10^{-5} \times 6.46 = 2.28 \times 10^{-4}$ ft^3

VAPOR DENSITY: .083 lb/ft^3 @ 40°R

.083 $lb/ft^3 \times 2.3 \times 10^{-4}$ $ft^3 = 1.91 \times 10^{-5}$ lb

1.91×10^{-5} lb leakage allowable

If we allow 1×10^{-2} SCCS leakage:

125×10^{-2}

11×10^{-2}

27×10^{-2}

163×10^{-2} SCCS

1.63 SCCS

1.63 SCCS x 4320 sec = 7042 SCC

$3.531 \times 10^{-2} \times 7.042 = 24.9 \times 10^{-2}$

.249 ft^3

VAPOR DENSITY: .083 lb/ft^3 @ 40°R

.083 $lb/ft^3 \times .249$ $ft^3 = 2.07 \times 10^{-2}$ lb

.02 lb leakage

(1) AFSC DH3-2 Space Vehicles, DN14E2.

HYDROGEN DEPLETION AND REENTRY PRESSURE CONDITIONS
FOR THE HYDROGEN TANK

OBJECT: Maintain the internal pressure of the hydrogen tank at 16±1 psia during reentry, landing, and soak.

Thermal conditions of the LH_2 tank wall from SOAR II/Tug Thermal Study Final Report, A3-250-AAAA-M-15, dated 20 February 1973 were as follows:

	Temperature (°R)
Start reentry	160°R (warmed by GHe)
Landing	305°F
30 minute soak	300°R (first allowed approach)
2.8 hour soak	410°R (GSE Hookup)

SOLUTION METHOD: Use PV = WRT where:

P is pressure in $lb/ft^2 \times 144\ in.^2/ft^2$ = psia

V is volume in ft^3 = 2078 ft^3 LH_2 tank

W is weight of gas in lb

R is gas constant = 766.8 for H_2
386.3 for He

T is temperature in °R

SOLUTION: It is intended that the LH_2 tank pressure be maintained at 16±1 psia during reentry, landing, and soak by venting to atmosphere as required.

In order to preclude liquefaction of air on the exterior of the LH_2 tank, most of the residual LH_2 will be dumped to vacuum. It is intended to bleed the H_2 tank to 3 psia. This value is well above the triple point pressure of 1 psia and should preclude the formation of H_2 ice in the tank, and the tank will be warmed to 160°R by the addition of approximately 48 lb of GHe.

The quantity of H_2 vapors which remain in the tank after dumping the 3 psia is determined as follows:

1. H_2 retained

$$PV = WRT$$

where

$$P = 3 \text{ lb/in.}^2 \times 144 \text{ lb/ft}^2 =$$

$$V = 2078 \text{ ft}^3$$

$$W = ?$$

$$R = 766.8$$

$$T = 29^\circ R$$

then

$$W = \frac{PV}{RT} = \frac{(3)(144)(2078)}{(766.8)(29)} = 40.4 \text{ lb } H_2$$

use: 40 lb H_2

The addition of the GHe to warm the tank then creates the following environment within the tank.

$$P_{He} = \frac{W_{He}R_{He}T}{Vx144} = \frac{(48)(386.3)(160)}{2078x144} = 9.9 \text{ psi}$$

$$P_{H_2} = \frac{W_{H_2}R_{H_2}T}{Vx144} = \frac{(40)(766.8)(160)}{2078x144} = 16.4 \text{ psi}$$

$$P_T = P_{He} + P_{H_2} = 9.9 + 16.4 = 26.3 \text{ psi}$$

The total gas weight is then H_2 + GHe = 40 +48 = 88 lb gas of which the percent split is

$$\frac{40}{88} = 45.5 \text{ percent } H_2$$

$$\frac{48}{88} = 54.5 \text{ percent GHe}$$

It is necessary to vent this pressure to 15 psia to achieve the desired internal pressure prior to reentry.

$\therefore$ partial pressure of He = 15 x .595 = 8.2 and

partial pressure of H_2 = 15 x .455 = 6.8

Then

$$W_{He} = \frac{P x 144 x V}{RT} = \frac{8.2(144)(2078)}{386.3 x 160} = 39.7 \text{ lb}$$

$$W_{H_2} = \frac{P x 144 x V}{RT} = \frac{6.8(144)(2078)}{766.8 x 160} = 16.6 \text{ lb}$$

TOTAL = 56.3 lb

The amount of gas dumped prior to reentry then becomes

88 lb - 56.3 lb = 31.7 lb with the H_2 gas equal to 23.4 lb.

2. Upon reentry and landing, the temperature of the tank wall increases to 305°F. In order to maintain 15 psia, it will be necessary to vent to the atmosphere.

$$W_{He} = \frac{(8.2)(144)(2078)}{(386.3)(305)} = 20.8 \text{ lb}$$

$$W_{H_2} = \frac{(6.8)(144)(2078)}{(766.8)(305)} = 8.7 \text{ lb}$$

29.5 lb

Therefore, it will be necessary to vent the following during descent.

56.3 lb - 29.5 lb = 26.8 lb with the H_2 gas equal to 7.9 lb.

At the end of the first 30 minute soak period, the temperature remains fairly stable and no additional venting is anticipated. However, the 2.8 hour soak prior to GSE hookup requires that we retain the following:

$$W_{He} = \frac{(8.2)(144)(2078)}{(386.3)(410)} = 15.5 \text{ lb}$$

$$W_{H_2} = \frac{(6.8)(144)(2078)}{(766.8)(410)} = \frac{6.5 \text{ lb}}{22.0 \text{ lb}}$$

Therefore, it will be necessary to vent as follows:

29.5 lb - 22.0 lb = 7.5 lb with the H_2 gas equal to 2.2 lb.

The total H_2 to be dumped into the atmosphere after reentry is 10.1 lb or at .0052 lb/ft^3 is equal to

$\frac{15.6}{.0052}$ = 3000 ft^3 H_2 exhausted at ambient temperature and pressure.

HYDRAZINE

Anhydrous hydrazine is a powerful reducing agent, particularly with acids, oxidizers, and organic substances. After long exposure to air or short subjection to elevated temperatures, it may decompose with explosive violence. Hydrazine mixes with water and the lower alcohols in all proportions, but it is only slightly soluble in other organic solvents.

Prolonged storage of hydrazine at room temperatures in sealed containers results in only a small release of amonia. However, at high temperatures, hydrazine decomposes at a different rate, dependent on the temperature, e.g., it first exhibits decomposition at 320°F and decomposes at the rate of 1.5 to 2 percent per hour at 392°F and 600 psi. Hydrazine explodes at 491°F after a rapid rise of decomposition rate.

The flash point of hydrazine is given as 100°F, and the fire point as 140°F. The average explosion temperature is approximately 450°F. Hydrazine is not sensitive to impact or friction. As an unconfined liquid, it is not very sensitive to a static spark; it withstands sparks of 12.5 joules at room temperature. Hydrazine vapor, when sparked at 212°F, explodes with a yellow flame. In contact with organic materials, such as wool and rags, hydrazine may burn spontaneously. Metallic oxides, such as iron, copper, lead, manganese, and molybdenum will start spontaneous combustion.

The lower limit of inflammability is 4.7 percent by volume of hydrazine vapor in air; the upper limit is 100 percent. In nitrogen and helium atmosphere, the lower limits are 38 percent and 37 percent, respectively.

Anhydrous hydrazine attacks natural rubber, cork, mild steel, and most other common metals, but polyvinyl chloride, polyisobutylene, and asbestos are resistant at ambient and high temperatures. Inconel appears to be the most resistant metal.

The environment anticipated in the orbiter bay during reentry shows an entry and post landing payload bay wall temperature of 200°F maximum. The minimum estimated free volume in the bay is 6598 ft^3.

Calculations for determining the amounts of hydrazine required to create an explosive atmosphere and one that is toxically hazardous are shown below.

1. Determine the pounds of hydrazine to reach the lower flammability (or explosive) limits in air at 212°F of 4.7 percent by volume.

Assumptions: Free volume of the bay is 6598 ft^3.

Entry and Post Landing Temp. = 200°F.

Dry air at 200°F = .0545 lb/ft^3.

Pressure = 14.7 psi.

Gas Density Relative to Air = 1.1

Then:

$$\begin{array}{r} 6598\ ft^3 \\ .047 \\ \hline 46186 \\ 26392 \\ \hline 310.106\ ft^3 \end{array}$$

$310\ ft^3 \times .0545\ lb/ft^3 \times 1.1 =$

310 x .05995 lb = 18.58 lb hydrazine required to create explosive atmosphere.

This is equivalent to 0.29 ft^3 of hydrazine liquid.

For a nitrogen inerted atmosphere, the value is 210 lb or 3.3 ft^3 of hydrazine liquid.

2. Determine the amount of hydrazine spilled/leaked in the orbiter bay to give the atmosphere a Threshold Limit Value (TLV) of 1.3 Mg/M^3. (TLV = allowable exposure for 8 hr/day, 5 days/week.)

Assumptions: Free volume of bay is 6598 ft^3 or 186.9 M^3

Pressure - 14.7 psi.

$\therefore$ 186.9 M^3 x 1.3 Mg/M^3 = 242.97 Mg

242.97 Mg of hydrazine in the bay causes the toxicity level to be at the TLV.

Then:

$$\frac{242.97 \text{ Mg}}{1000 \text{ Mg/G}} = .24297 \text{ grams}$$

and

$$.24297 \text{ gms} \times .03527 \text{ oz/gm} = 8.57 \times 10^{-3} \text{ oz}$$

In the event of leakage in the closed bay, the hydrazine vapors could also enter the payload motor nozzles in a reverse direction. This would expose the hydrazine vapors to the catalyst and could cause decomposition of the hydrazine with resulting high temperatures.

Ref: Rocket Propellant Handbook, Boris Kit and Douglas S. Everd, 1960

VOLUME OF GAS IN PURGE BAGS

Volume of gas in LO_2 tank purge bag

LO_2 tank surface area = 390 ft^2

For radiation type use 3 in. free volume height

Radiation: 390 x 3/12 = 97.5 ft^3

97.5 = .083 = 8.09 lb GO_2

97.5 x .0103 = 1.0 lb GHe

Volume of gas in LH_2 tank purge bag

LH_2 tank surface area = 764 ft^2

For radiation type use 3 in. free volume height.

Radiation: 764 x 3/12 = 191 ft^3

191 x .0052 = .99 lb GH_2

191 x .0103 = 1.96 lb GHe

Previous calculations for hydrogen limits in the orbiter bay show that 1.4 lb of GH_2 creates a flammable atmosphere in the orbiter bay. It appears that the maximum that could be dumped by a purge bag rupture is .99 lb which is well below the quantity required to create a flammable atmosphere in the orbiter bay.

PRESSURE RISE FOR MONO BLOWDOWN GN_2 HEAD PRESSURE

1. Determine the pressure rise of the GN_2 in the monopropellant blowdown N_2H_4 tanks on a "no usage" basis.

Assumptions:

Maximum operating pressure: 360 psi

Temperature at fill: 530°R (70°F)

Temperature at full heat soak: 660°R (200°F)

Burst disc rupture at: 400 psi

Relief valve cracks at: 400 psi

GN_2 vents to the H_2 vent

Use:

$$\frac{P_1 V_1^K}{T_1} = \frac{P_2 V_2^K}{T_2}$$

Where:

P_1 is start pressure, psi = 360°R

V_1^K is start volume = V_2^K is end volume

T_1 is 530°R

T_2 is 660°R

P_2 is maximum pressure reached without relief.

$$\therefore P_2 = \frac{P_1 T_2}{T_1}$$

$$P_2 = \frac{(360)\ (660)}{530} = 448 \text{ psi}$$

This pressure would cause disc rupture and GN_2 venting to the relief valve pressure settings.

PRESSURE RISE FOR THE PNEUMATIC GHe SYSTEM

1. Determine the pressure rise of the GHe in the pneumatic system tank on a "no usage" basis.

Assumptions:

Maximum operating pressure: 3100 psi

Temperature at fill: 530°R (70°F)

Temperature at full heat soak: 660°R (200°F)

Burst disc rupture at: 3410 psi

Relief valve cracks at: 3410 psi

GN_2 vents to the H_2 vent

Use:

$$\frac{P_1 V_1^K}{T_1} = \frac{P_2 V_2^K}{T_2}$$

Where:

P_1 is start pressure, psi = 3100 psi

V_1^K is start volume = V_2^K is end volume

T_1 is 530°R

T_2 is 660°R

P_2 is maximum pressure reached without relief.

$$\therefore P_2 = \frac{P_1 T_2}{T_1}$$

$$P_2 = \frac{(3100)(660)}{530} = 3860 \text{ psi}$$

This pressure would cause disc rupture and GHe venting to the relief valve pressure settings.

PRESSURE RISE FOR AMBIENT HELIUM PRESSURIZATION SYSTEM

1. Determine the pressure rise of the GHe in the ambient helium pressurization tanks on a "no usage" basis.

Assumptions:

Maximum operating pressure: 3100 psi

Temperature at fill: 530°R (70°F)

Temperature at full heat soak: 660°R (200°F)

Burst disc rupture at: 3410 psi

Relief valve cracks at: 3410 psi

GHe vents to the H_2 vent

Use:

$$\frac{P_1 V_1^K}{T_1} = \frac{P_2 V_2^K}{T_2}$$

Where:

P_1 is start pressure, psi = 3100 psi

V_1^K is start volume = V_2^K is end volume

T_1 is 530°R

T_2 is 660°R

P_2 is maximum pressure reached without relief.

$$\therefore P_2 = \frac{P_1 T_2}{T_1}$$

$$P_2 = \frac{(3100)(660)}{530} = 3860 \text{ psi}$$

This pressure would cause disc rupture and GHe venting to the relief valve pressure settings.

PRESSURE RISE FOR THE TANK PURGE GHe SYSTEM

1. Determine the pressure rise of the GHe in the tank purge tanks on a "no usage" basis.

Assumptions:

Maximum operating pressure: 3100 psi

Temperature at fill: 530°R (70°F)

Temperature at full heat soak: 660°R (200°F)

Burst disc rupture at: 3410 psi

Relief valve cracks at: 3410 psi

GN_2 vents to the H_2 vent

Use:

$$\frac{P_1 V_1^K}{T_1} = \frac{P_2 V_2^K}{T_2}$$

Where:

P_1 is start pressure, psi = 3100 psi

V_1^K is start volume = V_2^K is end volume

T_1 is 530°R

T_2 is 660°R

P_2 is maximum pressure reached without relief.

$$\therefore P_2 = \frac{P_1 T_2}{T_1}$$

$$P_2 = \frac{(3100)(660)}{530} = 3860 \text{ psi}$$

This pressure would cause disc rupture and GHe venting to the relief valve pressure settings.

Battery Hazards

One of the identified hazards for Tug batteries is cell overpressurization which could lead to explosive failure of the hermetic seal on an individual cell. Two possible failure causes have been identified. The first is hydrogen pressure buildup due to cell rapid charge or overcharge. The second is a possible battery heater failure in the on mode.

Battery cell overcharge is possible since individual cell voltage differences can occur and result in cell over voltage charging. Selecting individual battery cells made of stainless steel with a burst pressure capability of 1000 psi, and coupled with expected cell pressure levels of 0-100 psi makes the accident possibility remote. However, ground laboratory testing of battery sets have caused cell wall bulging due to improper charge/discharge operation. Therefore, it is recommended that the battery be enclosed in an hermetically sealed case. As an example, for a 22 cell battery with battery cell free volume at 2.44 cu. in. per cell, the sealed case volume required to reduce the total volume battery pressure to 500 psi is as follows:

$500 \text{ spi} = 72000 \text{ lb/ft}^2$

Assume $T_1 = 60°F$

$PV = WRT$

where:

P = pressure $\text{lb/ft}^2 = 144{,}000 \text{ lb/ft}^2$ (start)

V = volume $\text{ft}^3 = 2.44 \text{ cu. in./cell} \times 22 - 53.68/1728 = .031 \text{ ft}^3$

W = weight of gas lb =

R = gas constant = 766.8

T = temperature $°R = 460° + 60°F = 520°F$

$$W = \frac{PV}{RT} = \frac{144000 \times 031}{766.8 \times 520} = 1.12 \times 10^{-2} \text{ lb } H_2$$

Then:

$$V = \frac{WRT}{P} = \frac{1.12 \times 766.8 \times 520}{72000} = .062 \text{ ft}^3$$

Therefore, the container should provide an additional volume of .062 ft^3.

*Alternate protection measures include battery redesign to incorporate recombination electrodes, cell pressure relief, cell voltage monitors, and cell pressure monitors. Review of these possibilities indicates further development effort is required for all but the pressure relief valve option.

Section 6

RESIDUAL HAZARDS AND RATIONALE FOR ACCEPTANCE

The residual hazards identified to date are corrosion, fire explosion, pressure, and toxicity.

Corrosion

Two fluids to be carried aboard the Tug are considered corrosive. They are hydrazine, used in the ACPS, and potassium hydroxide, used as the electrolyte in the barriers.

Rationale for Acceptance

Hydrazine -- The ACPS system design precludes leakage which can cause corrosion by providing a pressure and leakage tested system, series redundant shut off valves, and a vent burst disc and relief valve which vents to the hydrogen vent line. In addition, monitoring for hydrazine vapors will be accomplished after propellant loading and through all phases of the operations deemed to be hazardous by the presence of hydrazine.

Potassium Hydroxide -- Battery system leakage which can cause corrosion will be precluded by selecting battery cells which will contain the electrolyte in all modes and by providing a container around the battery to retain spilled electrolyte.

Explosions

Explosions may occur from three sources aboard the Tug; hydrogen, hydrazine, and pressurants.

Rationale for Acceptance

The conditions under which explosions could result from these materials are shown in calculations in Section 5 of this document.

Fire

Materials aboard the Tug which can be considered as fuel are hydrogen, hydrazine, thermal insulation and purge bag, wiring insulation, and bonding resins.

Hydrogen

Hydrogen is the prime propellant on the cryogenic Tug. In addition, hydrogen gas can be created by dissociation of the battery electrolyte during battery charge.

Rationale for Acceptance

The design of the hydrogen system will be such that leakage of H_2 into the orbiter bay will be limited to a value well below the LEL for the volume in question. In addition, the orbiter bay will be inerted with GN_2.

The quantity of H_2 generated by the battery when compared to the quantity of prime propellant is not a significant amount, however, the hazard must be addressed.

The contained around the battery to retain spilled electrolyte will also provide containment for generated H_2.

Thermal Insulation

The thermal insulation consists of Dacron netting, aluminized Mylar sheeting, and a Kapton coated with Teflon and aluminum purge bag.

Material	Flammability Characteristics
Mylar-aluminized	slow to self-extinguishing
Dacron	slow to self-extinguishing
Kapton	self extinguishing
Teflon	nonflammable

Rationale for Acceptance

Three things are necessary for a fire to occur; i.e., fuel, oxygen, and ignition. As general design criteria, sources of ignition will be eliminated by correct design of electrical equipment. The atmosphere will be GN_2 during the launch phase and oxygen will be limited to leakage from the LO_2 system and that O_2 in air during reentry.

The flammability characteristics noted show that Kapton and Teflon should not be considered as fuels. The Mylar and Dacron must be considered, and further study is required on these materials prior to final acceptance. It would, however, require a double failure to create a fire situation.

Wiring Insulation

Wiring insulation must be considered as a potential fuel in the fire triangle.

Rationale for Acceptance

Prudent selection of wiring insulation from approved materials will preclude this hazard.

Bonding Resins

Bonding resins must be considered as a potential fuel in the fire triangle.

Rationale for Acceptance

Prudent selection of resins from approved materials will preclude this hazard. In addition, the quantity used is limited.

Hydrazine

Anhydrous hydrazine is a powerful reducing agent, particularly with acids, oxidizers, and organic substances. After long exposure to air or short subjection to elevated temperatures, it may decompose with explosive violence. Hydrazine mixes with water and the lower alcohols in all proportions, but it is only slightly.

Prolonged storage of hydrazine at room temperatures in sealed containers results in only a small release of ammonia. However, at high temperatures, hydrazine decomposes at a different rate, dependent on the temperature, e.g., it first exhibits decomposition at 320°F and decomposes at the rate of 1.5 to 2 percent per hour at 392°F and 600 psi. Hydrazine explodes at 491°F after a rapid rise of decomposition rate.

The flash point of hydrazine is given as 100°F, and the fire point as 140°F. The average explosion temperature is approximately 450°F. Hydrazine is not sensitive to impact or friction. As an unconfined liquid, it is not very sensitive to a static spark; it withstands sparks of 12.5 joules at room temperature. Hydrazine vapor, when sparked at 212°F, explodes with a yellow flame. In contact with organic materials, such as wool and rags, hydrazine may burn spontaneously. Metallic oxides, such as iron, copper, lead, manganese, and molybdenum will start spontaneous combustion.

The lower limit of inflammability is 4.7 percent by volume of hydrazine vapor in air; the upper limit is 100 percent. In nitrogen and helium atmosphere, the lower limits are 38 percent and 37 percent, respectively.

Rationale for Acceptance

The ACPS system design precludes leakage which can cause fire by providing a pressure and leakage tested system, series redundant shut off valves and a vent burst disc and relief valve which vents to the hydrogen vent line. In addition, monitoring for hydrazine vapors will be accomplished after propellant loading and through all phases of the operations deemed to be hazardous by the presence of hydrazine.

Calculations which demonstrate the quantity of hydrazine required to create a hazardous atmosphere show that it would require 18 lb to be distributed into the bay air environment and 210 lb into a GN_2 environment.

Pressure

The residual hazards related to pressure are:

System	Medium and Pressure Level		
Hydrogen propellant	H_2		16 psia
Oxidizer	O_2		16 psia
Pressurization and Pneumatics	GHe	@	3000
Tank Purge	GHe	@	3000
ACPS	GN_2	@	360

Rationale for Acceptance

All systems are protected by relief devices set to relieve at approximately 10 percent above maximum operating pressure. In addition, calculations have shown that an instant release of the stored volumes will not overpressurize the orbiter bay.

Toxicity

The substances utilized by the Tug which can be considered to create a toxic atmosphere are:

Material	Toxicity
GN_2	Simple asphyxiant
GH_2	Simple asphyxiant
GHe	Simple asphyxiant
GO_2	None
KOH	(No levels given: may cause death or injury after very short exposure to small quantities)
Hydrazine	TLV 1.3 mg/M^3

Rationale for Acceptance

When it is possible to have a toxic atmosphere where personnel are involved, monitoring for safe levels will be provided.

The presence of the simple asphyxiants must be monitored since their presence in hazardous concentrations is not readily detectable by odor or reaction.

The battery electrolyte, KOH, will be retained within the container which encloses the battery.

The potential toxic hazard created by hydrazine leakage is considered to be the most critical of the substances utilized. It is intended to perform the hydrazine loading in the Storable Propellants loading area. Prior to loading a complete pressure/leak test will be made on the system.

Subsequent to loading, it will be necessary to monitor the system for leakage through use of leak detectors which sample the surrounding volume for hydrazine vapors.

Procedural steps will be included in all operating procedures to assure continual monitoring during all subsequent operations. Specific personnel protective measures will be taken during all situations where the Tug is considered to be in a dynamic condition, i.e., transporting, handling, test, lifting, mating to the payload, and mating to the orbiter.

After installation into the orbiter bay, the volume will be continuously monitored for hydrazine vapors.

The ACPS system design precludes leakage which can cause a toxic atmosphere by providing a pressure and leakage tested system, series redundant shut off valves and a vent burst disc and relief valve which vents to the hydrogen vent line. Calculations which demonstrate the quantity of hydrazine required to create a toxic atmosphere in the orbiter bay show that it would require 0.24 grams to be distributed into the bay air environment to give a TLV of 1.3 Mg/M^3.

Section 7
SAFETY CRITERIA AND REQUIREMENTS

In addition to the safety criteria and requirements provided in the Data Package for the Tug Program (shown as Appendix 3 of this document), MDAC has developed additional requirements. These are displayed as the Possible Controls on the OHA's in Section 4 of this document.

In order to accept the identified residual hazards and assure minimization of the possibility of creating a hazardous condition, the following identified safety criteria and requirements must be applied.

Corrosion

Hydrazine:

A. Perform operations in controlled area. Ensure compatibility of materials and fluids. Do not use trichlor products to clean titanium parts. Ensure leak test solutions are correctly removed. Use galvanic chart when selecting materials. Ensure protective coatings do not react with system fluids. Ensure cleaning fluids will not be trapped in valves and lines.

B. Provide pressure relief in fill system. Monitor tank pressure. Provide pressure relief of tank at 10% above maximum operating. Relieve to closed vent system.

C. Ensure system integrity prior to propellant loading. Leakage not to exceed

   TBD SCCS valves

   TBD SCCS tank

   TBD SCCS fittings

   Design system to minimize points of potential leakage. Ensure system integrity after loading.

D. Ensure procedural operations do not allow leakage.

E. Monitor orbiter bay atmosphere. Leakage not to exceed

TBD SCCS valves

TBD SCCS tank

TBD SCCS fittings

Report valve positions prior to retrieval and monitor when in orbiter bay.

F. Provide series valves whose operational position prevents leakage. Leak check the system prior to making the system wet. Ensure valve positions. Upon completion of operations, sample all flanges, etc., for leakage.

G. Ensure no inadvertent operational signals are sent to system. Ensure no inadvertent signals/operations will activate system.

H. Ensure launch loads do not allow leakage through valves. Ensure latching methods will withstand launch loads.

Potassium Hydroxide

Select battery cells to contain electrolyte in all modes. Provide container to retain spilled electrolyte and be corrosion resistant.

Explosions

Hydrogen

A. Ensure provisions are made to deactivate systems which can provide an ignition source on crash impact.

B. Provide pressure relief design to preclude trapped cryogenics.

C. Provide insulation to preclude heat rise effect.

D. Ensure vent to TBD psi does not allow retention of cryogenics as solids.

E. Provide relief valve override.

F. Leak check system prior to filling.

G. Inert Orbiter bay prior to filling.

H. Double seal or weld all connections. Leakage not to exceed

TBD SCCS plumbing

TBD SCCS tank

TBD SCCS fittings

I. Design to preclude low thermal effects.

J. Design to eliminate all sources of ignition.

K. Ensure all confined areas are purged.

L. Leak check system after chilldown.

M. Design system to minimize points of potential leakage.

N. Locate electrical wiring or other potential ignition sources so that no contact can be made with the leaking fluid.

O. Start reentry with TBD pounds GHe in tank.

P. Provide sufficient GHe to establish GH_2 volume at TBD percent.

Q. Provide purge to maintain inert atmosphere and clear gaseous H_2 from center shell section.

R. Provide porting and purging system to ensure complete purge.

S. Provide detectors to signal H_2 presence.

T. After retrieval to orbiter bay, dump LH_2 remaining to space and vent tank to TBD psi. Close dump and vent system and allow tank to warm. Vent to TBD psia max. Close vent and fill with GHe. Blowdown and refill with GHe to TBD psia.

Hydrazine

A. Use a 4:1 safety factor for plumbing

B. Maintain ambient temperature below 110°F.

C. Ensure provisions are made to deactivate systems which can provide an ignition source on crash impact.

D. Vent to H_2 vent line.

E. Provide pressure relief at 10% above maximum pressure.

F. Leakage not to exceed

TBD SCCS valves

TBD SCCS tank

TBD SCCS fittings

G. Purge orbiter bay with GN_2 prior to launch.

H. Monitor orbiter bay atmosphere.

I. Monitor valve positions and report to crew.

J. Provide series valves whose operational position prevents leakage.

Fire

Hydrogen

A. Leak check system prior to filling.

B. Inert Orbiter bay prior to filling.

C. Double seal or weld all connections.

D. Leakage not to exceed

TBD SCCS plumbing

TBD SCCS tank

TBD SCCS fittings

E. Design to eliminate all sources of ignition.

F. Consider friction sparks, impact sparks, electrical sparks, and hot objects.

G. Purge bay and assure all confined areas are also purged.

H. Leak check system after chilldown.

I. Design system to minimize points of potential leakage.

J Provide pressure relief and bleed to allow for cryogenic expansion.

K. Locate electrical wiring or other potential ignition sources so that no contact can be made with the leaking fluid.

L. Provide gas detectors to signal hazardous conditions.

M. Insure electronic equipment is vapor tight to preclude entry of LH_2 or vapors.

N. Purge center shell section.

O. Vent H_2 to TBD psi and purge with GHe, vent to TBD psi and pressurize to TBD psi with GHe prior to reentry.

P. Provide GH_2 disposition by a burner system on the ground.

Q. Provide mechanical interrupt for main propulsion ignition system when installed in orbiter.

R. Design ignition system to require position crew action for activation.

Thermal Insulation

A. Provide thermal protection pads at ACPS rocket plumes.

B. Ensure insulation is a nonabsorbent material and cannot react chemically with the LH_2.

C. Ensure bag material will not rupture when exposed to cryogenic liquids.

D. Provide purge to create inert atmosphere and maintain thermal requirements.

E. Select materials which will not support combustion.

Hydrazine

A. Provide soft protective caps over thruster nozzles to preclude back flow. Caps to blowoff when thrusters operated.

B. Provide electrical interlocks to prevent inadvertent activation.

C. Provide series isolation and thruster shutoff valves.

D. Ensure system integrity prior to propellant loading.

E. Leakage not to exceed

TBD SCCS valves

TBD SCCS tank

TBD SCCS fittings

F. Design to eliminate sources of ignition.

G. Design system to minimize points of potential leakage.

H. Ensure correct fire protection equipment is available.

I. Ensure fuel containment and drainage are adequate.

J. Ensure system integrity after loading.

K. Ensure procedural operations do not create hazardous conditions.

L. Ensure correct valve positioning prior to creating a "wet" system.

M. Purge Orbiter bay with GN_2 prior to launch.

N. Monitor orbiter bay atmosphere.

O. Monitor valve positions.

Pressure

All Systems

A. Use a 4:1 safety factor on plumbing.

B. Provide overpressure protection and controls on GSE.

C. Ensure procedures preclude overpressure. Provide burst disc and/or relief device at 10 percent above maximum operating relieve to closed vent system.

D. Control thermal conditions of hydrazine tank to 110°F maximum under all conditions.

E. Monitor tank pressures.

F. Pressure test at no greater than 1/4 maximum operating pressure.

G. Provide pressure relief devices.

H. Design with adequate safety factor.

I. Apply fracture control program.

J. Provide procedural controls.

K. Provide redundant pressure relief devices.

L. Monitor tank pressures and provide vent and relief override. Size vents for maximum loading rate.

M. Provide flexibility in plumbing support.

N. Select valve operating times to preclude high surges.

O. Provide pressure limiting devices in pressurization system.

P. Provide vent and relief override.

Toxicity

Hydrazine

A. Provide protective clothing.

B. Monitor area for leakage.

C. Understand vapor dispersion characteristics for area.

D. Ensure emergency equipment is satisfactory.

E. Ensure emergency procedures are available.

F. Design to contain PTU propellant plus 10 percent, dike area.

G. Provide scrubber for vent system.

H. Ensure system is not activated.

I. Ensure drain and flush of components.

J. Test components for residuals prior to removing protective clothing.

K. Ensure procedures cover all safety aspects.

System Safety - Tug

Inhibit Functions

A. Main engine ignition

B. Main engine prevalves

C. Main tanks pressurization system

D. Main engine pneumatic valves

E. Main tank isolation valves

F. ACPS valves and pressurization

G. Thermal conditioning - engine recirc

H. Thermal conditioning - engine idle mode

I. Active thermal conditioning - engine

J. TVC system

K. GNC lasers

L. Fuel cell pressurization system

Override Functions

A. Main tanks vent and relief valves

B. Overboard dump

C. Thermal control purge system

D. Primary battery circuit

E. Emergency battery circuit

Section 8
EXCEPTIONS/DEVIATIONS

At the present time, the only identified exceptions/deviations from government furnished safety criteria and requirements is in the area of quantity-distance requirements for propellants on the Tug while in the orbiter bay. It is considered that this is inherent with the system and is therefore acceptable based upon the rationale for acceptance as noted in Section 6 of this document.

Appendix 1

CAPTURE AND DOCKING ANALYSIS

TUG/ORBITER CAPTURE AND DOCKING SAFETY ANALYSIS

There are a number of associated events in the various phases of Tug retrieval including the acquisition, capture, and subsequent stowage of the Tug in the Orbiter bay. The Tug and Orbiter initially perform readiness and gross location actions. Thereafter, the Orbiter is the active element and the Tug is the passive, cooperative target. The relative separation of the two is closed to 30 feet for this operation. The Shuttle Attached Manipulator System (SAMS) is then brought up to the Tug pickup fitting. The Orbiter maintains a very close station-keeping with this fitting by keeping the SAMS grappler within a foot of the Tug fitting. The velocity error of the SAMS grappler to the Tug will not exceed 0.1 foot per second and 0.1 degree per second about any axis. Thus, the SAMS is only required to complete its capture within these distance and motion limits--a soft capture.

After capture, it is necessary to position the Tug so that it may be remated with the tilt table. Upon remating, the mate/latch function is accomplished to fix the Tug to the tilt table and make all the disconnects required.

The Tug is rotated into the Orbiter bay and additional vent and electrical umbilicals are connected. Vent and dump of Tug fluids is then accomplished with subsequent safing of the Tug subsystems.

A sample time line with events of safety significance is added to provide information as to the critical nature of the capture events.

MISSION EVENT NO.	EVENT START TIME HR:MN:SC	EVENT DURATION HR:MN:SC	EVENT	TUG/ORBITER SAFETY IMPACT
101	29:53:25	00:05:00	ALIGN IMU. UPDATE STATE VECTOR (ORBITER)	NONE
102	29:58:25	00:10:00	ACQUIRE AND LOCKON TO TUG (ORBITER)	NONE
103	30:08:25	00:03:00	ESTABLISH COMMUNICATIONS BETWEEN VEHICLES (ORBITER)	NONE
104	30:11:25	00:02:00	TRANSFER TUG FLIGHT CONTROL TO ORBITER	NONE
105	30:08:25	00:05:00	RESPOND TO ORBITER COMMUNICATIONS	NONE
106	30:13:25	00:01:00	MANEUVER TUG TO PREFERRED RENDEZVOUS ATTITUDE	NONE
107	30:14:25	01:08:30	STATION KEEP, MAINTAIN ATTITUDE CONTROL	NONE
108	30:18:45	00:04:00	DETERMINE RANGE AND RANGE RATE (ORBITER)	NONE
109	30:22:45	00:02:00	DETERMINE RENDEZVOUS INTERCEPT MANEUVERS (ORBITER)	NONE
110	30:24:45	00:03:00	COMPUTE TPI BURN PARAMETERS (ORBITER)	NONE
111	30:27:45	00:05:00	MANEUVER ORBITER TO REQUIRED ATTITUDE FOR TPI BURN (ORBITER)	NONE
112	20:32:45	00:30:00	VERIFY ORBITER READINESS FOR TPI BURN (ORBITER)	NONE
113	30:35:45	00:01:00	PERFORM TPI BURN (ORBITER)	NONE
114	30:36:45	00:03:00	PERFORM COURSE CORRECTION OPERATIONS (ORBITER)	NONE
115	30:36:45	00:01:00	COMMAND DEACTIVATION/SAFE TUG MAIN PROPULSION (ORBITER)	NONE
116	30:37:45	00:01:00	DEACTIVATE/SAFE MAIN TUG PROPULSION	CRITICAL[1]
117	30:38:45	00:01:00	VERIFY COMPLETION OF MAIN PROPULSION SAFING	CRITICAL[2]
118	30:39:45	00:04:00	DETERMINE RANGE AND RANGE RATE (ORBITER)	NONE
119	30:43:45	00:03:00	COMPUTE TPF BURN PARAMETERS (ORBITER)	NONE
120	30:46:45	00:03:00	ORIENT ORBITER FOR INITIAL TPF BURN (ORBITER)	NONE
121	30:49:45	00:03:00	VERIFY ORBITER READINESS FOR TPS BURNS (ORBITER)	NONE
122	30:52:45	00:00:10	PERFORM TPS BURNS (ORBITER)	NONE
123	30:52:55	00:04:00	READY CARGO BAY AND MANIPULATOR FOR TUG RETRIEVAL (ORBITER)	NONE

MISSION EVENT NO.	EVENT START TIME HR:MN:SC	EVENT DURATION HR:MN:SC	EVENT	TUG/ORBITER SAFETY IMPACT
124	30:55:55	00:00:20	COMMAND TUG TO PREFERRED DOCKING ATTITUDE (ORBITER)	NONE
125	30:56:15	00:01:00	MANEUVER TUG TO PREFERRED DOCKING ATTITUDE	MARGINAL[3]
126	30:57:55	00:04:00	VISUALLY INSPECT TUG FOR DOCKING READINESS (TBD N MILES)	MARGINAL[4]
127	30:59:55	00:00:30	INHIBIT TUG ACPS	CRITICAL[5]
*128	31:00:25	00:06:00	VERIFY ALL TUG SUBSYSTEMS SAFE FOR DOCKING	CRITICAL[6]
*129	31:06:25	00:06:00	MANEUVER ORBITER TO FINAL DOCKING STATION	CRITICAL[7]
*130	31:12:25	00:15:00	STATION KEEP ORBITER AND ATTACH MANIPULATOR TO TUG	CRITICAL[8]
131	31:27:25	00:02:00	VERIFY PHYSICAL ATTACHMENT INTEGRITY (ORBITER)	CRITICAL[9]
132	31:29:25	00:10:00	POSITION TUG TBD FEET FROM TILT TABLE	MARGINAL[10]
133	31:39:25	00:20:00	REMATE TUG WITH TILT TABLE	CRITICAL[11]
134	31:59:25	00:05:00	MATE/LATCH TUG TO BASE RING	MARGINAL[12]
135	31:59:25	00:02:00	VERIFY ATTACHMENT (ORBITER)	CRITICAL[13]
136	32:01:25	00:05:00	CONNECT ELECTRICAL UMBILICALS	CRITICAL[14]
137	32:06:25	00:05:00	VERIFY UMBILICALS CONNECTED (ORBITER)	CRITICAL[15]
138	32:11:25	00:03:00	RELEASE, STOW/DEACTIVATE MANIPULATOR	NONE
139	32:14:25	00:05:00	ROTATE TUG INTO CARGO BAY	CRITICAL[16]
140	32:19:25	00:02:00	CONNECT VENT LINES (ORBITER/TUG)	CRITICAL[17]
141	32:16:45	00:15:00	SAFE TUG FOR RETURN TO EARTH. ADD GHe TO LH_2 TANK	CRITICAL[18]
142	32:31:45	00:06:00	CONFIGURE CARGO BAY FOR ORBITER ENTRY	NONE
143	32:37:45	00:03:00	CONFIGURE TUG SUBSYSTEMS FOR DEORBIT AND ENTRY	NONE

*TIME OF MANIPULATOR ATTACHMENT MUST BE MINIMIZED TO ASSURE TUG DOES NOT MOVE OUTSIDE OF RECAPTURE ENVELOPE.

1. Deactive/Safe Main Tug Propulsion

and

2. Verify Completion of Main Tug Propulsion Safing

This is considered a critical event since failure to completely deactivate the Tug main propulsion could result in unprogrammed motion in the vicinity of the Orbiter. This could occur either as a result of inadvertent activation of the system or through propulsive venting of fluids through the engine.

In addition, the failure to completely deactivate the system could result in subsequent leakage of gases in the Orbiter bay.

3. Maneuver Tug to Preferred Docking Attitude

and

4. Visually Inspect Tug for Docking Readiness

The preferred docking attitude controls rate of rotation in addition to other attitudes. It is necessary that these be within the conditions desired to preclude difficulties on orbiter approach and capture.

These maneuvers should be performed at TBD miles from the orbiter to preclude impingement of ACPS exhaust on the Orbiter. In addition, at this distance any unprogrammed motions would not affect the Orbiter.

5. Inhibit Tug ACPS

This is considered a critical event since failure to completely deactivate the Tug ACPS could result in unprogrammed motion in the vicinity of the Orbiter. This could occur either as a result of inadvertent activation of the system or from leakage creating propulsive forces near the Orbiter.

In addition, the failure to completely deactivate the system could result in subsequent leakage of gases in the Orbiter bay.

6. Verify All Tug Systems Safe for Docking

If we are unable to verify the safety of all Tug subsystems then the docking operation should be performed under emergency/special procedures.

It will be necessary to determine the particular system that is not indicating safe, the condition of the safing signal, and establish the rationale of acceptance or rejection of the indication based upon pre-planned operational procedures.

7. Maneuver Orbiter to Final Docking Station

One of the critical events associated with capture and docking is the approach of the Orbiter to the Tug. In order to maintain the Tug in a stable position it is important to assure that the OMS exhausts do not impinge on the Tug in such a manner as to cause unprogrammed movement of the Tug. In addition, the exhaust plume should not deposit contaminants on the Tug that could eventually contaminate the orbiter bay or degrade the Tug systems for future operations.

This maneuver should result in the Orbiter being at approximately 30 feet from the Tug and with its dynamics matching the Tug dynamics within the limits established.

8. Station Keep Orbiter and Attach Manipulator to Tug

The relationship of the Tug and Orbiter as established in the previous note should be continued until the manipulator may be extended and safely attached to the Tug. The operation of the manipulator should be such that through normal operation or inadvertent rapid operation, no unprogrammed motion be imparted to the Tug.

In addition, the manipulator should impart no damage to Tug structure by improper or inadvertent operations. All human errors must be considered in this critical event.

9. Verify Physical Attachment Integrity

Since the single manipulator arm is a single point failure at the Tug/Manipulator inferface it is important that the attachment integrity is verified prior to moving the Tug to the close vicinity of the Orbiter. It is recommended that in addition to an indicator showing a satisfactory attachment that a physical attach mechanism be provided to assure correct mating of the manipulator arm and the Tug.

10. Position Tug TBD Feet From Tilt Table

Upon affirmation of a positive capture by the manipulator, the Tug should be positioned TBD feet from the tilt table.

Since the manipulator operator cannot see the tilt table/Tug relationship from his position two gimballed TV cameras and associated lighting will be mounted on the tilt table. In addition, two bullseye tagets, well illuminated, should be strategically located on the Tug base to aid in alignment of the Tug to the tilt Table.

11. Remate Tug with Tilt Table

Utilizing the provided TV and bulls-eyes, the manipulator operator should slowly move the Tug toward the tilt table, assuring alignment and parallelism through the use of the bulls eyes.

The Tug should be guided to the point of engagment with the physical guides of the tilt table.

12. Mate/Latch Tug to Base Ring

and

13. Verify Attachment

Continuing the guidance established in the remating operation, the operator moves the Tug to the position where the latches can be operated. This should assure a complete latch and capture with umbilicals firmly attached.

It is important that the attachment be verified to preclude a Tug breaking loose and causing physical damage in the Orbiter bay.

14. Connect Electrical Umbilicals

and

15. Verify Electrical Umbilicals

Electrical power is required to assure the safing of various critical circuits such as the main propulsion system and the ACPS.

16. Rotate Tug to Cargo Bay

and

17. Connect Vent Lines

During the rotation of the Tug into the cargo bay it is necessary that strict control be maintained over the rate of rotation. Any failure in the rotation system could cause Tug damage which could subsequently harm the Orbiter.

It is also required that all umbilicals be firmly and securely mated as a result of this operation.

18. Safe Tug for Return to Earth

This is the most critical event of the Tug acquisition, capture, and stowage operations in that if this event cannot be verified then it may be necessary to re-accomplish some of the operations.

All systems must be verified for safety prior to any further operations. In the event that any event occurs that is unplanned, the crew must have complete manual override of all functions and available pre-planned procedures to cover the unplanned events. If the safety of the Tug cannot be verified in these checks, the Orbiter must be capable of depositing the Tug in space and returning to Earth without the Tug.

Appendix 2

PRELIMINARY SYSTEM SAFETY PROGRAM PLAN

June 7, 1973
Draft copy

McDONNELL DOUGLAS ASTRONAUTICS COMPANY-WEST

SYSTEM SAFETY PROGRAM PLAN (PRELIMINARY)

1.0 SCOPE & OBJECTIVE

1.1 Scope

This preliminary plan defines the activities to be conducted by MDAC-W in implementing a System Safety Program for the Space Tug.

1.2 Objective

The objective of this plan is to outline the methods to be utilized in developing safety design characteristics during the Phase A portion of the Space Tug Program.

2.0 DEFINITIONS

2.1 Hazard Classification

Identified hazards are evaluated and classified as follows:

2.1.1 Safety Catastrophic - Condition(s) such that environment, personnel error, design characteristics, procedural deficiencies, or subsystem malfunction will cause system or personnel loss.

2.1.2 Safety Critical - Condition(s) such that environment, personnel error, design characteristics, procedural deficiencies, or subsystem malfunction can be counteracted by urgent crew action (no time available for ground/flight crew analysis) to prevent system or personnel loss.

2.1.3 Safety Marginal - Condition(s) such that environment, personnel error, design characteristics, procedural deficiencies, or subsystems malfunction can be counteracted or controlled with time available for ground/flight crew analysis to prevent system and/or personnel loss.

2.1.4 Safety Negligible - Condition(s) such that personnel error, design characteristics, procedural deficiencies, or subsystem failure will not result in system or personnel loss.

2.2 Hazard Reduction Precedence Sequence

To eliminate or control hazards, the following sequence or combination of items shall be used as a minimum:

2.2.1 Design for Minimum Hazard. The major goal throughout the design phase shall be to ensure inherent safety through the selection of appropriate design features as fail operational/fail safe combinations and appropriate safety factors. Hazards shall be eliminated by design where possible. Damage control, containment and isolation of potential hazards shall be included in design considerations.

2.2.2 Safety Devices. Known hazards which cannot be eliminated through design selection shall be reduced to an acceptable level through the use of appropriate safety devices as part of the system, subsystem, or equipment.

2.2.3 Warning Devices. Where it is not possible to preclude the existence or occurrence of a known hazard, devices shall be employed for the timely detection of the condition and the generation of an adequate warning signal. Warning signals and their application shall be designed to minimize the probability of wrong signals or of improper personnel reaction to the signal.

2.2.4 Special Procedures. Where it is not possible to reduce the magnitude of an existing or potential hazard through design, or the use of safety and warning devices, special procedures shall be developed to counter hazardous conditions for enhancement of ground and flight crew safety. Precautionary notations shall be standardized.

3.0 SYSTEM SAFETY TASKS

3.1 Safety Analysis

The identification of hazards is accomplished by applying the safety criteria to the system concepts/design and to the operation concepts/plans.

The application of the safety criteria results in the cause and effect displayed as a hazard analysis. The hazard analysis is guided by the undesired event, energy source, system/subsystem function/event, and the operational flow of the system.

As the hazards are identified, the proposed solutions are reevaluated against the system and operations to assure that the impact of the solution will not provide an undesired effect upon the system.

The techniques applied at this phase of the program are the Preliminary Hazard Analysis and the Operational Hazards Analysis. These analyses are performed to show gross hazards in all program events for equipment and operations. The analysis for equipment is shown as the Preliminary Hazard Analysis and covers hardware related hazards while the analysis of operations is shown as Operational Hazards Analysis and covers functionally related hazards.

The purposes of these analyses are to develop a complete understanding of the system and identify areas where control of the hazard can be accomplished by prudent design or functional controls. The process is iterative in nature and results in improved system design.

The analyses covers each of the following activities:

1. Pre-flight Operations
2. Flight Operations
3. Post-flight Operations
4. Refurbishment and Maintenance Operations

The following potential hazards will be considered for each of the activities identified.

1. Acceleration
2. Contamination
3. Corrosion
4. Dissociation, chemical
5. Electrical
6. Explosion
7. Fire
8. Heat & Temperature
9. Leakage
10. Moisture
11. Oxidation
12. Pressure
13. Radiation
14. Replacement, chemical
15. Shock
16. Stress Concentrations
17. Stress Reversals
18. Structural Damage or failure
19. Toxicity
20. Vibration and Noise
21. Weather and Environment

3.1.1 Preliminary Hazard Analysis (PHA)

A PHA will be conducted as the initial system safety analysis task. This analysis will be a general qualitative study of the subsystem in its operating environment to detect and define potential hazards. This analysis will identify

PRELIMINARY HAZARD ANALYSIS

SUBSYSTEM	HAZARDOUS MATERIAL/OPERATION/ CONDITION	POSSIBLE INCIDENT	WORST PROBABLE CONSEQUENCE	HAZARD CATEGORY
1	2	3	4	5

Figure -1. Preliminary Hazard Analysis Format

features which can impair mission capability through accidental damage or loss and aid in developing steps which can be taken to ensure that these features are avoided. The PHA will be completed in the format shown in Figure 5-1.

In order that correct assignment of information to the format categories can be accomplished, it is necessary to interpret and define the column headings. The PHA format is explained as follows. The numbers are referenced to the encircled numbers in Figure 1.

1. Subsystem--This column carries the noun title of the subsystem being investigated.

2. Hazardous Material/Operation/Condition--This column carries information as to whether the material is toxic, radioactive, corrosive, etc.; whether the operation may cause a hazardous condition to exist; or whether the conditions of pressure, temperature, voltages, etc., are present.

3. Possible Incident--This column identifies the incident which is associated with the related hazardous condition.

4. Worst Probable Consequence--This column provides an estimate of the consequences to the system caused by the incident.

5. Hazard Category--This column identifies the level of the hazard as defined in Subsection.

3.1.2 The operational hazards format is shown on Figure 2.

1. Planned Operation - This column carries the subsystem name and the specific operational event being investigated.

OPERATIONAL HAZARDS ANALYSIS

PLANNED OPERATION	HAZARD	HAZARD CLASSIFICATION	SOURCE	POSSIBLE CONTROL

FIGURE 2

2. Hazard - The hazard column indicates the hazards identified as applicable to the planned operation.

3. Hazard Classification - The hazards are classified as safety catastrophic, safety critical, or safety marginal.

4. Source - The source column contains the identification of the source of the hazardous material/operation/condition under investigation.

5. Possible Control - This column indicates the action/control to be taken to eliminate the hazard, or reduce the risk to an acceptable level.

3.1.3 Hazards Analysis Action

All analyses developed are coordinated with the appropriate design or operations group for their concurrence. The information developed will be utilized to control the hazards identified through application to the design by the responsible engineering group. If adequate resolution cannot be accomplished at the designer level, the hazard data will be submitted to the management level for resolution.

Appendix 3

HAZARD REVIEW CHECKLIST

HAZARD REVIEW CHECKLIST

HAZARD	OCCURRENCE	POSSIBLE CAUSE	POSSIBLE EFFECTS
ACCELERATION:			
	Any mass which undergoes a change in velocity.	Vehicle, body, or fluid being set into motion, being stopped, or changing speed. Any body being dropped. Impact by or against another body. Friction or resistance to body motion. Applied force against an unrestrained body.	Seating or unseating of spring loaded valves, electrical contacts. Loss of fluid pressure head (cavitation). Pressure surges in fluid systems. Overloading of structural members. Sloshing and entrapment of liquids. Deflection of flexible or shock isolated parts. Deflection of piping. Propellant vent turbulence. Injury to personnel.
CONTAMINATION:			
	Any system or equipment: Open to entry of dirt, dust, or other contaminants. In presence of contaminants. In which contaminants can be formed.	Poor quality control. Polymerization. Microbial growth. Inadequate protection from contaminants. Filtration system overload or failure. Solvent residues. Inadequate solvent for cleaning. Tropical environment. Salt environment. Oxide scale. Metal particles. Airborne dirt. Silica sand. Lapping compound. Process residues. Organic fibers. Plastic and elastomer fragments. Misalignment or poor fitting of parts.	Deterioration of fluids; a breakdown or alteration of fluids by direct chemical reaction; particle surface catalysis; heat from friction; formation of sludge; emulsification with water. Increased friction between sliding surfaces. Degradation of performance. Clogging and blocking of lines, valves, regulators, filters, nozzles, orifices. Scoring and abrasion of closely fitted moving surfaces. Flammable contaminants in air being compressed may ignite. Large particles in fluids may erode lines and equipment. Impact of fast moving pieces may crack or break lines and equipment. Fungus growth. Electrical leakage. Increased corrosion. Penetration of resilient materials. Reduction in lubricity. Valve seating interference. Altered flow direction.
CORROSION:			
	Metals which react with air. Any system with reactive chemicals. Materials susceptible to moisture or airborne salts.	Lack of compatibility of materials as designed. Leakage of corrosive or reactive substances. Exposure to unforeseen environment. Damaged protective surfaces. Flooding or immersion. Condensation of atmospheric moisture. Electrolyte corrosion (dissimilar metals). Stray electrical currents. Vibration and fatigue. Salt atmosphere.	Material degradation. Changes in physical and chemical properties. Reduction in strength. Surface roughness. Binding of moving surfaces, nuts, and other parts. Contamination of the system. Loss in resiliency of springs.
DISSOCIATION, CHEMICAL:			
	Monopropellants, fuels or oxidizers. Explosives. Organic materials. Epoxy compounds.	Temperature of compound raised to point reaction begins. Presence of suitable catalyst. Shock.	Explosion. Nonexplosive exothermic reaction. Material degradation. Toxic gas production. Corrosion fraction production. Swelling of organic materials.

ELECTRICAL:

Shock	Any "live" electrical circuit. Power generators. Natural electrical sources (Lightning) Dry plastics and organic materials (static electricity). Batteries.	Contact with live circuit erroneous connection. Failure to discharge capacitive circuit. Cutting through insulation. Touching part of short circuit.	Personnel Electrocution Clamping Involuntary reactions Interference with performance
Thermal	Other electrochemical reactions.	Short circuit. Erroneous connection. Faulty connector. Ground at wrong point. Live wires touching. Dirt, contamination or moisture.	Burnout of equipment. Melting of soldered connections. Ignition of combustibles. Increased temperatures. Personnel burns.
Inadvertent Activation		Breakdown of dielectric. Stray energy due to inductive or capacitive coupling. Static electricity discharge. Lightning strike. Inadequate electrical insulation. Electrostatic discharge. Faulty connector or connection. Corrosion. Dirt or other contamination. Moisture. Excessive solder. Cut wires. Bent pins. Improper wiring. Improper mating. Worn keyways. Poor alignment devices.	Firing of ordnance devices. Untimely electrical equipment starts. Endangering of personnel working on circuits or equipment.
Power Source Failure		Inadequate electrical protection. Overloading of electrical equipment. Inadequate heat dissipation. High resistance circuits. Sparking and arcing. Welding or buildup of contacts. Lack of adequate grounding. Electrolytic action. Misapplied test equipment power. Photosensitive materials. Lack of "fail-safe" design. Lack of "backup" equipment. Power surges causing circuit breaker activation.	Entire system inoperative. Necessary equipment unavailable. Release of holding devices. Interruption of communications. Detection and warning devices inactivated.
Electromagnetic Radiation		Radar equipment operation. Communication equipment operation. Nuclear detonation.	Interference with electronic equipment operation. Heating of metal parts by induction and eddy currents.

EXPLOSION:

Ordnance or munitions systems. Any fuel system. High pressure equipment. Cryogenic liquid system.	Inadvertent activation of: High explosives. Propellant explosives or combustible gases in containers or confined spaces. Fine dusts and powders. Combustible gases or liquids. In high concentrations. In presence of strong oxidizers. At high temperatures. Activation of cracked or otherwise defective solid propellant motors. Afterburning of confined combustion products. Delayed combustion in a firing chamber. Cold soaking of solid propellants. Overpressurization of boilers, accumulators or other pressure vessels. Warming closed cryogenic or other system containing highly volatile fluid. Contact between water or moisture with water-sensitive materials such as molten sodium, potassium or lithium; concentrated acids or alkalis; or similar substances.	Rupture of engines, motors, or other pressurized container. Blast. Overpressures (impulse energy). Collapse of nearby containers. Damage to structures and equipment. Propagation of other explosions. Fragmentation. Holing of nearby containers and vehicles. Impact of pieces against personnel equipmen and structures. Dispersion of burning, hot, combustible, or corrosive materials. Heat (see heat and high temperature). Dispersion of toxic materials. Injury to personnel.

FIRE:

1. All normally combustible materials:
   a. Fuels
      (1) Propellants: liquid, solid, or gel.
      (2) Engine use: diesel oil, gasoline, JP & RP fuels.
      (3) Engine start: ethylene oxide, TEA, TEB.
      (4) Auxiliary power unit: hydrazine.
      (5) Heating: kerosene, fuel oil.
   b. Solvents and cleaning agents.
   c. Lubricants.
   d. Welding gases.
   e. Paints and varnishes.
   f. Coolants: ammonia.
   g. Elastomers (seals and gaskets)
   h. Hydraulic fluid.
   i. Wood products.
   j. Plastics.
   k. Clothing.
   l. Vegetation.
   m. Refuse and trash.
   n. Other organic materials.
2. Normally low combustible materials in presence of strong oxidizers or high temperatures:
   a. Solvents - trichloroethylene, methylene chloride.
   b. Lubricants.
   c. Hydraulic fluids.
3. Normally nonflammable metals in finely powdered form:
   a. Aluminum.
   b. Magnesium.
   c. Titanium.
   d. Iron.
4. Afterburning of products of combustion of engine operation: Carbon monoxide.

1. Combustible mixture with initiating sources such as:
   a. Open flame
      (1) Welding processes and flame cutting.
      (2) Matches, smoking.
      (3) Gas heaters or process equipment.
      (4) Engine exhaust.
      (5) Nearby fires.
   b. Sparks.
      (1) Electrical
      (2) Mechanical
      (3) Chemical - Carbon
   c. Catalyst
2. Combustible mixture heated to autoignition temperature by:
   a. External heat sources.
      (1) Electric heaters or hot plates.
      (2) Boilers, radiators, steam lines and equipment.
      (3) Operating engines, motors or compressors.
      (4) Exhaust stacks or manifolds.
   b. Friction.
   c. Inadequate dissipation of chemical reaction heat (spontaneous ignition).
      (1) Oily rags.
      (2) Sawdust, excelsior.
      (3) Powdered plastics.
   d. Compression of flammable mixture.
   e. Hypergolic mixture, including sensitivity to water.
   f. Pyrophoric reaction with air.
   g. Radiation from nuclear detonation.

Heat and its effects.
Loss of oxygen.
Production of toxic gases and smoke.
Production of corrosive materials.
Burns to personnel.
Explosions.
Renders equipment inoperative.
Destruction of material and resources.
Carbonization and contamination of materiel.

HEAT & TEMPERATURE:

High Temperature

Any fuel consuming process.
Other exothermic chemical process.
Electrical equipment.
Solar energy.
Biological or physiological processes.
Moving equipment or parts.

Fire or explosion.
Other exothermic reaction.
Heat engine operations.
Electrical energy losses.
Aerodynamic or other vehicular friction.
Friction between moving parts or vehicle and surrounding medium.
Gas compression.
Inadequate heat dissipation
Cooling system failure
Welding, soldering, brazing, or metal cutting.
Proximity to operations involving large amounts of heat (radiation, convection, conduction).
Immersion in hot fluid.
Lack of insulation.
Exposure to sun or artificial light.
Hot climates or weather.
Human or animal heat output.
Organic decay processes.

Ignition of combustibles.
Initiation of other reactions.
Melting of metals.
Charring of organic materials.
Increased reactivity.
Reduced materiel strength.
Reduced equipment life.
Distortion and warping of parts.
Expansion of solids and liquids.
Increased evaporation rate of liquids.
Expansion may cause binding or loosening of parts.
Increased gas diffusion.
Reduced relative humidity.
Increased absolute humidity.
Breakdown of chemical compounds.
Personnel burns.
Reduced personnel efficiency.
Heat cramps, strokes, and exhaustion.
Peeling of finishes, blistering of paint.
Evaporation or decreased viscosity of lubricants.
Changes in electrical characteristics.
Softening of insulation and sealants.
Opening or closing of electrical contacts due to expansion.

Low Temperature		
Any heat removal process. Refrigerating or cryogenic systems. Polar, high altitude, or winter conditions.	Cold climate or weather. Endothermic reactions. Exposure to heat sink. Mechanical cooling processes. Gas expansion. Rapid evaporation. Inadequate heat supply. Heat loss by radiation, conduction, or convection. Solid propellant cold soaking.	Freezing of liquids. Condensation of moisture. Reduced reaction rate. Frostbite or cryogenic burns. Reduced viscosity. Increased brittleness or metals. Loss of flexibility of organic materials. Fuel blend stratification. Contraction effects. Propellant cracking. Delayed ignition, and combustion instability in engines. Icing of operating equipment. Decreased viscosity of lubricants. Changes in electrical characteristics. Jamming or loosening of moving parts due to contraction.
Temperature Variations		
Any system or part which gains or loses heat.	Gain or loss of heat due to radiation, conduction, or convection. Input of electrical energy. Gas expansion. Diurnal heating and cooling. Stopping and starting of heat engines.	Dimension changes, expecially in metals. Pressure changes in confined gases and liquids. Imposition of stresses in and cracking of materials with low coefficients of expansion.
LEAKAGE:		
Any vessel or conductor which contains or is immersed in a fluid.	Cracks caused by structural failure. Hole caused by impact. Porosity or other weld defect. Inadequately fitted or tightened parts. Fittings loosened by vibration. Corroded metals or seals. Worn parts. Excessive fluid pressure. Cuts in organic materials (seals, gaskets, hoses) Poorly designed connections. Dirt or other solid contamination between mating surfaces. Erroneously opened drains or fittings. Overfilling of containers.	Release of toxic, corrosive, radioactive, flammable, or otherwise reactive material. Loss of system fluids. Loss of system pressure. Loss of lubricants. Contamination or degradation of materials in a container. Short circuiting of electrical equipment.
MOISTURE:		
High Humidity		
Wet climate or weather. Proximity to bodies of water Moisture producing processes. Inflow of underground water. Large amounts of vegetation. Personnel in inadequately ventilated enclosures or equipment.	High atmospheric humidity. Rain, snow, hail, ice, or dew. Flooding and immersion. Leakage. Perspiration. Temperature decrease without removal of moisture. Malfunction of air conditioning equipment. Condensation on cold surfaces. Presence of humidifying equipment. Contact with water-absorbent materials such as concentrated acids and alkalis, ammonium perchlorate.	Corrosion. Electrical short circuiting. Personnel discomfort. Contamination. Leaching of solid propellant ingredients. Clouding of viewing surfaces. Icing of equipment and aerodynamic surfaces. Violent reactions, explosions, or fire with water-sensitive materials. Swelling of water absorbent materials.
Low Humidity		
Dry climates or weather. Proximity to hot, dry processes.	Low atmospheric humidity. Temperature increase without addition of moisture. Operation of dehumidifying equipment.	Static electricity generation. Dehydration and cracking of organic materials. Dehydration of personnel. Dehydration and cracking of skin. High cooling rate on exposed body surfaces.

OXIDATION:

Missile propellants. Welding oxygen. Oxygen for respiratory protective equipment. Laboratory chemicals. Process chemicals. Cleaning compounds.	Chemical combination involving oxidants such as: Oxygen or ozone. Halogens or halogen compounds. Oxidizing acids and their salts. Nitrates, chlorates, perchlorates, hyperchlorites, chromates. Higher valence compounds of mercury, lead, selenium, and thallium.	Increased reactivity of combustibles. Easier ignition. Normally low flammable materials may burn easily. May cause violent or explosive reactions. Partner in hypergolic reactions. Corrosion. Forms explosive gels with some fuels. Deterioration of rubber, plastics, or other organic materials. Almost all volatile strong oxidizing agents but oxygen are toxic.

PRESSURE:

High		
Hydraulic systems. Pneumatic systems. Cryogenic systems. Pressurized containers Boilers Underwater vehicles. Engine cylinders.	Overpressurization. No pressure relief or vent. Faulty pressure or relief valve. Heating of fluids with high vapor pressures. Warming cryogenic liquids in a closed or inadequately vented system. Impact. Blast. Container hit by fragments. Failure or improper release of connectors. Inadequate restraining devices. Rapid submersion. Deep submersion Water hammer (hydraulic shock)	Container rupture. Blast. Fragmentation. Propelling of container. Hose whipping. Blowing other objects (eye hazards). Increased reaction rate. Skin penetration. Lung damage. Cutting effects. Shock. Leaks in lines and equipment designed for lower pressures. Dimensional changes. Actuation forces and opposition.
Low		
Vacuum systems. High altitude vehicles. Space vehicles.	Compressor failure. Increase of altitude without pressure relief Inadequate design against collapsing forces. Increase in altitude without suitable respiratory equipment. Rapid condensation of gas in a closed system. Decrease in gas volume by combustion. Cooling of hot gas in a closed system.	Unbalanced forces. Collapse of pressure vessels. Inadequate breathing air. Inadequate combustion air. Leaks. Bursting of pressurized vessels. Physiological damage (atelectasis).
Rapid Changes		
High altitude vehicles. Space vehicles. Underwater vehicles. Compressing or pumping equipment. Airfoils. Carburetors.	Rapid expansion of gas. High gas compression. Rapid changes of altitude. Loss of cabin pressurization at high altitudes or in space.	Joule-Thomas cooling. Compressive heating. Explosive decompression. Physiological disturbances. (cramps, bends, chokes)

RADIATION:

Thermal (Infrared)		
Any heat producing body or process.	Solar radiation. Flames. Highly heated surface.	Undesirable heat gain (see High Temperature under Heat). Overheating. Skin burns. Charring of organic materials.
Electromagnetic		
Radar equipment. Communication equipment.	Radar equipment operation. Communications equipment operation.	Initiation of ordnance devices. Interference with operation of other electronic equipment.
Ionizing		
Radioactive materials. X-ray equipment. Radar equipment. Communications equipment. Nuclear weapons.	Inadequate containment of radioactive materials. Inadequate protection of equipment. Excessive exposure to ionizing source.	Tissue damage. Degradation of material strength.
Ultraviolet		
Electrical welding processes. Light sources.	Sunshine. Welding arcs. Germicidal lamps.	Decomposition of chlorinated hydrocarbons into toxic gases. Ozone or nitrogen oxide generation. Vision damage. Deterioration of materiel. Color fading.

REPLACEMENT, CHEMICAL		
Fluorine and water. Sodium and water. Nitric acid and water.	Replacement of a chemical radical by a more active one.	Exothermic reactions. Explosions. Violent spraying of corrosive material.
SHOCK:		
Any part or piece of equipment.	Impact. Handling and transportation damage. Blast. Pneudraulic actuated devices. Acceleration. Electroexplosive detonating devices. Water hammer. Vibrations caused by heavy equipment.	Breakage of cables, ropes, chains, pin. Fracture of brittle materials. Detonation of sensitive explosives. Normally closed contacts may open. Normally open controls, valves, contacts may close. Parts may be displaced. Hinged parts may open or close. Disruption of metering equipment.
STRESS CONCENTRATIONS:		
Any load carrying part or solid material.	Sharp corners, expecially at line where two right angle planes meet. Residuals caused by manufacturing processes such as machining, grinding, extruding, drawing. Surface treatment, such as shot peening, cold working, plating. Assembly stresses caused by shrink or press fits, torquing Surface roughening due to corrosion, chemical action, abrasion, erosion. Notch sensitivity due to scratches or blows. Temperature variations on poor conductors, due to heating, cooling, or heat treatment. Welding arc start indentations. Cyclic changes in stress from tension to compression, Wide variations in temperature. Change from high pressure to vacuum (or vice versa) without suitable equalization.	Cracking. Chipping. Structural failure. Reductions in corrosion resistance.
STRESS REVERSALS:		
Vibrating or oscillating equipments. Flexing panels. Cryogenic equipment. High temperature equipment. Vacuum equipment.	Cyclic changes in stress from tension to compression. Wide variations in temperature. Change from high pressure to vacuum (or vice versa) without suitable equalization.	Structural failure. Reduction in corrosion resistance. Delaminations of layered material.
STRUCTURAL DAMAGE OR FAILURE:		
Any part, piece of equipment, vehicle, structure, container, or connector.	Impact and shock. Blast. Rough handling. Object dropped on hard surface. Hard object dropped on vulnerable part. Momentum against hard object (collision). Moving object hitting vulnerable part. Rotating part hitting foreign object. Inadequate design strength. Overloading. Reduction of strength by: Corrosion. Stress concentrations. Poor workmanship Crimping.	Bending - Distortion which prevents an object from: Fulfilling its function. Fitting into another part. Maintaining alignment of parts. In rotating equipment this may result in damage to other parts, vibration, noise, or shock. Being removed from another part. Cracking - Initial failure at a surface or edge creating: Stress concentrations leading to more serious failures such as breaking or rupture. Leakage of fluids. Rough surfaces. Regions contaminants may accumulate. Regions corrosion may take place. Breaking - Separation of an object by failure

STRUCTURAL DAMAGE OR FAILURE (cont)	Excessive centrifugal force. Overpressures due to internal or external fluids. Poorly fitted or inadequately tightened parts. Overtorquing. Loss of strength due to high temperatures. Expansion and distortion of parts due to heating. Brittleness and loss of ductility due to cold. Exposure to aerodynamic loads. High accelerations. Chafing of parts caused by vibration or other motion. Fatigue due to vibration. Cutting or punching by sharp pointed objects.	into two or more parts: Parting of cables, chains, slings. Rupture of pressure containers or lines. Tearing of materials. Shearing of metal or plastic parts, bolts, or pins. Twisting or torquing of shafts, nuts, or bolts. Crushing or collapse of containers or structures. Shattering or brittle materials. Splitting away of a portion or extension of a body from its main mass. Crimping - Cutting into a wire, cable, or pipe by a sharp object. Reduces strength permitting easy breakage. Creates a high resistance point in electrical wires. Reduces or blocks the flow of fluid. Permits leakage of fluid.
TOXICITY:		
Any substance whose presence in relatively small amounts will produce physiological damage or disturbance. Any situation where a lack of breathing oxygen may exist.	Toxic gases, liquids, or metal particles. Inadequate oxygen present for respiration: High altitudes. Dilution by inert gases. Combustion involving oxygen. Lack of ventilation in occupied space. Inadequate respiratory protection. Inadequate skin protection. Inadequate personal cleanliness. Accidental ingestion. Outgassing of substance at low ambient pressures.	Irritation of eyes, nose, throat, or respiratory passages. Respiratory system damage. Blood system damage. Damage to body organs. Skin damage (dermatitis) Nervous system effects (narcosis, anesthesia, paralysis, nerve damage). Annoyance by foul odors. Reduction of personnel efficiency or capabilities. Destruction of vegetation.
VIBRATION AND NOISE:		
Any type of mechanical equipment or parts.	Rotating or reciprocating equipment. Transportation. Engine exhaust. Flutter or buzz of aerodynamic surfaces. Water hammer (hydraulic shock). Vibrating tools. Misalignment of equipment, loose mountings. Worn bearings. High velocity fluid hitting a surface or object which can vibrate. Cavitation in pumps and blowers.	Fracture of brittle materials. Loosening of bolted or other threaded parts. Uncoordination and fatigue of personnel. Pressure waves. Interference with communications. Decrease in metal corrosion resistance. Metal fatigue or other changes in crystalline structure. Chattering of spring type contacts, valves. Pointer type devices may give false readings.
WEATHER AND ENVIRONMENT:		
Any out-of-doors location.	Moisture Rain Clouds Fog Snow Hail Extreme cold Extreme heat Solar radiation High winds Inversion Airborne salts, dust, dirt, fungi Lightning	High humidity conditions. Low humidity conditions. Ultraviolet radiation effects. Infrared radiation effects. High temperature effects. Low temperature effects. Temperature change effects. Corrosion. Contamination. Pressure effects on large surfaces may cause structural overloads, movement, or toppling. Loss of visibility due to fog, clouds, condensation. Impact damage by hail. Inversions may reflect noise or vibration. Inversions may prevent convection of toxic gases. Electrical shock, inadvertent activation, disruption of power systems, electromagnetic effects.

Appendix 4

SAFETY CRITERIA AND REQUIREMENTS

3.2.1 Reliability

3.2.1.1 Mission Success

3.2.1.1.1 The Tug shall be compatible with the STS mission success probability of 0.90. Mission success is defined as the ability of the STS to successfully complete a given mission. Tug mission success is defined as the ability of the Tug to successfully deploy or retrieve a given payload. DP

3.2.1.1.2 The mission completion reliability goal for the Tug shall be 0.97 minimum for each of the six reference missions. Mission profiles shall include all launch operations, mission operations, and recovery operations through completion of recovery and Tug safing by the Shuttle. Level of redundancy and component reliability shall be selected and defined to meet this criteria. SOW

3.2.2 Safety

3.2.2.1 General

3.2.2.1.1 The Tug shall be consistent with the safety implications of operations in the vicinity of manned vehicles. SOW/DP

3.2.2.1.2 The Tug shall be capable of providing a safe mission operation while passively contained within the orbiter cargo bay and have provisions for relaying immediately to the orbiter crew, while it is attached to the orbiter, any emergency condition originating in the Tug. DP

3.2.2.1.3 While in the orbiter cargo bay on the launch pad or during ascent, retrieval, reentry, and landing, the Tug shall provide a readout of parameters critical to Shuttle system and launch site safety. DP

3.2.2.2 Safe Return

The Tug shall be compatible with the safe return probability of the STS. Safe return is defined as the capability of the STS elements to return safely to the earth's surface after attempting or completing a mission operation. In the event a deployment has not been accomplished, or that a payload has been retrieved, safe return shall include return with a payload. Tolerance to failures shall be such that the combined probability of a safe return of the orbiter for any given STS mission shall have a design goal equal to or exceeding 0.999. DP

3.2.2.3 Normal Operations

3.2.2.3.1 No single Tug failure shall result in a hazard which jeopardizes the flight or ground crews. DP

3.2.2.3.2 Appropriate safety factors will be used where necessary to minimize the possibility of failures which might affect manned safety. DP

3.2.2.3.3 All primary and secondary structural components where critical load conditions occur while the Tug is attached to the Shuttle shall be designed with minimum allowable safety factors of 1.4 ultimate and 1.1 yield. For a structural component whose critical load condition occurs during Tug operation or other times where failure of the component will have no effect on the Shuttle system, the component shall be designed with minimum allowable safety factors of 1.25 ultimate and 1.10 yield. All pressure vessels shall have a safety factor of 2.0 ultimate. SOW

3.2.2.3.4 The Tug shall be capable of safely venting propellant boiloff gases. SOW

3.2.2.3.5 Stowage in Orbiter

3.2.2.3.5.1 A functional avionics interface between the Tug and the orbiter shall be provided with the capability for command DP

override control of necessary Tug functions while in flight within the cargo bay, attached to the deployment mechanism, and during rendezvous and docking with the orbiter.

3.2.2.3.5.2	The Tug shall be capable of being loaded in a safe and acceptable manner with propellants, pressurants, and other fluids while in the Shuttle payload bay.	SOW
3.2.2.3.5.3	Orbiter to Tug connections shall be designed for emergency manual release by orbiter crew member in extravehicular activity.	DP
3.2.2.3.5.4	Destruct charges shall not be incorporated in the Tug tanks which automatically limits the maximum pressure. Venting shall be through the Tug/Orbiter interface.	DP
3.2.2.3.5.5	The capability shall be provided on the Tug for remote emergency jettisoning of deployable equipment to allow retrieval and stowage in the orbiter cargo bay.	DP
3.2.2.3.5.6	Toxic or other chemically hazardous gases, liquids, or particles shall not be vented into the Orbiter payload compartment, and shall be isolated from the Orbiter ECS System.	DP

3.2.2.3.6 On-Orbit -- General

3.2.2.3.6.1	The Tug main and auxiliary propulsion shall be capable of being inhibited while attached to the orbiter, including deployment, and retrieval phases.	MDAC
3.2.2.3.6.2	No single failure shall result in unprogrammed motion of the Tug while within TBD distance of the Orbiter.	DP
3.2.2.3.6.3	All venting of the Tug within TBD distance of the Orbiter shall be non-propulsive.	DP
3.2.2.3.6.4	The Tug shall provide to the Orbiter such information concerning the status or the condition of the Tug, as is necessary to insure a safe post-deployment and pre-retrieval condition.	DP
3.2.2.3.6.5	Provision shall be made for control of critical Tug functions, including attitude and translational position control by Orbiter crew during post-deployment and preretrieval operations for Orbiter Tug separation distances to TBD.	DP
3.2.2.3.6.6	A backup means shall be provided for the orbiter crew to vent or pressurize upper stage vehicles with a pressure stabilized structure.	MDAC

3.2.2.3.6.7 Contaminants from outgassing systems or propellant combustible discharges of the Tug shall not impinge harmfully upon the payload or the Shuttle. The Tug shall not discharge or jettison solid debris in orbit in the vicinity of where payload operations are to be performed. DP

3.2.2.3.7 On-Orbit -- Deployment

3.2.2.3.7.1 Provision shall be made for Orbiter control of critical Tug functions while the deployment/retrieval mechanism is attached. DP

3.2.2.3.7.2 No single failure shall result in unprogrammed motion of the Tug. DP

3.2.2.3.7.3 When the Tug and/or payload are being deployed in orbit, the design of the Tug and/or payload control systems shall only allow supply of electrical energy to the start valves of the rocket engines following positive action by the orbiter crew. MDAC

3.2.2.3.7.4 When the Tug vehicle is undergoing a countdown in orbit, the design of the Tug and/or payload control systems shall only allow supply of electrical energy to the separation mechanism following positive action by the orbiter crew. MDAC

3.2.2.3.8 On-Orbit -- Retrieval

3.2.2.3.8.1 The Tug shall provide the Orbiter such information concerning the status or condition of the Tug as is necessary to insure a safe retrieval operation. DP

3.2.2.3.8.2 Provision shall be made for Orbiter control of critical Tug functions while the retrieval mechanism is attached. DP

3.2.2.3.8.3 No single failure shall result in unprogrammed motion of the Tug. DP

3.2.2.3.8.4 Provisions shall be made to confirm that all Orbiter/Tug interfaces are securely connected after Tug retrieval. DP

3.2.2.3.8.5 Provisions shall be made for static discharge. DP

3.2.2.4 Abort Operations

3.2.2.4.1 The Tug shall not preclude the Shuttle from intact abort as defined in Space Shuttle Specification No. MJ072-0001, Par. 3.2.1.5. DP

3.2.2.4.2 Manned factors of safety shall be maintained under abort load conditions. DP

3.3 Interface Requirements

3.3.1 General

3.3.1.1 The physical and mechanical spacecraft to Tug interfaces and Shuttle to Tug interfaces between an interim Tug and the evolved Tug of greater capability are intended to be the same. Functional interface changes as the Tug evolves shall be minimized. DP

3.3.1.2 The Tug communication systems shall be compatible with existing NASA and DOD ground and space networks. SOW

3.3.2 Orbiter/Tug Interfaces

3.3.2.1 Operations

The orbiter provides a standard mechanism for on-orbit deployment, docking, retrieval, and stowage of all Shuttle payloads. The Tug shall be compatible with this mechanism and shall have attachment and docking fittings which are compatible with those of the orbiter either directly or through a Tug-supplied adapter. DP

3.3.2.2 Initialization and Update

The Tug data management system shall be capable of accepting initialization and update services from the orbiter and shall DP

be capable of its own initialization within one-half revolution.

3.3.2.3 Abort

The Tug shall be compatible with all Shuttle abort modes and procedures. DP

3.3.2.4 Deployment/Retrieval Mechanism

The Tug to cargo bay attachment hardware and the deployment and retrieval mechanisms shall be compatible with the orbiter concepts and the hardpoint locations as specified in the Space Shuttle definition. DP

3.3.2.5 Post Retrieval Interfaces

After retrieval from orbit, the appropriate Tug/Shuttle interfaces will be re-established. SOW

3.3.2.6 Status Check

There shall be direct communication, during ascent or reentry of the orbiter between the orbiter and the Tug when Tug is stowed in the orbiter cargo bay. For the DOD mission, the rates shall be as follows: DP

16 kbps of status data with 2 kbps of command verification

interleaved shall be received from the orbiter by the Tug. The overall BER shall be no greater than 10^{-6}.

16 kbps of secure telemetry or status data shall be sent from the Tug to the orbiter. These data shall include command verification as well as 2 kbps of payload health data interleaved.

256 kbps of payload secure data shall be coupled directly through the Tug to the orbiter via hardwire connection.

A standard FM/FM IRIG channel H hardwire line shall be coupled directly through the Tug to the orbiter.

3.3.2.7 Post Deployment and Preretrieval RF Communications

There shall be direct communication between the Tug and orbiter when Tug is in the vicinity of the orbiter. For the DOD mission the rates shall be as follows: DP

The Tug shall be capable of receiving 2 kbps of SCF compatible secure commands having a BER no greater than 10^{-5} when at a range compatible with the mission requirements. The Tug shall be capable of transmitting TLM at 16 dbps. The data shall contain 2 kbps of payload health, Tug command verification, and Tug health status to the

orbiter. The overall BER shall be 10^{-5} at a range compatible with the mission requirements.

3.3.2.8 Navigation Update

Shuttle to Tug navigation update will consist of position velocity, attitude, and time. DP

Position will be to 3.0 nmi RSS 3σ

Velocity will be to 5.6 fps RSS 3σ

Attitude will be to 4 arc min, assuming an orbit Tug/Shuttle alignment of 3 arc min

Time will be to 1 part in 10^{10}

3.3.2.9 Umbilicals between Tug and Orbiter shall be provided for servicing, safing, control, and monitor of the Tug by the Orbiter. MDAC

3.3.2.10 The requirements for Tug electrical power from the Orbiter shall be minimized. MDAC

3.3.3 Payload/Tug Interfaces

3.3.3.1 Orientation and Alignment

3.3.3.1.1 Thermal Control

The Tug shall have the capability of maintaining a spatial orientation and/or providing a roll rate to satisfy payload thermal requirements. The thermal control system of the Tug shall not provide thermal control for any payload system. MDAC DP

3.3.3.1.2 Deployment

The Tug shall be capable of orientation relative to the orbit plane within 3 degrees and of deploying payloads in a stable mode with the following velocity and tip off rates maximum: DP/MDAC

Longitudinal velocity	5.0 ft/sec
Tipoff rates	0.1 deg/sec, pitch, yaw, and roll

3.3.3.1.3 Retrieval

The Tug shall have the capability to determine the payload orientation for docking and shall be designed to the following conditions: DP

Radial misalignment	±6 inches
Longitudinal velocity	0.1 to 1.0 fps
Lateral velocity	0.3 fps
Angular misalignment	±3 degrees
Angular rate	±2.4 deg/sec

3.3.3.2 Interface Structure and Loads

3.3.3.2.1 Loads

The Tug structure shall be designed to accommodate the worst case combination of payload weight, payload c.g., and Shuttle environment. MDAC

3.3.3.2.2 Attachment

Tug attachment for payloads, spin/despin kit, if required, servicing module and multipayload adapters shall be provided. MDAC

3.3.3.3 Mechanical

3.3.3.3.1 Latches

3.3.3.3.1.1 The Tug shall provide a means of unlatching the payload attaching restraints. MDAC

3.3.3.3.1.2 The Tug shall provide means for retracting the Tug/Payload umbilicals. MDAC

3.3.3.3.2 Separation

The Tug shall deploy payloads (stationary or spinning) such that the following is not exceeded: DP/MDAC

Longitudinal velocity	5.0 fps
Tipoff rates	0.1 deg/sec (all axes)
Torque	35 in.-lb, pitch and yaw
Acceleration	0.1 g

3.3.3.3.3 Docking

The Tug deployment mechanism shall be capable of capturing either a three-axis or spin stabilized Tug deployed payload. MDAC

3.3.3.4 Electrical

3.3.3.4.1 Power

The Tug shall be capable of supplying to the payload 300 watts (average) 28 vdc from liftoff through payload deployment and shall also be capable of supplying 300 watts 28 vdc from payload docking through orbiter retrieval, descent, and landing. D/P

3.3.3.4.2 Connector

The Tug shall provide a separable, remateable power connector to the payload. MDAC

3.3.3.4.3 Grounding

The Tug shall provide a means of preventing electrical current flow between the Tug and payload structures. MDAC

3.3.3.5 Avionics

3.3.3.5.1 Status Monitoring

The Tug shall be capable of monitoring and commanding the payload when the payload is attached or in the vicinity of the Tug. This shall include the capabilities for data transfer and communication and electric power while attached to the Tug and data transfer and communication while in the vicinity of the Tug. DP

3.3.5.2 Data Transfer and Communication

3.3.3.5.2.1 Status Checkout

There shall be direct communication, during ascent or reentry of the Orbiter, between the payload and the Tug when the Tug is stowed in the Orbiter bay. The data signals for the IDD missions are as follows: DP

16 kbps of telemetry or status data shall be received from the payload. The data shall contain command verification. The BER shall be no greater than 10^{-6}.

256 kbps of payload secure data shall be received by the Tug via hardwire.

Standard FM/FM IRIG Channel H data shall be received by Tug via hardwire.

3.3.3.5.2.2 Post Deployment and Preretrieval RF Communications

There shall be direct communication between the Tug and the payload for DOD missions as follows: DP

2 kbps of SCF compatible secure commands will be sent to the payload from the Tug. The BER shall be no greater than 10^{-5} when at a range compatible with the mission requirements.

16 kbps of SCF compatible secure TLM will be received from the payload by the Tug when the payload is at a range compatible with the mission. The BER shall be no greater than 10^{-5}.

The commands shall have an echo check capability.

The overall BER shall be no greater than 10^{-8}

when the echo check is compared with generated command bit.

3.3.3.5.3 Caution and Warning

A hardwire interface between the Tug and payload shall be provided for conveying health and safety signals through the Tug to the Orbiter while the Tug/payload is in the Orbiter bay. MDAC

3.3.3.5.4 RF Communications

RF communication capability shall be available between the Tug and payload for command and control functions. DP

3.3.3.5.6 Guidance, Navigation, and Control

3.3.3.5.6.1 Insertion

The Tug shall be capable of placing payloads in orbit with position and velocity accuracies relative to specific target orbit conditions to within the following position and velocity accuracies: DP

Synchronous Altitude (Deployment)

	Position (nmi)(3σ)	Velocity (fps)(3σ)
Tangential	60	20
Normal	20	50
Radial	70	70

3.3.3.5.6.2 Retrieval

The Tug shall be capable of rendezvous and docking with a payload, the position of which is known to ±1 nmi 3σ in each axis. DP

3.3.3.5.6.3 Station Keeping

For monitoring, inspection of, or observing a satellite, the Tug shall be capable of maintaining a preselected range and line-of-sight with respect to local vertical. MDAC

3.3.3.6 Ordnance

3.3.3.6.1 Command Discretes

The Tug shall provide discrete command signals to activate payload ordnance devices as required and to safe and verify all unused devices prior to retrieval. MDAC

3.3.3.7 Environment

3.3.3.7.1 Tug Induced Effects

The Tug shall not induce environmental effects on the payload significantly greater (10-20 percent) than those induced by the Shuttle. DP

3.3.3.7.2 Contamination

Contaminants from outgassing systems, fuel cell venting, or propellant combustible discharges of the Tug shall not impinge harmfully upon the payload. The Tug shall not discharge or jettison solid debris in orbit in the vicinity of where payload operations are to be performed. DP

3.3.3.8 Servicing

3.3.3.8.1 Checkout

The Tug shall be capable of checking out the payload prior to deployment. DP

3.3.3.8.2 Spin/Despin

In missions where payload spin/despin is required, the Tug will provide the spin/despin energy. DP

3.3.3.8.3 Appendages

The Tug shall provide power and command signals for retracting/stowing payload appendages as necessary for retrieval. MDAC

3.3.3.8.4 Repair

The Tug shall have the capability to service and/or repair payloads on orbit by accommodation of a servicing kit. MDAC

3.3.4 Ground Systems/Tug Interfaces

3.3.4.1 Servicing

The Tug shall be capable of being serviced by the standard Space Transportation System environmental, power, and fluids service facilities. Unique support requirements shall be provided by the Tug contractor. DP

3.3.4.1.2 The Tug shall be designed to remain in the Shuttle cargo bay in a safe condition for a maximum of 24 hours after landing prior to its removal and transfer to a maintenance and refurbishment area. MDAC

3.3.4.2 Facilities

3.3.4.2.1 The interface plates, cables, and lines required by the Tug to interface with the facilities and supporting ground support equipment shall be Tug supplied. Tug unique ground support equipment shall be supplied with the Tug and shall be compatible with the standard facilities services. DP

3.3.4.2.2 The Tug shall also be capable of interfacing with a secure SGLS compatible communications system when secure data transmissions are required to support Tug processing procedures. DP

3.3.4.3 Checkout and Test

3.3.4.3.1 The Tug shall utilize the automatic checkout AGE for pre- and post-flight checkout and test procedures. Unique Tug checkout and test equipment shall be provided by the Tug contractor. DP

3.3.4.3.2 When installed in the orbiter cargo bay on the launch pad, Tug access to the automatic checkout system shall be via the standard Tug to orbiter interfaces. DP

3.3.4.4 Avionics

3.3.4.4.1 Prelaunch

The Tug shall be capable of both RF and hardline checkout while stowed in the orbiter cargo bay. DP

3.3.4.4.2 On-Orbit

There shall be direct communications between Tug and ground stations for DOD missions as follows: DP

The Tug shall be capable of receiving 2kbps of SCF compatible secure commands having a BER no greater than 10^{-5} when at any range up to 30,000 nmi from an SCF ground site. Also, the Tug shall accept SCF compatible PRN signals and turn-around for SCF ranging. The Tug shall be capable of transmitting both 16 kbps of TLM at 10^{-5} BER and relaying of 256 kbps of data direct from the payloads to an SCF site.

3.3.4.5 Propellants and Pressurant Loading and Off-Loading

3.3.4.5.1 The cryogenic Tug shall be capable of being loaded and off-loaded with main propellants and pressurants while inside the orbiter cargo bay with the spacecraft attached. This shall be accomplished utilizing the main Shuttle propellant DP

loading system GSE through Tug fill and drain lines separate from those of the Shuttle and will be accessible with the Shuttle on the pad in the vertical position with the cargo bay doors closed.

3.3.4.5.2 Storable Tug propellants and pressurants may be loaded either on the pad while the Tug is in the cargo bay or at some remote tanking facility prior to Tug/Shuttle integration. Tug propellant loading and off-loading shall be accomplished in such a manner that no contaminants are introduced into the orbiter cargo bay. DP

3.3.4.5.3 Replenishment of the cryogenic Tug propellants in the event of a hold will be accomplished via the Tug main propellant loading system. GSE through Tug fill and drain lines will be separate from those of the Shuttle. Separate propellant loading lines shall not be required for the replenishment operation. DP

4.0 SUBSYSTEM DESIGN REQUIREMENTS.

4.1 General

The docking mechanisms, Tug, and payload shall be designed for the following conditions: DP

TUG/KICKSTAGE INTERFACE							
INTERFACE REQUIREMENT	MDAC PARA. NO.	DATA PACKAGE		INTERFACE TYPE		INCORPORATED	
		PAGE	PARA	HARD	SOFT	YES	NO
All structural components shall be designed with minimum allowable safety factors of 1.4 ultimate and 1.1 yield.	3.2.2.3.3						
All pressure vessels shall have a safety factor of 2.0 ultimate.	3.2.2.3.3						
Destruct charges shall not be incorporated in the kick stage when launched in the orbiter.	TBD						
Kick stage initiation systems shall be inhibited while attached to the Tug including deployment, and retrieval phases.	TBD						
Provide information concerning the status or the condition of the kick stage as is necessary to insure a safe post deployment and preretrieval condition.	TBD						
Contaminants or propellant combustible discharges of the kick stage shall not impinge harmfully upon the Tug.	TBD						
Provide information concerning status or condition of the kick stage as is necessary to insure a safe retrieval operation.	TBD						
Provisions shall be made for static discharge.	3.2.2.3.8.5	72	d4				
The kick stage shall not preclude the Shuttle from intact abort.	TBD						
Compatible with all Shuttle abort modes and procedures.	TBD						
Kick stage/Tug interfaces will be re-established on retrieval.	TBD						
Umbilicals between Tug and kick stage shall be provided for safing, control, and monitor of the kick stage.	TBD						

TUG/KICKSTAGE INTERFACE							
INTERFACE REQUIREMENT	MDAC PARA. NO.	DATA PACKAGE		INTERFACE TYPE		INCORPORATED	
		PAGE	PARA	HARD	SOFT	YES	NO
The kick stage shall provide a separable, remateable, and resafable/safe and arm device.	TBD						
Provide a means of preventing electrical current flow between the Tug and kick stage structures.	TBD						
Hardwire interface for conveying health and safety signals through the Tug to the Orbiter while the Tug/kick stage is in the Orbiter bay.	TBD						
Provide discrete command signals to activate kick stage ordnance devices as required and to safe and verify all unused devices prior to retrieval.	TBD						
Thermal control system shall provide an acceptable temperature for the kick stage.	TBD						
Safety design features such as interlocks, redundance, grounding, and isolation devices shall be incorporated so that no single detectable failure or combination of undetectable failures shall result in premature detonation of explosive devices.	4.10.1	73	5a				
Unused explosive devices aboard the kick stage must be safed on command and safing verification sent to the Orbiter prior to retrieval.	TBD						
Provide caution/warning information on the kick stage safe and arm device.	TBD						
Kick stages shall not contain destruct charges.	TBD						
RFI and EMI levels of the Orbiter/Tug shall not initiate kick stage firing circuits.	TBD						
Test on the kick stage firing circuits shall not be performed in the orbiter bay.	TBD						
Tests on the kick stage TVC shall not be performed in the Orbiter bay.	TBD						
Outgassing from the kick stage propellants while mounted in the Orbiter bay shall not contaminate the bay or create a hazardous atmosphere.	TBD						
Grounding provisions shall be provided for all phases of operations with the kick stage & its related hardware.	TBD						