August 9, 1973

Safety Presentation

Space Tug Systems Study (Storable)

GEORGE C. MARSHALL SPACE FLIGHT CENTER
HUNTSVILLE, ALABAMA

CONTRACT NAS 8 - 29675

(NASA-CR-179100) SPACE TUG SYSTEMS STUDY (STORABLE) Safety Presentation (Martin Marietta Aerospace) 101 p Avail: NTIS

N87-70408

Unclas
00/18 0074248

MARTIN MARIETTA

SAFETY PRESENTATION, AUGUST 9, 1973

CONTENTS

	Page No.
System Safety Overview	1 thru 14
System Safety Presentation	15 thru 39
System Safety Plan, Revision 1	40 thru 49
Operation & Maintenance Hazard Summary	50 thru 57
System Safety Checklist	58 thru 79
Operational Safety Checklist	80 thru 84
Potential Hazard Matrix	85 thru 86
Hazard Analysis	87 thru 93
Hazard Catalog, Part I	94
Hazard Catalog, Part II	95 thru 97
Proposed Safety Outline for September Presentation	98
Proposed Reliability Outline for September Presentation	99

SAFETY SUMMARY PRESENTATION AGENDA

1. SAFETY TASK OVERVIEW
2. SYSTEM SAFETY METHODOLOGY & RESULTS
3. RELIABILITY METHODOLOGY & RESULTS
4. PROPOSED OUTLINE FOR SEPTEMBER 17 DATA DUMP

MARTIN MARIETTA

SAFETY GUIDELINES

- ALL HAZARDS MUST BE IDENTIFIED
- ALL HAZARDS MUST BE ELIMINATED OR CONTROLLED
- NO SINGLE POINT FAILURE SHALL RESULT IN HAZARDS TO FLIGHT OR GROUND CREW (STRUCTURAL ELEMENTS AND PRESSURE VESSELS ARE EXCLUDED)
- TUG SHALL BE DESIGNED TO MANNED FACTORS OF SAFETY
- TUG SHALL PROVIDE TUG SAFETY STATUS INFORMATION TO ORBITER
- ORBITER CREW SHALL HAVE COMMAND OVER SAFETY CRITICAL FUNCTIONS WHILE TUG IS IN OR IN THE VICINITY OF ORBITER

MARTIN MARIETTA

SAFETY APPROACH

- DIFFUSE SAFETY CONSCIENCENESS
- DESIGN SAFETY INTO SUBSYSTEM/SYSTEM
- EVALUATE SAFETY IN TRADE STUDIES
- CONDUCT SYSTEM SAFETY ANALYSIS
- REDUCE HAZARDS
- IDENTIFY RESIDUAL HAZARDS

MARTIN MARIETTA

SAFETY - PRIMARY CONSIDERATIONS

- STORABLE PROPELLANTS
  - FUEL - MONOMETHYL HYDRAZINE (MMH); FLAMMABLE, TOXIC, GENERALLY CONSIDERED NON-CORROSIVE AND NON-EXPLOSIVE
  - OXIDIZER - NITROGEN TETROXIDE (N_2O_4); CORROSIVE, TOXIC, GENERALLY CONSIDERED NON-EXPLOSIVE, AND NOT A FIRE HAZARD
  - MONOPROPELLANT - HYDRAZINE; SIMILAR TO FUEL
- HIGH PRESSURE SYSTEMS
  - PRESSURIZATION - AMBIENT HELIUM, APPROX 3700 PSIA
  - PROPELLANT TANKS - OXIDIZER TANK, APPROX 55 PSIA - MAX
    FUEL TANK, APPROX 25 PSIA - MAX
  - ACPS PRESSURIZATION - AMBIENT HELIUM, APPROX 3700 PSIA
  - MONOPROPELLANT TANK - HELIUM, APPROX 300 PSIA
- ORDNANCE
  - PAYLOAD SEPARATION MECHANISM
  - DROP TANK SEPARATION MECHANISM
  - KICK STAGE SRM IGNITER
- TRANSPORATION AND HANDLING
  - THIN SKIN CONSTRUCTION
  - LARGE VOLUME/WEIGHTS OF PROPELLANTS

MARTIN MARIETTA

HISTORY ON SAFETY HAZARDS

- STORABLE PROPELLANTS

  OVER 10,000,000 GAL OF PROPELLANT TRANSFERRED

- RUPTURE HISTORY ON TANKS AND PRESSURE VESSELS

	TITAN II	TITAN III	TRANSTAGE
PROOF TEST	5	0	1
LAUNCH OPERATIONS	0	0	0
FLIGHT	0	0	0

- ORDNANCE HISTORY

INADVERTENT ACTIVATION	2	0	0
FAILURE TO ACTIVATE	0	0	0

5

MARTIN MARIETTA

HISTORY ON SAFETY HAZARDS

300-400 ppm leak detectable

IN THE HANDLING OF STORABLE PROPELLANTS THE MARTIN MARIETTA CORPORATION HAS HANDLED IN EXCESS OF 10,000,000 GAL OF PROPELLANT.

THE TITAN II LEAK DATA FOR ALL SITES AS OF OCTOBER 1972 FOR THE PREVIOUS TWO CALENDAR YEAR SHOWED THE MINIMUM TIME FROM LOAD TO LEAK WAS 4 MONTHS. THE LOWEST TIME FOR A SEAL LEAK AFTER VEHICLE INSTALLATION IN THE SILO WAS 17 MONTHS. THE AVERAGE LEAK FOR BOTH SEALS AND COMPONENTS OCCURRED AFTER 40 MONTHS. AS OF OCTOBER 1972 THERE WERE THREE VEHICLES THAT HAD BEEN IN THE SILO FOR MORE THAN 58 MONTHS AND NEVER HAD A LEAK. THE LEAKS THAT DID OCCUR WERE EXTREMELY SMALL (NOT VISIBLE) AND WERE FOUND BY A PORTABLE LEAK DETECTOR PLACED DIRECTLY ON THE LEAKING COMPONENT.

THE RUPTURE HISTORY ON TANKS AND PRESSURE VESSELS IS VERY GOOD. ON TITAN II, TITAN III, AND TRANSTAGE ALL OF WHICH USE THE SAME PROPELLANTS, THERE HAS NEVER BEEN A FAILURE DURING LAUNCH OPERATIONS OR FLIGHT. ON TITAN II THERE WERE 5 PROPELLANT TANK FAILURES DURING HYDROSTATIC PROOF TESTING. THESE FAILURES OCCURRED APPROXIMATELY 10 YEAR AGO AND WERE ASSOCIATED WITH POOR WELDS. MANY OF THE PROCEDURES NOW USED TO VERIFY WELD INTEGRITY ON THE TITAN PROGRAM RESULTED FROM THESE FAILURES. ONE TRANSTAGE FAILURE OCCURRED DURING HYDROSTATIC PROOF TESTING, AND RESULTED FROM A MANUFACTURING PROBLEM DURING CHEMICAL MILLING OF THE PROPELLANT TANK.

THE ONLY ORDNANCE FAILURE ON TITAN II, III, AND TRANSTAGE WAS AN INADVERTANT IGNITION OF A TRANSLATION MOTOR ON TITAN II. THERE HAS NEVER BEEN AN ORDNANCE FAILURE ON TITAN III OR TRANSTAGE.

Table VI-5 Titan II Leak Data for Extended Storage

LITTLE ROCK AFB ARKANSAS

CMPX	MISSILE	DATE	*EXPOSURE TIME	LEAK LOCATION	TYPE LEAK	LEAK RATE	CORRECTIVE ACTION
				1971			
373-1	B-96	3/71	59 Mo.	St I Ox Burst Disc	S	N/A	Off-load & replace seals
				St II Ox Fill & Drain Q.D.	S	N/A	Off-load & replace seals
373-3	B-101	2/71	10(44) Mo	St I Ox Fill & Drain Cap	S	2 PPM	Replace cap wet
				St I Ox Vent inbd. seal	S	4 PPM	Replace seal wet
373-5	B-25	9/71	28 Mo.	St II Ox F&D ontbd. Seal	S	165 PPM	Off-load & replace seals
373-6	B-8	12/71	14(55)Mo	St II Ox Press Sw. Seal	S	N/A	Replace Seal Wet
373-7	B-38	7/71	30 Mo.	St II Ox Manhole Cover	S	11 PPM	Off-load & replace seals
374-2	B-63	6/71	59 Mo.	St II Ox F&D Outbd Seal	S	N/A	Off-load & replace seals
374-3	B-49	10/71	17 Mo.	St I Ox Prevalve Seal (Metal)	S	250 PPM	Off-load & replace seals
374-6	B-84	6/71	50 Mo	St I Ox Press Sw. Internal	C	N/A	Replace Sw. wet
374-8	B-34	2/71	58 Mo.	St II Ox Press Sw. Seal	S	4 PPM	Replace Seal Wet
		12/71	68 Mo.	St I Ox Low Level Sensor Seal	S	N/A	Off-load & replace seals
				1972			
373-7	B-38	4/72	39 Mo.	St II Ox Press Sw. Internal	C	200 PPM	Replace Sw. wet
373-8	B-71	3/72	29 Mo.	St II Ox Press Sw. Seal	S	N/A	Replace Seal Wet
		5/72	31 Mo.	St II Ox F&D outbd Seal	S	N/A	Off-load & replace seals
373-9	B-108	6/72	30 Mo.	St I Ox Press Sw. Internal	C	250 PPM	Replace Sw. Wet
374-1	B-11	6/72	4 Mo.	St I Ox Press Sw. Internal	C	N/A	Replace Sw. Wet
374-2	B-63	7/72	72 Mo.	St I Ox Low Level Sensor Seal	S	10 PPM	Off-load & replace seals
374-3	B-49	5/72	6(23)Mo.	St II Ox Press Sw. Seal	S	N/A	Replace seal wet
374-6	B-84	4/72	62 Mo.	St I Ox Manhole Cover	S	9 PPM	Off load & replace seals
374-7	B-72	3/72	65 Mo.	St II Ox F&D outbd Seal	S	200 PPM	Off-load & replace seals

Table VI-5 Titan II Leak Data for Extended Storage (Concl)

DAVIS-MONTHAN AFB ARIZONA

1971

CMPX	MISSILE	DATE	* EXPOSURE TIME	LEAK LOCATION	LEAK TYPE	LEAK RATE	CORRECTIVE ACTION
570-1	B-97	7/71	39 Mo.	St II Ox F&D Seal	S	250 PPM	Off-load & replace seals
570-8	B-66	12/71	66 Mo.	St I Ox Manhole Cover	S	25 PPM	Off-load & replace seals
570-9	B-56	8/71	19 (47) mo.	St I Ox Dead leg drain	S	6 PPM	Off-load & replace seals
571-8	B-65	3/71	48 Mo.	St II Ox F&D Seal	S	4 PPM	Off-load & replace seals
571-9	B-74	9/71	64 Mo.	St II Ox Manhole Cover	S	16 PPM	Off-load & replace seals

1972

NO LEAKS

MCCONNELL AFB KANSAS

1971

CMPX	MISSILE	DATE	* EXPOSURE TIME	LEAK LOCATION	LEAK TYPE	LEAK RATE	CORRECTIVE ACTION
532-3	B-106	12/71	48 Mo.	St II Ox Vent Seal Outbd	S	100 PPM	Replace seal wet
533-6	B-44	11/71	17(53)Mo.	St I Ox Manhole Cover	S	1 PPM	Off-load & replace seals

1972

532-4	B-86	1/72	55 Mo.	St II Ox Press Sw. Seal	S	5 PPM	Replace seal wet
		3/72	57 Mo.	St I fuel prevalve leaking thru casting	C	3 PPM	Apply sodium silicate
532-5	B-90	2/72	81 Mo.	St I Ox Press Sw. Internal	C	N/A	Replace sw. Wet

N/A means data is not available.

* Exposure time is the time the seal or component has been exposed to propellant prior to the leak developing. On 5 of the vehicles the Stage I and II oxidizer was off-loaded, all seals replaced and reloaded. These vehicles are indicated by the value in parentheses which represents the propellant exposure time of the mechanical joint. This additional data is provided to show the prior long term seal and joint integrity.

Leak Type - S is Seal and C is Component

SAFETY IMPACT ON PROPULSION SYSTEMS DESIGN

BASELINE DESIGN

- OFFSITE PROPELLANT LOADING (Structural design is loading - storage is airlock in orbiter)
- PROPELLANT DUMP CAPABILITY
  - BOTH HORIZONTAL & VERTICAL POSITIONS
  - EITHER IN OR SEPARATED FROM ORBITER
  - EITHER TANK FIRST
  - EITHER TANK SEPARATILY OR BOTH TANKS SIMULTANEOUSLY
- DOUBLE ISOLATION OF LIQUIDS AND GASES
- ATTITUDE CONTROL PROPULSION SYSTEM
  - FAIL OPERATE, FAIL SAFE
  - 16 NOZZELS FOR REDUNDANT CONTROL IN ALL SIX DEGREES OF FREEDOM FOR BOTH DEPLOY AND RETRIEVE

6

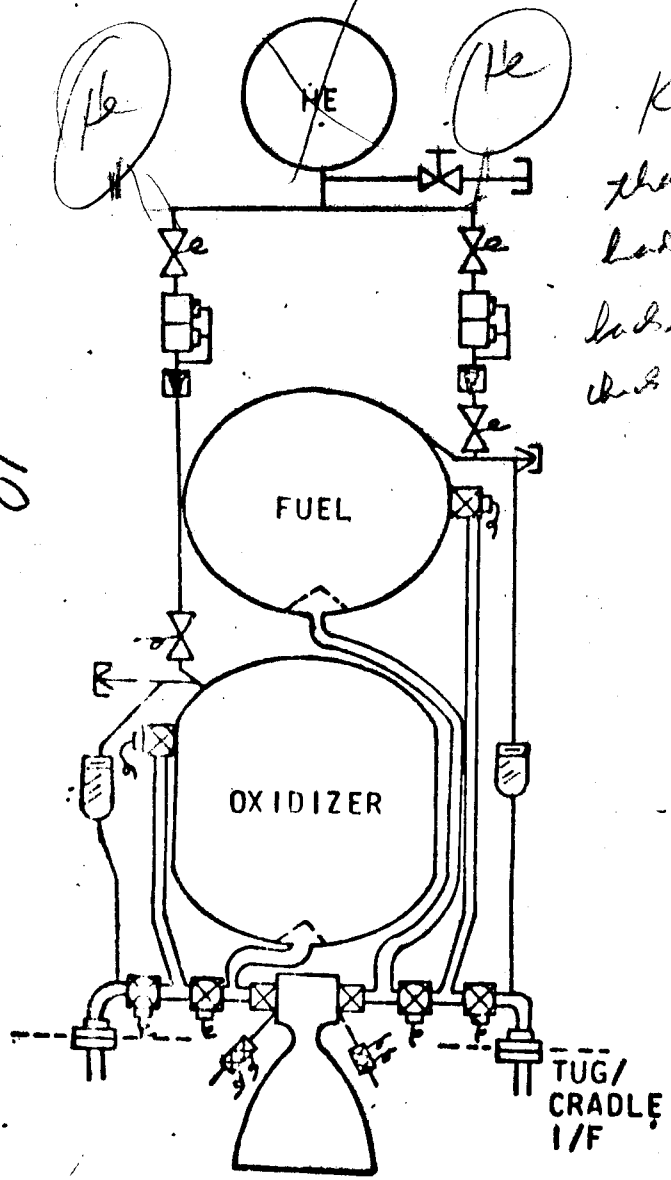
Cryogen. L/2

~~SENSITIVITY TO PROPELLANT DUMP BASED ON ASCENT ABORT TRAJECTORIES OVER 110,000 FT~~

- SIMULTANEOUS DUMP
- OXIDIZER ONLY DUMP
- PRELIMINARY RESULTS
  - INCREASED LINES SIZES TO 3 TO 4 IN DIA
  - POTENTIAL WEIGHT INCREASE OF 50 POUNDS

MARTIN MARIETTA

BLOCK DIAGRAM - CONFIGURATION PR-1 - SPACE TUG REGULATED HELIUM - AMBIENT STORAGE



KSC says that they have had trouble by backflow through this valve!!!

- HE MANUAL VALVE
- HE SOLENOID VALVE
- HE REGULATOR
- CHECK VALVE
- CAPPED DISCONNECT
- CAPPED DISCONNECT (SELF-SEALING)
- PROPELLANT SHUTOFF VALVE
- UMBILICAL DISCONNECT
- BURST/RELIEF VALVE

ID NO	WT CAT	MISSION (DAYS)	TUG	DRY WT	REMARKS
(1)	MAX	2/7	SS	367	T1 SPHERE, 18 # HE
(2)	AV	2/7	SS	307	COMPOSITE SPHERE, 18 # HE
(3)	MAX	2/7	DS	290	T SPHERE, 9 # HE
(4)	AV	2/7	DS	246	COMPOSITE SHPERE, 9 # HE
(5)	AV	2/7	1-1/2 S	674	80% IN DROP TANK

NOTE: TANKS ARE REVERSED ON SOME TUG CONFIGURATIONS

MARTIN MARIETTA

10

SAFETY IMPACT ON STRUCTURES DESIGN

- ISOLATED FUEL AND OXIDIZER TANKS
- PROPELLANT AND PRESSURANT TANKS PROTECTED FROM EXTERNAL DAMAGE (Pogo type damage)
- DESIGN CONSIDERATIONS IN ADDITION TO SPECIFIED FACTORS OF SAFETY
  - FRACTURE MECHANICS .018 T/T wall thickness
  - LEAK BEFORE BURST
  - MATERIAL SELECTION BASED ON STRESS CORROSIONS CONSIDERATIONS
- TUG CAN WITHSTAND NORMAL LANDING WITH LOADED PROPELLANT TANKS
- TUG CAN WITHSTAND CRASH LANDING WITH EMPTY PROPELLANT TANKS

MARTIN MARIETTA

SAFETY IMPACT ON AVIONICS

- SKEWED REDUNDANT IMU'S
- REDUNDANT DATA BUSES
- REDUNDANT GENERAL PROCESSORS
- REDUNDANT MEMORY UNITS
- FUNCTIONALLY REDUNDANT ACS NOZZELS
- EXTENSIVE CAUTION & WARNING LIMIT CHECKS/ TREND CHECKS VIA DATA MANAGEMENT SYSTEM
- REDUNDANT COMMUNICATION SYSTEM
- REDUNDANT MAIN POWER BUSES
- REDUNDANT LOAD POWER BUSES
- PROGRESSIVE CIRCUIT BREAKER SYSTEMS
- DATA MANAGEMENT SYSTEM FAIL OPERATE - FAIL SAFE

Arm control
use safety critical
function

MARTIN MARIETTA

SAFETY IMPACT ON GROUND OPERATIONS

- PROPELLANT AND PRESSURANT LOADING PRIOR TO ORBITER MATE
  - REMOTE SITE - CONTROLLED CONDITIONS
  - LEAK CHECK PRIOR TO LOADING
  - LEAK CHECK AFTER LOADING
  - REDUNDANT CRANES FOR TUG/ORBITER MATE
  - MONITOR VAPOR DETECTION SYSTEM
  - RESTRICT OVERHEAD ACCESS
  - INSTALL ADDITIONAL PROTECTIVE COVERING WHEN ORBITER BAY DOORS OPEN
- PYROTECHNIC INSTALLATION PRIOR TO ORBITER MATE
  - EMC VERIFIED
  - CIRCUIT VERIFIED
  - STRAY VOLTAGE TESTS
  - USE OF STANDARD PYROTECHNIC OPERATING PROCEDURES

MARTIN MARIETTA

SAFETY IMPACT ON MISSION OPERATIONS

- PROPELLANT TANKS NOT FULLY PERSSURIZED UNTIL AFTER DEPLOYED FROM ORBITER
- ORBITER CREW RETAINS CONTROL OF TUG UNTIL A SAFE DISTANCE FROM THE ORBITER
- TUG CAN SEPARATE FROM ORBITER USING ACPS
- MAIN ENGINE NOT STARTED UNTIL TUG SEPARATED FROM ORBITER $\approx$ 1 MI.

MARTIN MARIETTA

SYSTEM SAFETY PRESENTATION OVERVIEW

- SYSTEM SAFETY APPROACH
- SYSTEM SAFETY PLAN
- ANALYSIS METHODOLOGY
- ANALYSIS DISCUSSION AND RESULTS
- SUMMARY

MARTIN MARIETTA

SYSTEM SAFETY APPROACH

- DIFFUSE SAFETY CONSCIENCENESS
- TRADE STUDY CONSIDERATION
- SYSTEM SAFETY ANALYSIS
- HAZARD REDUCTION
- RESIDUAL HAZARDS

MARTIN MARIETTA

- SUBMITTED 17 MAY 1973
- REVISED 1 AUG 1973
  - CLARIFICATION OF SCOPE
  - NHB 5300.4 (ID) HAZARD LEVELS
  - CURRENT ANALYSIS FORMS

SYSTEM SAFETY ANALYSIS METHODOLOGY

- DEFINE OPERATIONAL PHASES
- DEFINE HAZARD GROUPS
- DEFINE SYSTEM/SUBSYSTEMS
- HAZARD IDENTIFICATION
- DETAILED HAZARD ANALYSIS
- ANALYSIS OUTPUT

MARTIN MARIETTA

SPACE TUG OPERATIONAL PHASES

- TRANSPORTATION AND HANDLING
- PREFLIGHT OPERATIONS
- LAUNCH OPERATIONS
- ORBITER FLIGHT
- TUG DEPLOYMENT/RETRIEVAL
- TUG FREE FLIGHT
- PAYLOAD DEPLOYMENT/RETRIEVAL
- POST FLIGHT OPERATIONS
- ABORT

MARTIN MARIETTA

HAZARD GROUPS

NO.	HAZARD	DEFINITION
1	ACCELERATION/SHOCK	CHANGE IN VELOCITY, APPLIED FORCE, IMPACT
2	CONFIGURATION	COMPONENT LOCATION, SYSTEM DEFICIENCIES
3.	CONTAMINATION	PRODUCING OR INTRODUCING CONTAMINANTS
4.	CORROSION	DAMAGE TO MATERIAL SURFACES
5.	ELECTRICAL	SHOCK, THERMAL, INADVERTENT ACTIVATION
6.	ENERGY SOURCES	PROPELLANTS, BATTERIES, ORDNANCE DEVICES
7.	ENVIRONMENT	NATURAL, INDUCED, POLLUTION
8.	FIRE/EXPLOSION/IMPLOSION	CHEMICAL REACTIONS, HEAT GENERATION, OVER/UNDER PRESSURE
9.	MAN-MACHINE RELATIONS	CONTROLS, DISPLAYS, HUMAN ERROR
10.	PRESSURE	HIGH, LOW, OR VARIATION
11.	RADIATION	ELECTROMAGNETIC, IONIZING
12.	STRUCTURAL	DEGRADATION, FAILURE
13.	SYSTEM INTERACTIONS	COMPATIBILITY BETWEEN INTERFACING SYSTEMS/GSE
14.	TEMPERATURE	HIGH, LOW, OR VARIATION
15.	TOXICITY	ADVERSE HUMAN EFFECTS

MARTIN MARIETTA

I. PROPULSION, GENERAL

II. MAIN ENGINE SUPPORT

III. ENGINE

IV. ATTITUDE CONTROL PROPULSION SYSTEM

V. AVIONICS

VI. THERMAL CONTROL

VII. STRUCTURES

VIII. KICK STAGE

HAZARD IDENTIFICATION

- POTENTIAL HAZARD MATRIX
  - INHERENT HAZARDS
  - OTHER ANALYSES
    - FMEA
    - OPERATIONS & MAINTENANCE
    - SYSTEM SAFETY CHECKLIST

MARTIN MARIETTA

POTENTIAL HAZARD MATRIX

CONFIGURATION: All System Study Task 5

SYSTEM: Propulsion, General

DATE: 08-01-73

PAGE: I-1

SUBSYSTEM/ COMPONENT	TRANSPORTATION & HANDLING	PREFLIGHT OPERATIONS	LAUNCH OPERATIONS	ORBITER FLIGHT	TUG DEPLOYMENT/ RETRIEVAL	TUG FREE FLIGHT	PAYLOAD DEPLOYMENT/ RETRIEVAL	POST FLIGHT OPERATIONS	ABORT	OTHER ANALYSES: FMEA	OTHER ANALYSES: OPERATIONS & MAINTENANCE	OTHER ANALYSES: DESIGN CHECK LIST
1. Propellants												
1.1 Oxidizer, N_2O_4		4,6,8, 15 (1.001)									2.2.1.9 (1.001)	
1.2 Fuel, MMH		6,8, 15 (1.002)									2.2.1.11 (1.002)	
2. Tanks												
2.1 Oxidizer		10 (1.003)								SFP-I,10 (1.003)		63 (1.003)
2.2 Fuel		10 (1.003)								SFP-I,11 (1.003)		63 (1.003)
3. Special Considerations												
3.1 Tug with propellants loaded	8 (1.004)										2.2.1.13 2.2.2.3 2.2.3.1 2.3.1 2.3.3.1 (1.004)	

2
3

POTENTIAL HAZARD MATRIX

CONFIGURATION: PR-1 (2)

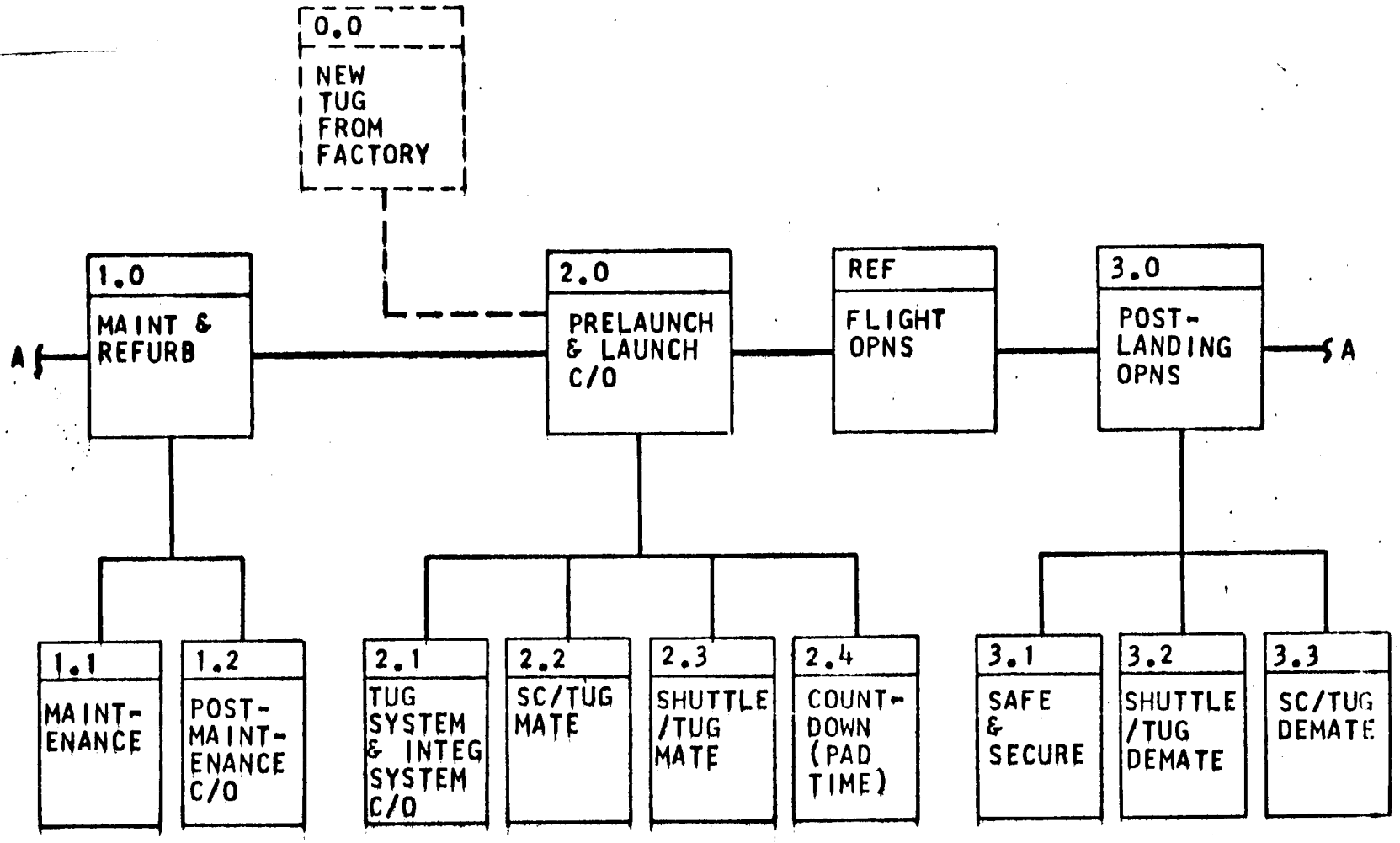
SYSTEM: Main Engine Support

DATE: 08-01-73

PAGE: II-1

SUBSYSTEM/ COMPONENT	TRANSPORTATION & HANDLING	PREFLIGHT OPERATIONS	LAUNCH OPERATIONS	ORBITER FLIGHT	TUG DEPLOYMENT/ RETRIEVAL	TUG FREE FLIGHT	PAYLOAD DEPLOYMENT/ RETRIEVAL	POST FLIGHT OPERATIONS	ABORT	OTHER ANALYSES		
										FMEA	OPERATIONS & MAINTENANCE	DESIGN CHECK LIST
1. Pressurization												
1.1 He Sphere												
1.2 He Solenoid Valve												
1.3 He Regulator												
1.4 He Check Valve												
1.5 Burst/Relief Valve												
1.6 Lines & Fittings												
2. Propellant Feed												
2.1 Propellant Valves												
2.2 Lines & Fittings												

FUNCTIONAL FLOW OUTLINE



MARTIN MARIETTA

TEST INFORMATION SHEET

FUNCTION NO. _____

TITLE: _____

OBJECTIVE: _____

_____

FREQUENCY: _____ SAFETY: HAZARDOUS _____, NON-HAZARDOUS _____

TIME REQ'D TO COMPLETE: _____ HRS. PERSONNEL & SKILL REQM'TS: _____

SOFTWARE REQUIREMENTS: _____

_____

LPS REQUIREMENTS: _____

_____

GSE REQUIREMENTS: _____

_____

_____

FACILITY REQUIREMENTS: _____

MARTIN MARIETTA

26

OPERATION & MAINTENANCE HAZARD SUMMARY

	ITEM	HAZARD	CRITICALITY	REQUIREMENT
21	*2.1.4.5 - Kick Stage weight and CG verification	See Items 1 and 17	Catastrophic	See Items 1 & 17 Define Kick Stage handling & hoisting plan
22	*2.2.1.1 - Mate Tug with spacecraft	Structural damage to stage or spacecraft from mismanagement of two cranes. Excessive acceleration and shock loads	Critical	Define two crane plan Define acceleration and shock level limits
23	*2.2.1.5 - Install payload in cradle on servicing trailer	Structural damage to payload during hoisting operations & transporting. Excessive acceleration and shock levels	Critical	Define payload handling plan and payload transportation plan Define acceleration and shock levels
24	*2.2.1.6 - Move payload to propellant loading area	Structural damage to payload during transportation. Excessive acceleration and shock levels	Critical	See item 23.
25	*2.2.1.8 - Rotate payload to vertical	Structural damage to payload from mismanagement of crane	Critical	Define payload rotation plan
26	*2.2.1.9 - Load N_2O_4 & secure	Personnel exposure to propellants during loading operation	Critical	Define propelland handling & loading plan Define leak check plan
27	*2.2.1.10 - Load ACS & secure	See Item 26	Critical	See Item 26
28	*2.2.1.11 - Load MMH & secure	See Item 26	Critical	See Item 26
29	*2.2.1.12 - Load Pressurants & secure	See Item 26	Critical	See Item 26 & define pressurization plan.
30	*2.2.1.13 - Rotate payload to horizontal	See Item 25 and propellant tank failure	Catastrophic	See Item 25

*Indicates a normal operations function.

SYSTEM SAFETY CHECKLIST

ITEM NUMBER	SUBSYSTEM: Composite HARDWARE DESCRIPTION: Space Tug Systems Study DATE: 8/2/73 — COMPLETED BY: (NAME) Summary	DESIGN COMPLIES	DESIGN DOES NOT COMPLY	DETAIL DESIGN WILL COMPLY	DETAIL DESIGN WILL NOT COMPLY	NOT APPLICABLE
	B. FUEL/PROPELLANT SYSTEMS					
62	N_2O_4 is inhibited with NO to prevent corrosion of titanium.	X				
63	Limit Fuel and Propellant pressure rise to 10% over normal pressure.		X		X	
64	Provide that tank pressure will be relieved before structural limits are exceeded.	X				
65	Provide overpressure relief where fluid lines or components may be exposed to fire.		X		X	
66	Provide underpressure relief during defueling operations or during reentry.	X				

HAZARD CLASS	Catastrophic
STATUS	Open
PROGRAM PHASE	System Study

NO.	1.004
PAGE	1 of 1
DATE	08-04-73

SYSTEM: Propulsion, General SUBSYSTEM: N/A

OPERATION/PHASE: Transportation and Handling

HAZARD GROUP: 8 - Fire/Explosion/Implosion

REFERENCES: AFM 127-100, Explosives Safety Manual

HAZARD DESCRIPTION: Mishandling of the Space Tug after propellants are loaded presents a fire/explosion hazard if shock loads would cause the tanks to rupture.

POTENTIAL EFFECTS:

1. Loss of life, the Space Tug, Orbiter and equipment in the vicinity.
2. Extensive damage to facilities.

ASSUMPTIONS/RATIONALE:

1. Mass mixing of the hypergolic propellants would create a low grade explosion or fire ball.
2. Explosive Quantity - Distance criteria may be determined from AFM 127-100 as follows:

   60,000 lbs of propellant x 10% (for N_2O_4 and MMH) = 6000-lb equivalent high explosive.

   Required separation distance (from Table 5-10) = 730 feet.

MARTIN MARIETTA

REQUIREMENTS:	REFERENCE
A. Design	
1. Lifting and handling equipment shall be fail-safe.	
2. No single malfunction shall result in loss of control of lifted load.	
3. Design factors of safety for lifting and handling equipment shall be a minimum of 5.0 (ultimate).	
B. Operations	
1. Hoisting equipment shall be proof tested to 2.0 times load at least annually.	
2. Establish Danger Area of 730 ft radius around Space Tug during any movement after propellants are loaded.	
3. Non-essential personnel shall be evacuated from established Danger Area.	
4. Establish safe transportation routes for moving loaded Space Tug.	

DISPOSITION:

1. Entered in Hazards Catalog.

ORIGINATOR/LOCATION: W. R. O'Halloran, Ext. 4203

ANALYSIS OUTPUT

- HAZARD REDUCTION
- DESIGN AND OPERATIONS REQUIREMENTS
- HAZARD CATALOG
  - PART I - HAZARDS LIST
  - PART II- RESIDUAL HAZARDS

MARTIN MARIETTA

HAZARD CATALOG

PART I - HAZARDS LIST

SECTION: I - Propulsion, General

PAGE: 1

32

HAZARD NO.	HAZARD	ELIMINATED	RESIDUAL	HAZARD LEVEL	ACCEPTED	OPEN
1.001	Highly toxic, corrosive oxidizer, N_2O_4		1.1	Crit.		X
1.002	Highly toxic, flammable/explosive fuel, MMH		1.2	Crit.		X
1.003	Propellant tank ullage overpressure	X				
1.004	Fire/Explosion from both tanks rupture		1.3	Cat.		X

HAZARDS CATALOG
PART II - RESIDUAL HAZARDS

SYSTEM: Propulsion	ITEM NO. 1.3
SUBSYSTEM: Propellant Tanks	HAZARD CLASS Catastrophic
COMPONENT: N/A	DATE 08-4-73

HAZARD DESCRIPTION:

Mishandling of the Space Tug after propellants are loaded presents a fire/explosion hazard if shock loads would cause the tanks to rupture. A low grade explosion or fire ball would occur with possible loss of life and/or flight hardware and extensive damage to facilities.

RECOMMENDATION: hazard controlled

1. Establish and enforce rigid criteria/requirements for the design and operation of lifting and handling equipment.

2. The hazard will remain open until detail design and operating procedures meet requirements and adequate Danger Areas have been established.

DISPOSITION:

ANALYSIS STATUS

HAZARD IDENTIFICATION	
● INHERENT HAZARDS	IN PROCESS
● FMEA	1ST ITERATION COMPLETE
● OPERATIONS & MAINTENANCE	1ST ITERATION COMPLETE
● SYSTEM SAFETY CHECKLIST	1ST ITERATION COMPLETE
DETAILED HAZARD ANALYSIS	IN PROCESS

MARTIN MARIETTA

SINGLE POINT FAILURE SUMMARY

SUBSYSTEM	CATEGORY I* SFP'S	CATEGORY II SFP'S
GUIDANCE & NAVIGATION, ALL CONFIGURATIONS	0	2
SOLAR ARRAY POWER 1 AV-1, -2, -3, -4	0	2
CONTROLS, ALL CONFIGURATIONS	0	2
COMMUNICATIONS, ALL CONFIGURATIONS	0	0
FUEL CELL POWER, AV-7, AV-8	2	5
DATA MANAGEMENT, ALL CONFIGURATION	0	0
OME ENGINE (OR HIGH P_C ENGINE)	1	2
ATTITUDE CONTROL SYSTEM, ACPS-2 (8)	2	0
MAIN ENGINE SUPPORT, PR-1 (2)	3	12
MAIN ENGINE SUPPORT, PR-1 (4)	6	24
MAIN ENGINE SUPPORT, PR-1 (5)	6	26
MAIN ENGINE SUPPORT, PR-1 (6)	4	15
DOCKING, AV-2, -4, -7	0	2
ORBITER INTERFACE, ALL CONFIGURATIONS	0	4
KICK STAGE, ALL CONFIGURATIONS USING KICK STAGES	2	4

* NOTE: ALL CATEGORY I SFP'S ARE HIGH ENERGY STORAGE DEVICES.

MARTIN MARIETTA

OPERATIONS & MAINTENANCE HAZARD SUMMARY

HAZARD	HAZARD LEVEL	HAZARDOUS FUNCTIONS NORMAL	HAZARDOUS FUNCTIONS ALTERNATE
ENERGY SOURCE (KICK STAGE)	CATASTROPIC	5	0
ENERGY SOURCE (ORDNANCE)	CATASTROPHIC	6	8
FIRE/EXPLOSION (PROPELLANTS LOADED)	CATASTROPHIC	5	5
ACCELERATION/SHOCK (HANDLING)	CRITICAL	18	11
FIRE (ENGINE CLEANING)	CRITICAL	0	1
TOXICITY (PROPELLANT HANDLING)	CRITICAL	10	3

SYSTEM SAFETY CHECKLIST SUMMARY

CHECKLIST	TOTAL ITEMS	DESIGN COMPLIES	DESIGN DOES NOT COMPLY	DETAIL DESIGN WILL COMPLY	DETAIL DESIGN WILL NOT COMPLY	NOT APPLICABLE
TUG DATA PACKAGE REQUIREMENTS	39	25	7	7	4	0
STRUCTURAL SYSTEMS	14	4	1	7	0	2
FUEL/PROPELLANT SYSTEMS	38	22	10	5	10	0
LIQUIDS AND GASES	18	9	0	9	0	0
ELECTRICAL/ELECTRONIC	61	22	7	31	3	1
SOLID ROCKET MOTORS	9	9	0	0	0	0
CAUTION AND WARNING	8	3	2	0	0	3
CRYOGENIC SYSTEMS	12	1	0	11	0	0

MARTIN MARIETTA

OPERATIONAL SAFETY CHECKLIST

CHECKLIST	TOTAL ITEMS	DO ACCO-MODATE	DON'T ACCO-MODATE	DETAIL WILL COMPLY	DETAIL WON'T COMPLY	NOT APPLICABLE
GENERAL	11	4	2	4	0	1
HAZARDOUS FLUIDS/MATERIALS	11	2	1	8	0	0
FLIGHT OPERATIONS	7	6	1	0	0	0

MARTIN MARIETTA

ANALYSIS METHODOLOGY

- SYSTEMATIC
- COMPREHENSIVE

ANALYSIS STATUS

- HAZARD IDENTIFICATION
- HAZARD ANALYSIS

ANALYSIS OUTPUT

- MATRIX BY SUBSYSTEM CONFIGURATION
- ANALYSIS BY SYSTEM
- HAZARD CATALOG BY SYSTEM

TECHNICAL MEMORANDUM

TM-29675-SY-09

Revision 1

SPACE TUG (STORABLE) STUDY

SYSTEMS SAFETY PLAN

1 August 1973

D. Whiteside
Q. Eberhardt
W. O'Halloran

40

1.0 PURPOSE

The purpose of this plan is to identify those System Safety tasks that will be performed for the Space Tug System Study (Storable).

1.1 Scope - This plan describes the System Safety activities to be performed during the Space Tug System Study and shall terminate at the end of the study phase.

1.2 Objective - The objective of this plan is to emphasize the importance of safety in the conceptual design that effects ground and flight operations of a Space Tug using storable propellants. The tug safety must be compatible with the manned Orbiter operations concept.

1.3 Applicable Documents - The applicable documents are to be used as reference material only for the study phase or as prescribed herein.

a. NHB 5300.4 (1D), Safety, Reliability, Maintainability and Quality Provisions for Space Shuttle Program.

b. Data Package, Space Tug System Studies.

c. KMI 1710.1B, The KSC Safety Program.

d. AFETR 127-1, Volume I, Range Safety Manual.

2.0 SYSTEM SAFETY APPROACH

Concern for a low cost, high performance Space Tug configuration requires that each potentially hazardous situation be identified. Once the identifications are established, each hazardous situation must be assessed to determine the most cost effective approach to maintain an acceptable level of safety risk. In performing this study, Martin Marietta will:

a. Evaluate each hazardous situation to determine the feasibility for elimination of each situation by design and remain within program and mission constraints.

b. Determine the added margins of control provided by the selection of safety devices or performing margin of safety testing to reduce or control the hazard.

c. Assess the advantages related to crew caution and warning systems as a function of reducing or controlling the hazards.

d. Identify the hazardous situations that can be satisfactorily controlled by procedures.

These objectives will be accomplished within the context of a Phase A study and are commensurate with Section V (Space Tug System Safety Criteria) of the Data Package, dated April 1973.

2.1 Develop Program Safety Plan for Implementation - Martin Marietta will develop a System Safety Plan as an in-house document to be used by the Study Manager to track the safety effort. This method ensures that those safety concerns that are drivers in the design selection are not overlooked. It also serves as a management tool to maintain the safety effort requirements within the perimeters of a Phase A study.

2.2 Identify Hazard Groupings - Hazard groups will be identified; i.e., Acceleration/Shock, Electrical, Pressure, Fire/Explosion/Implosion, etc., to assist the designers in system and subsystem selection and as a basis for hazard identification. (See attachment 1.)

2.3 Review and Update System Safety Criteria - The System Safety criteria contained in the Data Package will be used to eliminate potentially catastrophic hazards in the design concepts to be recommended as Tug Options. Rationale will be developed for accepting risks as well as baselining additional System Safety criteria for Tug/Orbiter interfaces and interactions as required by the data package.

2.4 Trade Studies - Safety will be a major consideration in all configuration trade studies. Results of trade studies will indicate that the selected concept includes the optimum safety provisions consistent with other program considerations.

2.5 System Safety Analysis - The System Safety Analysis shall be qualitative and in sufficient detail to identify all catastrophic and critical hazards. The analysis consists of an iterative process of hazard identification and detailed analysis as described below.

2.5.1 Hazard Identification - A potential hazard matrix will be developed for each configuration to provide a means to systematically identify all hazards. All operational phases from prelaunch through Shuttle touchdown and recycle will be

examined to identify potential or inherent hazards. Hazards identified from other analyses, such as Failure Modes and Effects Analysis (FMEA), Operations and Maintenance Analysis, and Subsystem Safety Check Lists, will also be included in the potential hazard matrix. (See Attachment 2 for Potential Hazard Matrix format.)

2.5.1.1 FMEA - FMEA will be the source of identification of hazards due to hareware failure and Single Failure Points (SFP) Categories I and II will be included in the potential hazard matrix.

2.5.1.2 Safety Checklist - System Safety Checklists will be developed from the Data Package safety requirements and existing checklists such as Skylab System Safety Checklists and AFSC Design Handbook DH1-6. The checklists will be completed by the design areas and each case of non-compliance will be included in the potential hazard matrix.

2.5.1.3 Operations and Maintenance Analysis - Hazardous operations will be identified as a part of the operations and maintenance analysis of compliance with the requirements of KMI 1710.1B/SF. Operations identified as being hazardous will be included in the Potential Hazard Matrix.

2.5.2 Hazard Analysis - The detailed analysis of identified hazards will be accomplished and documented utilizing the Hazard Analysis format provided in Attachment 3. Analysis data will include all pertinent facts or assumptions used as the basis of analysis, calculations, reference data, and analysis performed to develop the rationale for classification of the hazard and disposition actions. The analysis will also develop design and operational requirements to eliminate/control the hazard.

Each hazard will be classified, considering incorporated safety features, in accordance with the following hazard levels:

a. Catastrophic - No time or means are available for corrective action.

b. Critical - May be counteracted by emergency action performed in a timely manner.

c. Controlled - Has been counteracted by appropriate design, safety devices, alarm/caution and warning devices, or special automatic/manual procedures.

All residual hazards classified as catastrophic or critical shall be reported as a part of the study in a summary Hazard Catalog. (See Attachment 4 for format.)

2.6 Hazard Reduction - The following sequence, or combination of sequences, will be used to eliminate or control identified hazards:

- Design for Minimum Hazards - During all phases of design, primary consideration is given to minimize hazards through the selection of appropriate design features and qualified components and materials. System Safety requirements, standards and margins are included in specifications and requirements for parts, subsystems and systems.

- Safety Devices - Hazards which cannot be eliminated through design selection shall be reduced to an acceptable level through the use of appropriate safety devices as a part of the subsystem, system or component.

- Warning Devices - Where it is not possible to preclude the existence of a known hazard, devices shall be assessed for the timely detection and adequate warning of the hazardous condition. Warning signals and their application shall be designed to minimize the possibility of improper signals or improper personnel reaction to the signals.

- 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, the need for special procedures shall be assessed to counter and control hazardous conditions.

3.0 SAFETY OUTPUTS

The safety effort will be an influencing factor in design and operations planning throughout the study. Each of the Tug options defined in Task 5 of the study will include a safety analysis to include identification and evaluation of hazards, definition of System Safety Design criteria, definition of operations Safety Requirements, and identification of Mission Safety Requirements.

Attachment 1

HAZARD GROUPS

No.	Hazard	
1	Acceleration/Shock	Change in velocity, applied force, impact
2	Configuration	Component location, system deficiencies
3	Contamination	Producing or introducing contaminants
4	Corrosion	Damage to material surfaces
5	Electrical	Shock, thermal, inadvertent activation
6	Energy sources	Propellants, batteries, ordnance devices
7	Environment	Natural, induced, pollution
8	Fire/Explosion/Implosion	Chemical reactions, heat generation, over/under pressure
9	Man-machine relations	Controls, displays, human error
10	Pressure	High, low, or variation
11	Radiation	Electromagnetic, ionizing
12	Structural	Degradation, failure
13	System Interactions	Compatibility between interfacing systems/GSE
14	Temperature	High, low, or variation
15	Toxicity	Adverse human effects

POTENTIAL HAZARD MATRIX

CONFIGURATION:

SYSTEM:

DATE:

PAGE:

SUBSYSTEM/ COMPONENT	TRANSPORTATION & HANDLING	PREFLIGHT OPERATIONS	LAUNCH OPERATIONS	ORBITER FLIGHT	TUG DEPLOYMENT/ RETRIEVAL	TUG FREE FLIGHT	PAYLOAD DEPLOYMENT/ RETRIEVAL	POST FLIGHT OPERATIONS	ABORT	OTHER ANALYSES		
										FMEA	OPERATIONS & MAINTENANCE	DESIGN CHECK LIST
List subsystem and components as identified by design			Identify Hazard Group and Relate to Hazard Analysis							Identify Source of Hazard Identification		

Attachment 3
HAZARD ANALYSIS

HAZARD CLASS	
STATUS	
PROGRAM PHASE	

NO.	
PAGE	
DATE	

SYSTEM: SUBSYSTEM:

OPERATION/PHASE:

HAZARD GROUP:

REFERENCES:

HAZARD DESCRIPTION:

POTENTIAL EFFECTS:

ASSUMPTIONS/RATIONALE:

REQUIREMENTS:	REFERENCE

DISPOSITION:

ORIGINATOR/LOCATION:

Attachment 4

HAZARD CATALOG

PART I - HAZARDS LIST

SECTION:

PAGE:

HAZARD NO.	HAZARD	ELIMINATED	RESIDUAL	HAZARD LEVEL	ACCEPTED	OPEN

Attachment 4 (cont)

HAZARDS CATALOG
PART II - RESIDUAL HAZARDS

SYSTEM:	ITEM NO.
SUBSYSTEM:	HAZARD CLASS
COMPONENT:	DATE

HAZARD DESCRIPTION:

RECOMMENDATION:

DISPOSITION:

OPERATION & MAINTENANCE HAZARD SUMMARY

ITEM	HAZARD	CRITICALITY	REQUIREMENT
	PREPARATION EXPLANATION		
List function number and title from Launch Site Ground Operations Flow Diagram. Major categories are: 0. Initial Launch Site Receipt 1. Maintenance & Refurbish 1.1 Maintenance 1.2 Post-Maintenance Checkout 2. Prelaunch & Launch 2.1 System & Integrated System Checkout 2.2 Spacecraft/Tug Mate & Propellant Loading 2.3 Shuttle/Tug Mate 2.4 Countdown (Pad Operations) 3.0 Post Landing Ops. 3.1 Safe & Secure 3.2 Shuttle/Payload Demate 3.3 Spacecraft/Tug Demate	Hazard Description	Most severe (worst case) hazard level per NHB 5300.4 (ID)	List items required to control hazard.

*Indicates a normal operations function.

OPERATION & MAINTENANCE HAZARD SUMMARY

	ITEM	HAZARD	CRITICALITY	REQUIREMENT
1	0.1 - Tug unload from aircraft	Structural damage to Tug/Spacecraft from handling and/or movement operations	Critical	Define Tug removal operations from Orbiter
2	0.3 - Move to PPF(WTR) or MCF (KSC)	Structural damage to Tug/Spacecraft during transportation operations.	Critical	Define acceleration & shock limits. Define transportation plan & environments.
3	0.4 - Install Tug in C/O fixture	Structural damage to Tug during hoisting operation	Critical	Define handling and installation plan
4	0.5 - Engine nozzle installation	Structural damage to nozzle during hoisting operation	Critical	Define hoisting, installation plan and nozzle torque requirements.
5	*0.14 - Unload Kick Stage Motor	Structural damage to Kick Stage Motor during unloading operation	Critical	Define Kick Stage unloading plan.
6	*0.15 - Move to PPF (WTR) or MCF (KSC)	Structural damage to Kick Stage Motor	Critical	Define transportation plan and environments Define acceleration and shock levels.
7	*0.16 - Receive & inspect components	Structural damage to Kick Stage Motor and components	Critical	Define receiving, inspection and handling plan
8	*1.1.1 - Move Tug to PPF (WTR) or MCF (KSC)	Structural damage to Tug from hoisting and lifting operations and transporting of Tug	Critical	Define Tug handling plan, transportation plan & environments, define accel. & shock levels.
9	1.1.1.1 - Return Tug to repair depot if required	See Item 8	Critical	See Item 8
10	*1.1.2 - Install Tug in C/O Fixture	See Item 3	Critical	See Item 3
11	1.1.12 - Engine cleaning/ teardown	1. Fire 2. Material degradation	Critical	Define engine purge plan

*Indicates a normal operations function.

OPERATION & MAINTENANCE HAZARD SUMMARY

	ITEM	HAZARD	CRITICALITY	REQUIREMENT
12	2.1.3.1 - Move Tug to PPF (WTR) or MCF (KSC) & install in test fixture	See Items 2 and 3	Critical	See Items 2 & 3
13	*2.13.2 - Mission configure Tug	Similar to Item 1 - See Item 1	Critical	See Item 1
14	*2.1.3.6 - Weight and CG verification	Similar to Item 1 - See Item 1	Critical	See Item 1
15	2.1.3.7 - Ship to WTR	Excess structural loading from dynamic loads	Critical	Define acceleration/ shock levels/limits Define transporter configuration Define transportation plan & environments
16	*2.1.4 - Assemble Kick Stage in Assembly Fixture	See Item 5	Critical	See Item 5
17	*2.1.4.1 - Kick Stage Pwr System Activation & Checkout	Kick Stage explosive potential	Catastrophic	Define Kick Stage checkout & verification plan Define ordnance safing plan
18	*2.1.4.2 - Kick Stage Motor & Ignition Sys checkout	See Item 17	Catastrophic	Same as Item 17
19	*2.1.4.3 - Kick Stage avionics systems check-out	See Item 17	Catastrophic	Same as Item 17
20	*2.1.4.4 - Kick Stage combined systems test	See Item 17	Catastrophic	Define Kick Stage avionics checkout and See Item 17, and Define Kick Stage CST

*Indicates a normal operations function.

OPERATION & MAINTENANCE HAZARD SUMMARY

	ITEM	HAZARD	CRITICALITY	REQUIREMENT
21	*2.1.4.5 - Kick Stage weight and CG verification	See Items 1 and 17	Catastrophic	See Items 1 & 17 Define Kick Stage handling & hoisting plan
22	*2.2.1.1 - Mate Tug with spacecraft	Structural damage to stage or spacecraft from mismanagement of two cranes. Excessive acceleration and shock loads	Critical	Define two crane plan Define acceleration and shock level limits
23	*2.2.1.5 - Install payload in cradle on servicing trailer	Structural damage to payload during hoisting operations & transporting. Excessive acceleration and shock levels	Critical	Define payload handling plan and payload transportation plan Define acceleration and shock levels
24	*2.2.1.6 - Move payload to propellant loading area	Structural damage to payload during transportation. Excessive acceleration and shock levels	Critical	See Item 23
25	*2.2.1.8 - Rotate payload to vertical	Structural damage to payload from mismanagement of crane	Critical	Define payload rotation plan
26	*2.2.1.9 - Load N_2O_4 & secure	Personnel exposure to propellants during loading operation	Critical	Define propellant handling & loading plan Define leak check plan
27	*2.2.1.10 - Load ACS & secure	See Item 26	Critical	See Item 26
28	*2.2.1.11 - Load MMH & secure	See Item 26	Critical	See Item 26
29	*2.2.1.12 - Load Pressurants & secure	See Item 26	Critical	See Item 26 & define pressurization plan
30	*2.2.1.13 - Rotate payload to horizontal	See Item 25 and propellant tank failure	Catastrophic	See Item 25

*Indicates a normal operations function.

OPERATION & MAINTENANCE HAZARD SUMMARY

	ITEM	HAZARD	CRITICALITY	REQUIREMENT
31	2.2.1.14 - Move Tug to orbiter MCF or Integration/Mate facility	Excessive structural loading from dynamic loads & acceleration/shock cushioned transporter (propellant tank failure)	Catastrophic	Define acceleration load limits Define shock limit level Define transportation plan & environment Define transporter & total payload support
32	*2.2.2.2 - Install Tug in cradle on servicing trailer	See Item 23	Critical	Similar to Item 23 Define Tug handling plan
33	*2.2.2.3 - Move Tug to PPF (WTR) or MCF (KSC)	See Item 31	Catastrophic	See Item 31.
34	*2.2.3.1 - Mate Tug w/Kick Stage & interface verification	Structural damage to Tug, Kick Stage and/or spacecraft from mismanagement of two cranes, excessive acceleration and shock loads (propellant tank failure)	Catastrophic	Define Tug/Kick Stage mating plan Define two crane concept and plan Define acceleration and shock level limits
35	*2.2.4 - Load Kick Stage RCS propellant	See Item 26	Critical	See Item 26
36	*2.3.1 - Move Payload to Orbiter MCF	See Item 31	Catastrophic	See Item 31
37	*2.3.2 - Install, verify and safe ordnance hardware	Total Tug/Payload loss due to explosion caused by static electricity, EMC and/or sparks	Catastrophic	Define ordnance installation safing and verification plan

*Indicates a normal operations function.

OPERATION & MAINTENANCE HAZARD SUMMARY

	ITEM	HAZARD	CRITICALITY	REQUIREMENT
38	*2.3.3.1 - Mate payload with orbiter	1. Structural damage to Tug or payload from mismanagement of crane (Propellant Tank Failure)	Catastrophic	Define crane concept/ operation Define acceleration load limits Provide loading guides and snubbers
		2. Payload impact to Orbiter from crane mismanagement	Critical	
39	*2.3.3.2 - Payload-Orbiter I/F verification	See Item 37	Catastrophic	See Item 37
40	*2.3.3.3 - Prepare systems for IS_T	See Item 37	Catastrophic	See Item 37
41	*2.3.3.4 - Payload/ Orbiter I.S.T.	See Item 37	Catastrophic	See Item 37 Define I.S.T. procedures
42	2.3.3.4.1 - Payload/ Orbiter EMC tests.	See Item 37	Catastrophic	See Item 37 and define EMC test
43	2.3.4.1 - Mate Tug with Orbiter	See Item 38	1. Catastrophic 2. Critical	See Item 38
44	2.3.4.2 - Tug/Orbiter I/F verification	See Item 37	Catastrophic	See Item 37
45	2.3.4.3 - Prepare systems for I.S.T.	See Item 37	Catastrophic	See Item 37
46	2.3.4.4 - Tug/Orbiter integrated systems test	See Item 37	Catastrophic	See Item 37
47	2.3.4.4.1 - Tug/Orbiter EMC testing	See Item 37	Catastrophic	See Item 37 & 42

*Indicates a normal operations function.

OPERATION & MAINTENANCE HAZARD SUMMARY

	ITEM	HAZARD	CRITICALITY	REQUIREMENT
48	2.3.7.2 - Mate Orbiter/ launcher with Tug or P/L	1. Excessive structural loading from dynamic loads and hoist system resulting in structural failure - Excessive acceleration loads. (Propellant tank failure)	Catastrophic	Define crane operations Define acceleration load limits Provide GSE for total support.
		2. Payload impact to Orbiter from mismanagement of mating operations	Critical	Define Mating operation
49	2.3.7.3 - Tug/PL - Orbiter I/F verification	See Item 37	Catastrophic	See Item 37
50	*2.3.8 - Shuttle integrated systems test	See Item 37	Catastrophic	See Item 37
51	2.4.2.3 - Mate payload to Orbiter and verify interface	See Item 22 and 34	Catastrophic	See Item 22 & 34 and define payload/ Orbiter mating plan
52	2.4.2.4 - Payload/ Orbiter integrated systems test	See Item 37	Catastrophic	See Items 37 and 41
53	2.4.3 - Hold - Backout recycle procedure SAFE Shuttle	Similar to Item 48 - See Item 48	1. Catastrophic 2. Critical	See Item 48 & define hold - backout - recycle procedures.
54	*3.1.1.5 - Drain & purge Tug fuel tank	Personnel safety during drain & purge operations	Critical	Define Drain & Purge Procedures
55	*3.1.1.6 - Drain & purge RCS tanks	See Item 54	Critical	See Item 54
56	*3.1.1.7 - Drain & purge Tug or tank	See Item 54	Critical	See Item 54
57	*3.1.1.8 - Vent remaining Tug pressurants	Personnel safety during venting operations	Critical	Define venting procedures

*Indicates a normal operations function.

OPERATION & MAINTENANCE HAZARD SUMMARY

	ITEM	HAZARD	CRITICALITY	REQUIREMENT
58	3.1.2.3 - Safe Orbiter/ payload ordance not expended	Ordnance explosive potential	Catastrophic	Define ordnance safing procedures and operations
59	3.1.3.1 - Move Tug to propellant loading facility	See Item 24	Critical	See Item 24
60	3.1.3.2 - Unload MMH & purge	See Item 54	Critical	See Item 54
61	3.1.3.3 - Unload ACS & purge	See Item 54	Critical	See Item 54
62	3.1.3.4 - Unload N_2O_4 & purge	See Item 54	Critical	See Item 54
63	*3.1.4.1 - Tug Ordnance Removal	See Item 58	Catastrophic	See Item 58 and define ordnance hardware removal plan
64	*3.1.4.2 - Tug Engine removal	Structural damage to engine due to crane mishandling	Critical	Define hoisting & movement plan
65	*3.1.5 - Decontaminate Tug propellant system	Personnel safety	Critical	Define decontamination plan
66	*3.2.1 - Remove payload from Orbiter	Structural damage to payload during removal. Excessive acceleration and shock loads	Critical	Define payload removal plan Define acceleration & shock level limits
67	*3.3.1 - Install payload on service trailer	See Item 23	Critical	See Item 23
68	*3.3.2 - Separate Tug from spacecraft	Structural damage to spacecraft due to crane mishandling. Excessive acceleration & shock loads	Critical	Define hoisting plan Define acceleration & shock level limits

*Indicates a normal operations function.

SYSTEM SAFETY CHECKLIST

The attached checklist presents the composite results of lists completed individually by:

J. Hurley - Main Engine Support

J. Hurley - Engines

J. Hurley - Attitude Control Propulsion System

M. Imamura - Electrical Power Subsystem

A. Brook - Guidance & Navigation

R. Sheppard - Data Management

R. Sheppard - Communications

J. Parham - Structures

M. Murphy - Kick Stage SRMs

NOTE: When any subsystem response indicated design does not comply and/or detail design will not comply, only those responses are shown for emphasis.

SYSTEM SAFETY CHECKLIST

ITEM NUMBER	SUBSYSTEM: Composite HARDWARE DESCRIPTION: Space Tug Systems Study DATE: 8/2/73 — COMPLETED BY: (NAME) Summary	DESIGN COMPLIES	DESIGN DOES NOT COMPLY	DETAIL DESIGN WILL COMPLY	DETAIL DESIGN WILL NOT COMPLY	NOT APPLICABLE
	STORABLE TUG DATA PACKAGE SAFETY REQUIREMENTS					
	A. GENERAL					
1	a. No single failure shall result in a hazard which jeopardizes the flight or ground crews.	X				
2	b. Appropriate safety factors are used where necessary to minimize the possibility of failures which might affect manned safety (i.e., structures, pressure vessels, etc.).	X				
3	c. Manned factors of safety are maintained under abort load conditions.	X				
4	d. The Tug design is capable of providing to the Orbiter such information concerning the status or condition of the Tug as is necessary to insure safety of the Orbiter and crew during stowage, deployment and retrieval.	X				
5	e. Provision for command override of critical Tug functions by the Orbiter crew is provided during stowage, deployment and retrieval operations.	X				
6	f. The subsystem design has self-contained protective devices or provisions against generating hazards while mounted to the Orbiter.	X				
7	g. Provisions are provided for emergency manual release of Tug to Orbiter connections.		X			
	1. Normal Operations					
	a. Stowage in Orbiter					
8	1) Destruct charges are not incorporated in the design.	X				
9	2) A pressure relief capability is provided for the Tug tanks which automatically limits the maximum pressure. Venting is through the Tug/Orbiter interface.		X		X	
10	3) Toxic or other chemically hazardous gases, liquids or particles are not vented into the Orbiter payload compartment and are isolated from the Orbiter ECS System.	X				

SYSTEM SAFETY CHECKLIST

SUBSYSTEM: Composite

HARDWARE DESCRIPTION: Space Tug Systems Study

DATE: 8/2/73

COMPLETED BY: (NAME) Summary

ITEM NUMBER		DESIGN COMPLIES	DESIGN DOES NOT COMPLY	DETAIL DESIGN WILL COMPLY	DETAIL DESIGN WILL NOT COMPLY	NOT APPLICABLE
	STORABLE TUG DATA PACKAGE SAFETY REQUIREMENTS					
	1. Normal Operations (Continued)					
	b. On-Orbit Deployment					
11	1) No single failure of this subsystem shall result in unprogrammed motion of the Tug.		X			
	c. On-Orbit - General					
12	1) Provision is provided for control of all critical Tug functions, including attitude and translational position control by Orbiter crew during post-deployment and pre-retrieval operations.	X				
13	2) All venting of the Tug while within the vicinity of the Orbiter is non-propulsive.	X				
14	3) No single failure of this subsystem shall result in unprogrammed motion of the Tug, while within the vicinity of the Orbiter.		X			
	d. On-Orbit - Retrieval					
15	1) Provisions are provided for Orbiter control of critical Tug functions while the retrieval mechanism is attached.	X				
16	2) No single failure of this subsystem shall result in unprogrammed motion of the Tug.	X				
17	3) Provisions for static discharge are provided.			X		
18	4) Tug propellants and pressurants are reduced to a predetermined safe level prior to Tug retrieval.		X		X	
19	5) Provisions are made to confirm that all Orbiter/Tug interfaces are securely connected.		X		X	
20	6) Provisions are provided for remote emergency jettisoning of Tug deployable equipment as necessary to complete retrieval and stowage operations.		X		X	

SYSTEM SAFETY CHECKLIST

SUBSYSTEM: Composite

HARDWARE DESCRIPTION: Space Tug Systems Study

DATE: 8/2/73

COMPLETED BY: (NAME) Summary

ITEM NUMBER		DESIGN COMPLIES	DESIGN DOES NOT COMPLY	DETAIL DESIGN WILL COMPLY	DETAIL DESIGN WILL NOT COMPLY	NOT APPLICABLE
	STORABLE TUG DATA PACKAGE SAFETY REQUIREMENTS					
	3. Abort					
21	a. The subsystem design does not preclude the Shuttle from intact abort.	X				
	B. SUBSYSTEMS CRITERIA					
	1. Structures					
22	a. Factors of safety for Tug pressure vessels, tanks and general structures are in accordance with MSFC-HDBK-505, "Structural Strength Design & Verification Program Requirements".			X		
23	b. Pressure vessels and tanks are designed to, and maintained under, a fracture mechanics control program.			X		
	2. Propulsion					
24	a. The propulsion system is designed to be fail-safe.	X				
25	b. Relief capability to automatically limit maximum pressure is provided for pressurized propellant tanks.	X				
26	c. Provision is provided to detect potential tank failures.	X				
27	d. Propellant isolation valves are provided upstream from all start valves.	X				
28	e. Provisions are made to permit emergency off-loading of Tug propellants while the Tug is stowed in the Orbiter cargo bay on the launch pad.	X				
	3. Auxiliary Propulsion					
29	a. The APS is designed to be fail-operational/fail safe.	X				
30	b. The APS is capable of being shut down by one command from the Orbiter.	X				

SYSTEM SAFETY CHECKLIST

SUBSYSTEM: Composite

HARDWARE DESCRIPTION: Space Tug Systems Study

DATE: 8/2/73

COMPLETED BY: (NAME) Summary

ITEM NUMBER		DESIGN COMPLIES	DESIGN DOES NOT COMPLY	DETAIL DESIGN WILL COMPLY	DETAIL DESIGN WILL NOT COMPLY	NOT APPLICABLE
	STORABLE TUG DATA PACKAGE SAFETY REQUIREMENTS					
	4. Avionics					
31	a. RF communication capability is available between the Orbiter and the Tug and payload for command and control functions.	X				
32	b. The critical command and control circuitry is designed to be fail-operational/fail-safe.	X				
33	c. The design of the Tug control system shall only allow supply of electrical energy to the start valves of the rocket engines following positive action by the Orbiter crew during Tug countdown in orbit.	X				
34	d. The design of the Tug control system shall only allow supply of electrical energy to the separation mechanism following positive action by the Orbiter crew during Tug countdown in orbit.	X				
	5. Ordnance					
35	a. Safety design features such as interlocks, redundancy grounding and isolation devices are incorporated so that no single detectible failure or combination of undetectible failures result in premature detonation of explosive devices.			X		
36	b. Unused explosive devices aboard the Tug will be safed on command the safing verification sent to the Orbiter prior to retrieval.	X				
37	Power supplies shall be protected from short circuit of ordnance firing circuits after firing.			X		
38	Ordnance initiators shall be protected from induced voltages.			X		
39	Shielding is provided to protect ordnance initiator and firing circuit from stray voltage.			X		

SYSTEM SAFETY CHECKLIST

SUBSYSTEM: Composite

HARDWARE DESCRIPTION: Space Tug Systems Study

DATE: 8/2/73

COMPLETED BY: (NAME) Summary

ITEM NUMBER		DESIGN COMPLIES	DESIGN DOES NOT COMPLY	DETAIL DESIGN WILL COMPLY	DETAIL DESIGN WILL NOT COMPLY	NOT APPLICABLE
	A. STRUCTURAL SYSTEMS					
40	1. Hypergolic fuels shall not be separated by only a single weld.					X
41	2. Proof test requirements for all components shall be compatible with manned requirements.			X		
42	3. All lines, flexible hoses, fittings, tanks and pressure vessels/reservoirs shall have safety factors consistent with manned requirements.			X		
43	4. Pressure vessels are capable of internal inspection for contamination, corrosion, defects, etc.	X				
44	5. All liquid vessels shall have a drain valve located such that all liquid may be drained from the vessel during ground (horizontal or vertical) operations.	X				
45	6. Materials with a high susceptibility to stress corrosion will not be used.	X				
46	7. Materials with a low fracture toughness will not be used.	X				
47	8. Material selection will preclude galvonic corrosion.			X		
48	9. Design will not overload structure above the stress corrosion limits.			X		
49	10. Design will preclude exposure of titanium to liquid oxygen (or low temperature gaseous oxygen); fuel cell boil-off.					X
50	11. Design will prevent hydrogen embrittlement of titanium.			X		
51	12. The upper stage vehicle shall be supported in the Orbiter so that failure of any one structural support member will not jeopardize support of the upper stage vehicle during return to earth.		X			

SYSTEM SAFETY CHECKLIST

ITEM NUMBER	SUBSYSTEM: Composite		DESIGN COMPLIES	DESIGN DOES NOT COMPLY	DETAIL DESIGN WILL COMPLY	DETAIL DESIGN WILL NOT COMPLY	NOT APPLICABLE
	HARDWARE DESCRIPTION: Space Tug Systems Study						
	DATE: 8/2/73	COMPLETED BY: (NAME) Summary					
52	13. a. Tanks shall be designed so that failure due to overpressure will not produce shrapenl. OR				X		
53	b. Pressurized tanks shall be located or protected by shrapnel proof barriers so that explosion of one will not propagate.				X		

SYSTEM SAFETY CHECKLIST

ITEM NUMBER	SUBSYSTEM: Composite / HARDWARE DESCRIPTION: Space Tug Systems Study / DATE: 8/2/73 / COMPLETED BY: (NAME) Summary	DESIGN COMPLIES	DESIGN DOES NOT COMPLY	DETAIL DESIGN WILL COMPLY	DETAIL DESIGN WILL NOT COMPLY	NOT APPLICABLE
	B. FUEL/PROPELLANT SYSTEMS					
54	Separate incompatible fluid systems to prevent inadvertent mixing.	X				
55	Design adjacent incompatible systems so that it is impossible to interconnect them.	X				
56	Select fluid line insulation that cannot react chemically with the system fluid.	X				
57	Select non-absorbent fluid line insulation.		X		X	
58	Use sleeves or barriers to isolate exposed fluid lines.		X		X	
59	Hypergolic fuels shall not be separated by only a single weld.	X				
60	Fill port back flow is prevented by design.		X		X	
61	Propellant valves are protected from damage by Thrust Chamber heat soak.		X		X	
62	N_2O_4 is inhibited with NO to prevent corrosion of titanium.	X				
63	Limit fuel and propellant pressure rise to 10% over normal pressure.		X		X	
64	Provide that tank pressure will be relieved before structural limits are exceeded.	X				
65	Provide overpressure relief where fluid lines or components may be exposed to fire.		X		X	
66	Provide underpressure relief during defueling operations or during reentry.	X				
67	Transfer lines for propellants shall be located outside of tanks or shall be double walled with the capability of venting the space between the two containers to space.	X				

SYSTEM SAFETY CHECKLIST

SUBSYSTEM: Composite

HARDWARE DESCRIPTION: Space Tug Systems Study

DATE: 8/2/73

COMPLETED BY: (NAME) Summary

ITEM NUMBER		DESIGN COMPLIES	DESIGN DOES NOT COMPLY	DETAIL DESIGN WILL COMPLY	DETAIL DESIGN WILL NOT COMPLY	NOT APPLICABLE
68	Propellant shut-off valves upstream from all start valves shall be provided so that inadvertent main valve opening would not start engines on upper stage vehicles while in or near the Orbiter.	X				
69	Liquid line insulation shall be made of nonabsorbent materials.		X		X	
70	All lines, flexible hoses, fittings and pressure vessels/reservoirs shall have a minimum design burst pressure consistent with manned safety requirements.	X				
71	System connectors shall be keyed or sized so that it is physically impossible to connect an incompatible commodity or pressure level.	X				
72	Pressure vessels are capable of internal inspection for contamination, corrosion, defects, etc.			X		
73	Initial opening of all pressure vessel primary relief devices shall be no higher than 110% of the maximum design operating pressure of the vessel.			X		
74	All pressure vessels and reservoirs shall have an isolation shutoff valve located as the first component down stream of the vessel and as close as possible to the vessel.			X		
75	All pressure vessels shall have a valve to vent or bleed the pressure.		X		X	
76	All liquid vessels shall have a drain valve located such that all liquid may be drained from the vessel during ground (horizontal or vertical) operations.	X				
77	A pressure relief device shall be located downstream of any pressure regulating device where source pressure can exceed the proof pressure of the downstream system.	X				
78	The initial opening of system relief valves shall be no higher than 110% of the upstream regulator setting.			X		

SYSTEM SAFETY CHECKLIST

SUBSYSTEM: Composite

HARDWARE DESCRIPTION: Space Tug Systems Study

DATE: 8/2/73

COMPLETED BY: (NAME) Summary

ITEM NUMBER		DESIGN COMPLIES	DESIGN DOES NOT COMPLY	DETAIL DESIGN WILL COMPLY	DETAIL DESIGN WILL NOT COMPLY	NOT APPLICABLE
79	All venting of the Tug while near the Orbiter shall be non-propulsive or shall translate the vehicle away from the Orbiter.	X				
80	Manually operated valves shall not be used to by-pass pressure regulator or flow control devices.	X				
81	Shutoff valves shall not be used for isolating relief valves.			X		
82	Check valves shall be located in pressure systems to minimize downstream pressure loss resulting from loss of source pressure.	X				
83	Check valves shall be used to isolate parallel supply systems which can be used to service a common downstream system.	X				
84	Check valves shall be used to isolate parallel vent lines each of which vents into a common manifold.	X				
85	An isolation shutoff valve shall be installed in each system supplied from a common liquid or gas pressure source.	X				
86	Flow restrictors, orifices and similar flow limiting devices shall be installed immediately downstream of all components which could fail in a manner that would exceed the relief/vent capacity of any spacecraft compartment.	X				
87	Ball valves with nylon seats shall not be used in systems operating above 1000 psi.				X	
88	Filter housings that are required to be removed from the system for element replacement shall not be used.	X				

SYSTEM SAFETY CHECKLIST

SUBSYSTEM: Composite

HARDWARE DESCRIPTION: Space Tug Systems Study

DATE: 8/2/73

COMPLETED BY: (NAME) Summary

ITEM NUMBER		DESIGN COMPLIES	DESIGN DOES NOT COMPLY	DETAIL DESIGN WILL COMPLY	DETAIL DESIGN WILL NOT COMPLY	NOT APPLICABLE
89	Visual monitoring capability shall be provided for each level of system pressure.		X		X	
90	Freeze protection provided for all overboard dump lines, e.g., fuel cell water dump.	X				
91	Gaseous content of pressurized tanks shall be small enough so that rapid isentropic expansion into the Orbiter cargo bay will not result in overpressure		X			

SYSTEM SAFETY CHECKLIST

ITEM NUMBER	SUBSYSTEM: Composite HARDWARE DESCRIPTION: Space Tug Systems Study DATE: 8/2/73 — COMPLETED BY: (NAME) Summary	DESIGN COMPLIES	DESIGN DOES NOT COMPLY	DETAIL DESIGN WILL COMPLY	DETAIL DESIGN WILL NOT COMPLY	NOT APPLICABLE
	C. LIQUIDS AND GASES					
92	Systems shall be designed so that it is physically impossible to install components in a reverse position from which they were intended to function within the system.	X				
93	Systems shall be designed to minimize the effects of shock waves or pressure surges generated by sudden changes in flow.	X				
94	Proof test requirements for all components shall be a minimum of 1.5 times the maximum pressure at which they will be required to operate within the system.	X				
95	Components containing mercury shall not be used.	X				
96	The maximum system operating pressure delivered by each regulator shall not be greater than 85% of the maximum pressure regulating capability of the regulator.	X				
97	All piping and components shall be grounded to reduce static electricity potential.	X				
98	Electrical/electronic components such as motors, sensors or switches used in liquid or gas systems shall be installed with the component housing external to the vessel or piping containing the liquid or gas.	X				
99	Solder joints shall not be used for coolant system installation.	X				
100	Pumps shall be protected against damage by use of protective devices such as thermal overloads, by-pass relief devices, vibration sensitive cutout switches, pump suction pressure interlocks and overspeed controls.			X		

SYSTEM SAFETY CHECKLIST

SUBSYSTEM: Composite

HARDWARE DESCRIPTION: Space Tug Systems Study

DATE: 8/2/73

COMPLETED BY: (NAME) Summary

ITEM NUMBER		DESIGN COMPLIES	DESIGN DOES NOT COMPLY	DETAIL DESIGN WILL COMPLY	DETAIL DESIGN WILL NOT COMPLY	NOT APPLICABLE
101	Pressure relief valves shall be sized to exceed the maximum flow capacity of the upstream pressure regulating device.			X		
102	Backup or redundant positive relief capability shall be provided wherever a primary relief device malfunction could allow system proof pressure levels to be exceeded.			X		
103	Initial opening of backup or redundant relief devices excluding cabin relief valves shall be no higher than 125% of the upstream regulator setting.			X		
104	Backup or redundant relief devices shall be located in the system so as not to render the primary relief device ineffective.			X		
105	A relief device shall be located between any restrictor orifice installation and an upstream pressure regulating device.	X				
106	Flow orifices shall not be located in system vent or relief lines.			X		
107	All relief ports and vent lines shall be located so that escaping gases will not be hazardous to personnel and/or equipment during flight or ground operations.			X		
108	All system vent and relief valves shall be designed to fail open.			X		
109	Vent or bleed valves shall be located in the system wherever liquids or pressure could be trapped between components.			X		

SYSTEM SAFETY CHECKLIST

SUBSYSTEM: Composite

HARDWARE DESCRIPTION: Space Tug Systems Study

DATE: 8/2/73

COMPLETED BY: (NAME) Summary

ITEM NUMBER		DESIGN COMPLIES	DESIGN DOES NOT COMPLY	DETAIL DESIGN WILL COMPLY	DETAIL DESIGN WILL NOT COMPLY	NOT APPLICABLE
	D. ELECTRICAL/ELECTRONIC					
110	The spacecraft structure shall not be used for the return of current to the power source.		X		X	
111	DC returns shall not be disconnected or isolated from the single point ground connection to the spacecraft structure during any power system mode of operation.		X		X	
112	Module mating surfaces shall be electrically bonded so that a fault current may be safely returned from any point in the module through the structure to the vehicle single point ground.	X				
113	Redundant power distributor buses shall not be routed through the same connector.	X				
114	The electrical power system shall include the capability to isolate all loads from the power source to permit load selection during emergency conditions.	X				
115	Equipment shall not be damaged by momentary power interruptions.	X				
116	Circuits having capacitors shall discharge to less than 1 volt within 2 seconds after power removal.			X		
117	Design will prevent "make before break" or "break before make" relay races.	X				
118	All external parts of RF equipment, excluding the driven elements of the antenna and transmission lines, shall be at ground potential at all times.	X				
119	RF equipment shall be shielded to prevent personnel exposure to RF levels greater than 10 mw/cm^2 except in front of the antenna.			X		
120	Components containing mercury shall not be used.			X		

SYSTEM SAFETY CHECKLIST

SUBSYSTEM: Composite

HARDWARE DESCRIPTION: Space Tug Systems Study

DATE: 8/2/73

COMPLETED BY: (NAME) Summary

ITEM NUMBER		DESIGN COMPLIES	DESIGN DOES NOT COMPLY	DETAIL DESIGN WILL COMPLY	DETAIL DESIGN WILL NOT COMPLY	NOT APPLICABLE
121	Conformal coatings which place stress on glass diodes shall not be used.			X		
122	Polyurethane conformal coatings containing solvents which dissolve polystyrene shall not be used on circuit boards containing polystyrene components.			X		
123	Components used in areas with flammable fluids shall be incapable of causing ignition.			X		
124	Gaskets, seals and similar components containing sulphur shall not be used within or in contact with electrical components containing copper, zinc, nickel or solver.			X		
125	All connectors, circuit boards, terminal boards, switches or relays and similar components shall be potted, sealed or similarly protected against shorting by materials floating in a zero G environment.			X		
126	All connectors, circuit boards, terminal boards, switches, relays and similar components shall be potted, sealed or similarly protected against the effects of liquid leakage or condensation.			X		
127	Equipment shall revert to a safe configuration when an input power loss occurs.	X				
128	Power and signal (including command) wiring shall not be routed through the same cable, cable bundle, or wiring harness to minimize voltage induced into adjacent circuits.		X			
129	Shields used to protect against induced voltage for frequencies up to 50 KHz shall be grounded at only one end.			X		
130	Shields used to protect against induced voltage for frequencies above 50 KHz shall be grounded at both ends.	X				

SYSTEM SAFETY CHECKLIST

SUBSYSTEM: Composite

HARDWARE DESCRIPTION: Space Tug Systems Study

DATE: 8/2/73

COMPLETED BY: (NAME) Summary

ITEM NUMBER		DESIGN COMPLIES	DESIGN DOES NOT COMPLY	DETAIL DESIGN WILL COMPLY	DETAIL DESIGN WILL NOT COMPLY	NOT APPLICABLE
131	Polyvinyl chloride shall not be used as wire insulation.			X		
132	Electrical wire or cable insulated or coated with polytetraflouroethylene (TFE) or flourinatedethylene propylene (FEP) shall be etched prior to potting to assure positive bond and environmental seal.			X		
133	When etching of insulation is required, the design shall specify that the open end of the wire will not be exposed to the etchant.			X		
134	Organic pigments will not be used in teflon insulation.			X		
135	All mating plugs and receptacles shall be marked or coded to clearly indicate the correct mating connection.			X		
136	All adjacent connectors shall be shaped, sized or keyed so that it is physically impossible to mismate or cross-connect.			X		
137	Connectors with unkeyed symmetrical pin arrangements shall not be used.		X			
138	Only female connectors shall be used to terminate source of power.			X		
139	No flammable potting will be used in electrical connectors.			X		
140	Power circuits and signal circuits shall not be routed through the same connector to minimize the introduction of voltage transients into the signal wiring.		X			
141	All battery vents and relief devices shall be designed to prevent the ejection or electrolyte from the battery.			X		
142	All battery vents and relief devices shall be located so that escaping gas shall not damage adjacent equipment.			X		

SYSTEM SAFETY CHECKLIST

SUBSYSTEM: Composite

HARDWARE DESCRIPTION: Space Tug Systems Study

DATE: 8/2/73

COMPLETED BY: (NAME) Summary

ITEM NUMBER		DESIGN COMPLIES	DESIGN DOES NOT COMPLY	DETAIL DESIGN WILL COMPLY	DETAIL DESIGN WILL NOT COMPLY	NOT APPLICABLE
143	Batteries are thermally isolated from one another.			X		
144	All battery cases shall be designed to contain all electrolyte during all over pressure conditions such as those which could be caused by overload or internal shorts.	X				
145	Installed batteries (single or multiple celled) shall be enclosed within a container which will prevent electrolyte leakage to the surrounding area in case of damage to the battery case.	X				
146	Self-test circuits shall indicate the actual system response, rather than indicate only the initiation of a command or test signal.	X				
147	All circuit breakers or switches used to control equipment or circuitry intended for emergency purposes shall have positive protection against inadvertent operation.			X		
148	Design will prevent high resistance coating of contacts from outgassing products of potted compound at elevated temperatures or low pressures.			X		
149	All circuit breakers or switches used to control the arming of pyrotechnic devices shall have positive protection against inadvertent operation.			X		
150	Redundant control circuit components shall be independent of those components used in the primary control circuit.	X				
151	Primary and redundant control circuit wiring shall not be routed through the same cable or connector.	X				
152	Primary and redundant control circuits shall include an in-flight checkout capability which will verify the independent operation of each circuit.	X				

SYSTEM SAFETY CHECKLIST

SUBSYSTEM: Composite

HARDWARE DESCRIPTION: Space Tug Systems Study

DATE: 8/2/73

COMPLETED BY: (NAME) Summary

ITEM NUMBER		DESIGN COMPLIES	DESIGN DOES NOT COMPLY	DETAIL DESIGN WILL COMPLY	DETAIL DESIGN WILL NOT COMPLY	NOT APPLICABLE
153	Primary and redundant system circuits shall not be supplied from the same power bus or circuit breaker.	X				
154	All circuits (including latching relay circuits) shall be protected against inadvertent operation due to voltage transients.	X				
155	All system indicators used to monitor system status shall indicate the actual system response rather than indicate only the initiation of a command or application of power.	X				
156	Loss of control circuit power shall not result in the loss of indication power for that circuit.			X		
157	Tantalum wet slug capacitors shall not be used in timing circuits, circuits designed to stabilize frequency or circuits subject to polarity reversal.	X				
158	Metal film resistors shall not be used where tolerances of 5% or <u>less</u> are required.		X			
159	Point-contact, grown-junction or alloy-junction semi-conductors shall not be used.			X		
160	Design will prevent powering up system with latching relays in unknown positions.	X				
161	Design will prevent contamination of magnetic latches on magnetic latch relays.			X		
162	Terminal lugs and insulated washers used with stud-mounted diodes shall have sufficient matching surface area to ensure that the terminal lug will remain insulated from the mounting structure.			X		
163	All power and signal returns shall be isolated from the chassis and shall be routed through connectors or terminals to the vehicle single point ground.		X		X	

SYSTEM SAFETY CHECKLIST

SUBSYSTEM: Composite

HARDWARE DESCRIPTION: Space Tug Systems Study

DATE: 8/2/73

COMPLETED BY: (NAME) Summary

ITEM NUMBER		DESIGN COMPLIES	DESIGN DOES NOT COMPLY	DETAIL DESIGN WILL COMPLY	DETAIL DESIGN WILL NOT COMPLY	NOT APPLICABLE
164	Resistors subject to significant resistance changes (5% or greater) when subjected to electrostatic fields will not be used.			X		
165	All circuit breakers located in or used with equipment containing flammable vapors or liquids shall be explosion proof.			X		
166	Circuit breakers shall provide a visual indication when tripped.	X				
167	Circuit breakers shall trip and protect the circuit even if the switch lever is physically held in the "ON" position.	X				
168	Overload protection devices shall be installed in each ungrounded conductor in three (3) phase power systems and shall be designed so that all three (3) devices trip simultaneously.					X
169	All circuit breakers shall be sized (or set) to protect the smallest wire within a circuit, including all branches which do not have independent circuit protection.	X				
170	Overload protection devices shall be sized (or set) so that the combination of current and time at which the device operates will not cause the operation of upstream protective devices.			X		

SYSTEM SAFETY CHECKLIST

ITEM NUMBER	SUBSYSTEM: Composite HARDWARE DESCRIPTION: Space Tug Systems Study DATE: 8/2/73 — COMPLETED BY: (NAME) Summary	DESIGN COMPLIES	DESIGN DOES NOT COMPLY	DETAIL DESIGN WILL COMPLY	DETAIL DESIGN WILL NOT COMPLY	NOT APPLICABLE
	E. SOLID ROCKET MOTORS					
171	The propellant shall have a demonstrated auto ignition temperature at least 100°F higher than the maximum Orbiter bay temperature (Orbiter bay maximum temperature=200°F).	X				
172	The propellant shall have a demonstrated insensitivity to the shock levels experienced in the cargo bay of the Orbiter.	X				
173	The propellant shall have a demonstrated stability to ground transportation, ground handling, installation and checkout without accidental ignition.	X				
174	SRM ignitors shall be non-fragmenting.	X				
175	SRM ignitors shall be shock insensitive to Orbiter bay shock levels.	X				
176	SRM ignitors shall have auto ignition temperatures at least 100°F higher than the maximum Orbiter bay temperature (200°F maximum Orbiter bay temperature).	X				
177	SRM ignitor-ignition circuits or devices shall be protected from induced voltages and shall be protected against a single failure causing premature ignition; example, safe/arm device.	X				
178	SRM ignitors shall be seasoned designs with proven performance and safety, preferably in manned systems.	X				
179	SRM propellants shall be seasoned designs with proven performance and safety, preferably in manned systems.	X				

SYSTEM SAFETY CHECKLIST

SUBSYSTEM: Composite

HARDWARE DESCRIPTION: Space Tug Systems Study

DATE: 8/2/73

COMPLETED BY: (NAME) Summary

ITEM NUMBER		DESIGN COMPLIES	DESIGN DOES NOT COMPLY	DETAIL DESIGN WILL COMPLY	DETAIL DESIGN WILL NOT COMPLY	NOT APPLICABLE
	F. CAUTION AND WARNING (C&W)					
180	All C&W sensors shall fail in such a manner that a signal input will be initiated to the Data Management System, resulting in an alarm.	X				
181	All sensors for all parameters monitored for C&W shall be independently powered to prevent loss of hazard indication due to power failure of a monitored system.		X			
182	Out-of-limit conditions in the C&W primary power circuitry shall initiate an alarm.	X				
183	All sensors used for inputs to systems other than C&W, which are also used for C&W, shall be isolated such that a failure in the other system will not affect the C&W.		X			
184	Use explosive vapor detectors wherever explosive vapors can collect.					X
185	Design the explosive vapor detection system to trigger an alarm at 20% of the lower explosive level.	X				
186	Design hazard warning systems so they can be reset to indicate a hazard reoccurrence.					X
187	Provide fire detection systems for all potential fire zones.					X

SYSTEM SAFETY CHECKLIST

SUBSYSTEM: Composite

HARDWARE DESCRIPTION: Space Tug Systems Study

DATE: 8/2/73

COMPLETED BY: (NAME) Summary

ITEM NUMBER		DESIGN COMPLIES	DESIGN DOES NOT COMPLY	DETAIL DESIGN WILL COMPLY	DETAIL DESIGN WILL NOT COMPLY	NOT APPLICABLE
	G. CRYOGENIC SYSTEMS					
188	Cryogenic systems and lines shall be located and/or insulated adequately to prevent freezing of fluid lines in other systems.			X		
189	Hydrogen and oxygen boil-off shall be controlled to prevent intermixing of the boil-off gases.			X		
190	All materials in the system are LO_2 and LH_2 compatible.	X				
191	Fuel cell water dump lines are protected against freezing.			X		
192	Fuel cell water dump lines are protected against freezing after a single failure in the freeze protection system.			X		
193	System design will prevent cryogenic fluid from being trapped without a means of adequate pressure relief.			X		
194	System design will prevent cryogenic fluid from being trapped after a single failure in the pressure relief system.			X		
195	System design will prevent cryogenic boil-off from accumulating in the Orbiter cargo bay.			X		
196	System design will route vent lines for cryogenic boil-off over board and prevent accumulation of boil-off gases in the Orbiter cargo bay.			X		
197	LO_2 and LH_2 (or GO_2 and GH_2) disconnects shall be designed to prevent accidental mismating.			X		
198	System design will prevent static charge build-up due to fluid flow.			X		
199	System design will prevent air intrusion into purged hydrogen system.					

OPERATIONAL SAFETY CHECKLIST

This attached checklist presents the composite results of lists completed individually by:

J. Kimpton - Operations & Maintenance

A. Brook - Avionics

J. Hurley - Propulsion

OPERATIONAL SAFETY CHECKLIST

ITEM NO.	OPERATIONS: [X] GROUND [X] FLIGHT DATE: 8/2/73 — COMPLETED BY: Summary	DO ACCOMODATE	DON'T ACCOMODATE	DETAIL WILL COMPLY	DETAIL WON'T COMPLY	NOT APPLICABLE
	GENERAL					
1	Special protective garments and equipment shall be provided for personnel working in a toxic environment or near potentially toxic elements.	X				
2	Manually and remotely controlled means shall be provided for controlling and extinguishing fires.					X
3	The pressures on each side of a hatch shall be verified before opening the hatch.			X		
4	Any Tug lifting or hoisting operations which could result in a catastrophic condition (e.g., propellants loaded) if the lift/hoist mechanism fails, will be single malfunction proof.			X		
5	Transportation and hoisting load limits, static and dynamic, shall be less than flight load limits in all cases.			X		
6	Continuous propellant dump provisions are provided from propellant load to liftoff.	X				
7	Continuous environmental control of the Tug is provided after propellants/pressurants are loaded until Tug/Orbiter bay installation is complete.		X			
8	Propellant/pressurization tank parameters are monitored continuously from time of loading through liftoff by GSE sources.	X				
9	Propellant tank venting will be controlled to prevent toxic vapors in the atmosphere.			X		
10	Purge provisions are provided by GSE sources to neutralize propellant leaks after propellant loading and after Shuttle landing.	X				
11	Emergency ventilation provisions are available under positive pressures for all ground operations subsequent to propellant loading.		X			

OPERATIONAL SAFETY CHECKLIST

ITEM NO.	OPERATIONS: [X] GROUND [X] FLIGHT DATE: 8/2/73 — COMPLETED BY: Summary	DO ACCOMODATE	DON'T ACCOMODATE	DETAIL WILL COMPLY	DETAIL WON'T COMPLY	NOT APPLICABLE
	HAZARDOUS FLUIDS/MATERIALS					
12	The pressures, temperatures or other parameters which indicate the status of hazardous fluids or materials shall be verified before they are transported.			X		
13	Mutually reactive fluids shall not be handled or transferred simultaneously.			X		
14	Manual handling and transfer of hazardous fluids or materials shall be carried out by two or more personnel who shall have no other duties during this operation.	X				
15	The "buddy" system is recommended when hazardous fluids or material is being handled so that one man can come to the assistance of the other in the event of an accident or problem. Handling of hazardous fluids or materials should be a dedicated task, so as not to allow a problem to occur because of interference with other tasks.	X				
16	Emergency procedures shall be available for handling, containing and disposing of spilled hazardous fluids or materials so as to safeguard personnel.			X		
17	Corrosive fluids or materials shall be double contained during handling and transfer in unpressurized areas. Capability shall be provided to verify the integrity of both containers before and after transfer.		X			
18	Transfer lines in unpressurized areas shall be purged after the transfer of hazardous fluids.			X		
19	Special protective garments and equipment shall be provided for personnel working in a toxic environment or near potentially toxic elements.			X		
20	Transfer lines in pressurized areas shall be purged after the transfer of hazardous fluids and before breaking plumbing connections.			X		

OPERATIONAL SAFETY CHECKLIST

ITEM NO.	OPERATIONS: [X] GROUND [X] FLIGHT DATE: 8/2/73 — COMPLETED BY: Summary	DO ACCOMODATE	DON'T ACCOMODATE	DETAIL WILL COMPLY	DETAIL WON'T COMPLY	NOT APPLICABLE
	HAZARDOUS FLUIDS/MATERIALS (CONTINUED)					
21	Means shall be provided for detecting the presence of spilled hazardous fluids or materials while being handled or transferred.			X		
22	Procedures shall be available for handling and transferring hazardous fluids or materials without releasing fluid or material to the spacecraft atmosphere.			X		

OPERATIONAL SAFETY CHECKLIST

ITEM NO.	OPERATIONS: [X] GROUND [X] FLIGHT DATE: 8/2/73 COMPLETED BY: Summary	DO ACCOMODATE	DON'T ACCOMODATE	DETAIL WILL COMPLY	DETAIL WON'T COMPLY	NOT APPLICABLE
	FLIGHT OPERATIONS					
23	Pressurizing gas shall be turned off until immediately prior to release of the vehicle from the Orbiter.	X				
24	Tug attitude shall be controlled by command of the Orbiter crew immediately following release.	X				
25	Tug shall be switched from command control to internal attitude control after Orbiter has been sufficiently moved that no attitude change could result in collision.	X				
26	Internal attitude control signal of the Tug shall be monitored for accuracy by the Orbiter crew before release.	X				
27	The planned attitudes of the Tug during release and separation from the Orbiter shall be such that the attitude control engines at no time accelerate the vehicle towards the Orbiter.	X				
28	Orbiter crew control of the Tug shall be provided until separation from the Orbiter precludes possibility of recontact.	X				
29	Vehicle propellant tank pressures shall be reduced to the minimum operating value before retrieval into the Orbiter cargo bay.		X			

POTENTIAL HAZARD MATRIX

CONFIGURATION: All System Study Task 5

SYSTEM: Propulsion, General

DATE: 8-1-73

PAGE: I-1

SUBSYSTEM/ COMPONENT	TRANSPORTATION & HANDLING	PREFLIGHT OPERATIONS	LAUNCH OPERATIONS	ORBITER FLIGHT	TUG DEPLOYMENT/ RETRIEVAL	TUG FREE FLIGHT	PAYLOAD DEPLOYMENT/ RETRIEVAL	POST FLIGHT OPERATIONS	ABORT	OTHER ANALYSES		
										FMEA	OPERATIONS & MAINTENANCE	DESIGN CHECK LIST
1. Propellants												
1.1 Oxidizer, N_2O_4	4,6,8, 15 (1.001)										2.2.1.9 (1.001)	
1.2 Fuel, MMH	6,8, 15 (1.002)										2.2.1.11 (1.002)	
2. Tanks												
2.1 Oxidizer	10 (1.003)									SFP-I,10 (1.003)		63 (1.003)
2.2 Fuel	10 (1.003)									SFP-I,11 (1.003)		63 (1.003)
3. Special Considerations												
3.1 Tug with propellants loaded	8 (1.004)										2.2.1.13 2.2.2.3 2.2.3.1 2.3.1 2.3.3.1 (1.004)	

POTENTIAL HAZARD MATRIX

CONFIGURATION: PR-1 (2)

SYSTEM: Main Engine Support

DATE: 8-1-73

PAGE: II-1

SUBSYSTEM/ COMPONENT	TRANSPORTATION & HANDLING	PREFLIGHT OPERATIONS	LAUNCH OPERATIONS	ORBITER FLIGHT	TUG DEPLOYMENT/ RETRIEVAL	TUG FREE FLIGHT	PAYLOAD DEPLOYMENT/ RETRIEVAL	POST FLIGHT OPERATIONS	ABORT	OTHER ANALYSES		
										FMEA	OPERATIONS & MAINTENANCE	DESIGN CHECK LIST
1. Pressurization												
1.1 He Sphere												
1.2 He Solenoid Valve												
1.3 He Regulator												
1.4 He Check Valve												
1.5 Burst/Relief Valve												
1.6 Lines & Fittings												
2. Propellant Feed												
2.1 Propellant Valves												
2.2 Lines & Fittings												

HAZARD ANALYSIS

HAZARD CLASS	Critical	NO.	1.001
STATUS	Open	PAGE	1 of 2
PROGRAM PHASE	System Study	DATE	8/1/73

SYSTEM: Propulsion SUBSYSTEM: Oxidizer, N_2O_4

OPERATION/PHASE: All

HAZARD GROUP: 4, 6, 8, and 15

REFERENCES: AFSC DH 1-6, AFM 160-39

HAZARD DESCRIPTION:

Nitrogen Tetroxide, N_2O_4, is a corrosive, highly toxic oxidizing agent. It is non-flammable in air but supports combustion and is hypergolic with the hydrazines.

POTENTIAL EFFECTS:

Liquid nitrogen tetroxide in contact with organic materials such as sawdust, excelsior, paper or cotton waste may cause fires.

(Continued on Page 2)

ASSUMPTIONS/RATIONALE:

1) Nitrogen tetroxide (N_2O_4) is a yellow to dark brown colored fuming liquid at room temperature. It emits yellowish to reddish brown fumes having a characteristic pungent odor. The material is an equilibrium mixture of nitrogen tetroxide and nitrogen dioxide (NO2), with a Threshold Limit Value of 2.5 ppm.
2) Nitrogen tetroxide is not sensitive to mechanical shock, heat or detonation.
3) Nitrogen tetroxide is soluble in water, forming nitric acid and nitrous acid. The latter decomposes to form additional nitric acid and evolves oxides of nitrogen.

~~(Continued on Page 2)~~

REQUIREMENTS:	REFERENCE
A. Design	
1. Separate incompatible fluid systems to prevent inadvertent mixing.	DCL-54
2. Design adjacent incompatible systems so that it is impossible to interconnect them.	DCL-55
3. Hypergolic fuels shall not be separated by <u>only</u> a single weld.	DCL-59
4. Inhibit N_2O_4 with NO to prevent corrosion of titanium.	DCL-62
5. Provide personnel showers and eye wash in propellant transfer area.	
6. Provide facility vent stacks for controlled venting.	

(Continued on Page 2)

DISPOSITION:

1. Entered in Hazard Catalog.

ORIGINATOR/LOCATION:

W. R. O'Halloran, Ext. 4203

(LIST ADDITIONAL CONTENT IN THE ORDER OF SHEET 1)

POTENTIAL EFFECTS

4) Nitrogen Tetroxide contacting the skin causes severe burns.
5) Vapors are extremely toxic to breathe. Low concentration that may be inhaled without discomfort may cause serious damage to the lungs. Symptoms of lung damage may be delayed 5 to 30 hours after exposure.
6) Nitrogen Tetroxide contacting the eyes may cause permanent damage.
7) Concentrated nitrogen tetroxide vapor contacting the skin may cause burns.
8) Low concentration of vapor contacting the skin may cause a yellowing of the skin.

ASSUMPTIONS/RATIONALE:

4) Nitrogen tetroxide has been used safely on the Titan II and Titan III Programs.

5) Detail design and handling procedures can be developed to reduce the hazard level to Controlled.

REQUIREMENTS

B. Operations

1. Provide protective clothing for propellant handling personnel.

2. Propellant handlers will be trained and certified.

3. Propellant handlers must pass an annual propellant physical examination.

4. Define the propellant handling and loading plan.

5. Operations will be controlled by detailed procedures that have been approved by System Safety.

HAZARD ANALYSIS

HAZARD CLASS	Critical
STATUS	Open
PROGRAM PHASE	System Study

NO.	1.002
PAGE	1 of 2
DATE	8/2/73

SYSTEM: Propulsion SUBSYSTEM: Fuel, MMH

OPERATION/PHASE: All

HAZARD GROUP: 4, 6, 8, and 15

REFERENCES: AFSC DH 1-6, AFM 160-39

HAZARD DESCRIPTION:

Monomethyl Hydrazine, MMH, presents fire and explosion hazards and is highly toxic.

POTENTIAL EFFECTS:

1) MMH can be ignited/exploded in air by spark or flame, the degree of violence of reaction varies with concentration, temperature and catalytic conditions.

2) Effects on personnel include the following: (Continued on Page 2)

ASSUMPTIONS/RATIONALE:

1) Propellant grade MMH contains a minimum of 98% MMH, water is the other main constituent. It is a clear, water-white, hydroscopic liquid (able to absorb moisture from the atmosphere) with an ammonia-like odor.

2) The flammability limits of MMH are 2.5% to 98% in air; vapors within these limits can be exploded by an electric spark or open flame.

3) Liquid MMH is not sensitive to impact or friction. (Continued on Page 2)

REQUIREMENTS:	REFERENCE
A. Design	
1. Separate incompatible fluid systems to prevent inadvertent mixing.	DCL-54
2. Design adjacent incompatible systems so that it is impossible to interconnect them.	DCL-55
3. Hypergolic fuels shall not be separated by <u>only</u> a single weld.	DCL-40
4. Provide personnel showers and eye wash in propellant transfer area.	
5. Provide facility vent stacks for controlled venting.	
B. Operations	
1. Provide protective clothing for propellant handling personnel.	OCL-1
2. Propellant handlers will be trained and certified.	
(Continued on Page 2)	

DISPOSITION:

1. Entered in Hazard Catalog

ORIGINATOR/LOCATION:

W. R. O'Halloran, Ext. 4203

(LIST ADDITIONAL CONTENT IN THE ORDER OF SHEET 1)

POTENTIAL EFFECTS:

a. Liquid - MMH is a highly toxic chemical for which there is no known antidote. It is highly irritating and has a severe corrosive effect on the skin. Hydrazine may be absorbed through the skin. In the blood, it will destroy hemoglobin and lower the sugar content. Liquid splashed in the eyes will cause severe tissue damage and may cause permanent corneal opacity.

b. Vapor - MMH vapors are irritating to the eyes, nose and throat. Inhalation of the vapors can cause dizziness, nausea and hoarseness. The effects are not immediately noticeable, but appear gradually over a period of several hours exposure. Severe exposure to the eyes will produce burns similar to flash burn from a welding arc. In known cases, these effects have been temporary, lasting one to three days.

ASSUMPTIONS/RATIONALE:

4. Physical characteristics include: Boiling Point - 189.5°F; Freezing Point - -62.5°F, Flash Point - 61 - 63°F, Auto Ignitiion Point - 382°F.

5. MMH has been used safely on other aerospace applications.

6. Detail design and handling procedures can be developed to reduce the hazard level to Controlled.

REQUIREMENTS:

3. Propellant handlers must pass an annual propellant physical examination.

4. Define the propellant handling and loading plan.

5. Operations will be controlled by detailed procedures that have been approved by System Safety.

HAZARD ANALYSIS

HAZARD CLASS	Controlled
STATUS	Closed
PROGRAM PHASE	System Study

NO.	1.003
PAGE	1 of 2
DATE	8/3/73

SYSTEM: Propulsion, General SUBSYSTEM: Propellant Tanks

OPERATION/PHASE: Prelaunch and Launch

HAZARD GROUP: 10 - Pressure

REFERENCES:

HAZARD DESCRIPTION:
Propellant Tank ullage pressure increasing as a function of increasing temperature, due to loss of environmental control, after propellant loading and lockup could cause tank rupture.

POTENTIAL EFFECTS:
Injury or death of personnel exposed to toxic vapors released by tank rupture.

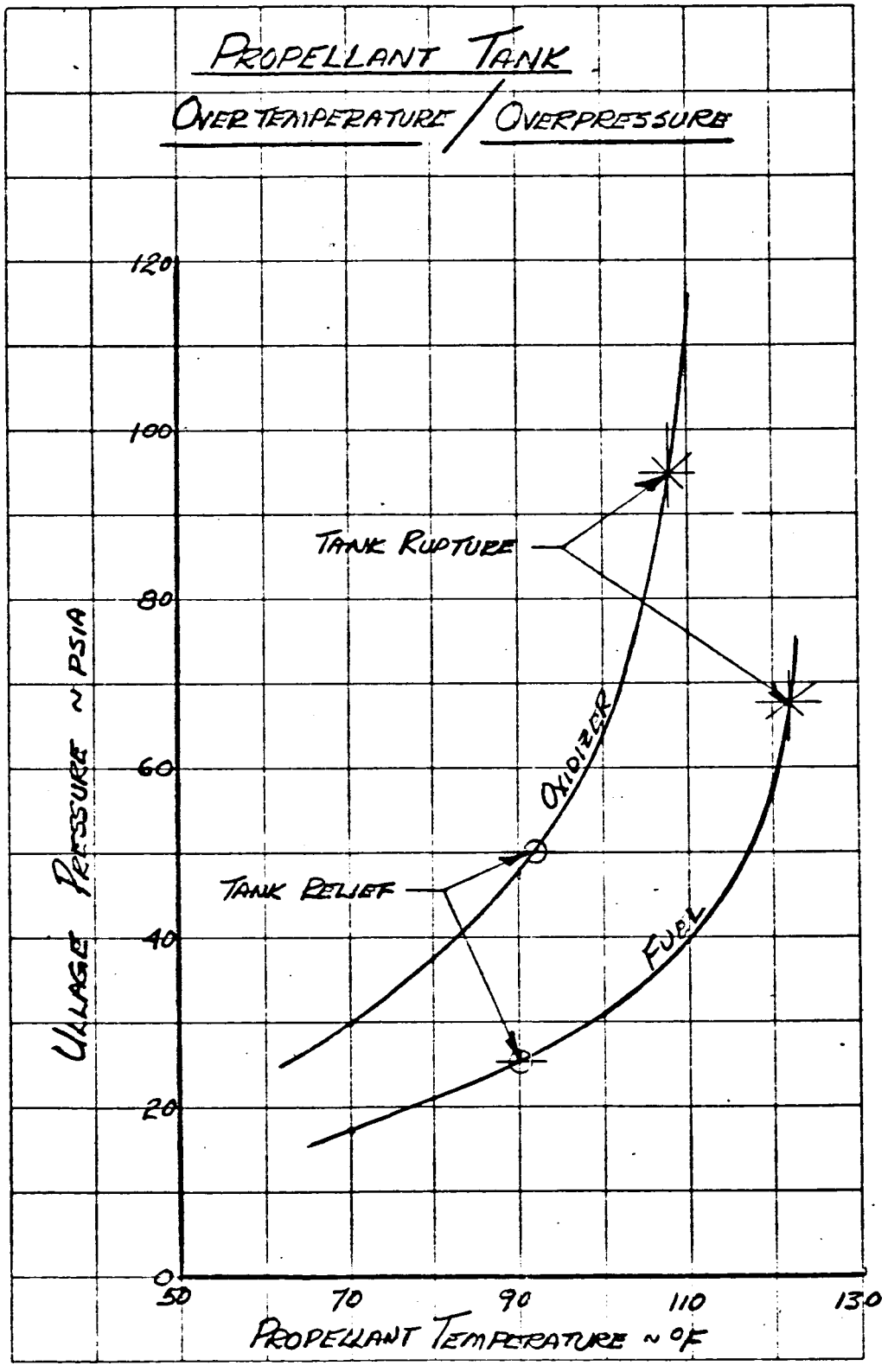
ASSUMPTIONS/RATIONALE:
1. Propellants are loaded at 65 $\pm$ 5°F.
2. Propellant tanks are pressurized with Helium to 17.5 psia for fuel and 30 psia for oxidizer (at 70°F) after propellant loading and locked up.
3. Series redundant burst/relief valves are provided to relieve at 25 psia for fuel and 50 psia for oxidizer.
4. Propellant tank overtemperature/overpressure relationships are shown on page 2.
5. These data demonstrate this hazard is eliminated.

REQUIREMENTS:	REFERENCE
A. Design	
1. Limit fuel and propellant pressure rise to 10% over maximum operating pressure.	DCL-63
2. Provide that tank pressure will be relieved before structural limits are exceeded.	DCL-64

DISPOSITION:
Potential hazard eliminated from further consideration due to inherent characteristics of propellants and provision of redundant pressure relief devices.

ORIGINATOR/LOCATION:
W. R. O'Halloran, Ext. 4203

91


PROPELLANT TANK
OVERTEMPERATURE / OVERPRESSURE
120
100
80
60
40
20
0
50
70
90
110
130
ULLAGE PRESSURE ~ PSIA
PROPELLANT TEMPERATURE ~ °F
TANK RUPTURE
TANK RELIEF
OXIDIZER
FUEL

HAZARD ANALYSIS

HAZARD CLASS	Catastrophic
STATUS	Open
PROGRAM PHASE	System Study

NO.	1.004
PAGE	1 of 1
DATE	08-04-73

SYSTEM: Propulsion, General SUBSYSTEM: N/A

OPERATION/PHASE: Transportation and Handling

HAZARD GROUP: 8 - Fire/Explosion/Implosion

REFERENCES: AFM 127-100, Explosives Safety Manual

HAZARD DESCRIPTION: Mishandling of the Space Tug after propellants are loaded presents a fire/explosion hazard if shock loads would cause the tanks to rupture.

POTENTIAL EFFECTS:

1. Loss of life, the Space Tug, Orbiter and equipment in the vicinity.
2. Extensive damage to facilities.

ASSUMPTIONS/RATIONALE:

1. Mass mixing of the hypergolic propellants would create a low grade explosion or fire ball.
2. Explosive Quantity - Distance criteria may be determined from AFM 127-100 as follows:

   60,000 lbs of propellant x 10% (for N_2O_4 and MMH) = 6000-lb equivalent high explosive.

   Required separation distance (from Table 5-10) = 730 feet.

REQUIREMENTS:	REFERENCE
A. Design	
1. Lifting and handling equipment shall be fail-safe.	
2. No single malfunction shall result in loss of control of lifted load.	
3. Design factors of safety for lifting and handling equipment shall be a minimum of 5.0 (ultimate).	
B. Operations	
1. Hoisting equipment shall be proof tested to 2.0 times load at least annually.	
2. Establish Danger Area of 730 ft radius around Space Tug during any movement after propellants are loaded.	
3. Non-essential personnel shall be evacuated from established Danger Area.	
4. Establish safe transportation routes for moving loaded Space Tug.	

DISPOSITION:

1. Entered in Hazards Catalog.

ORIGINATOR/LOCATION: W. R. O'Halloran, Ext. 4203

HAZARD CATALOG

PART I - HAZARDS LIST

SECTION: I - Propulsion, General

HAZARD NO.	HAZARD	ELIMINATED	RESIDUAL	HAZARD LEVEL	ACCEPTED	OPEN
1.001	Highly toxic, corrosive oxidizer, N_2O_4		1.1	Crit.		X
1.002	Highly toxic, flammable/explosive fuel, MMH		1.2	Crit.		X
1.003	Propellant tank ullage overpressure	X				
1.004	Fire/Explosion from both tanks rupture		1.3	Cat.		X

HAZARDS CATALOG

PART II - RESIDUAL HAZARDS

SYSTEM:	Propulsion	ITEM NO.	1.1
SUBSYSTEM:	Oxidizer, N_2O_4	HAZARD CLASS	Critical
COMPONENT:	N/A	DATE	8/1/73

HAZARD DESCRIPTION:

Nitrogen Tetroxide, N_2O_4, is a corrosive, highly toxic oxidizing agent. It is nonflammable in air but supports combustion and is hypergolic with the hydrazines. H_2O_4 in contact with organic materials may cause fires. Health hazards include skin and eye burns from liquid or vapor, and the extreme toxic effects of breathing vapor.

RECOMMENDATION:

1) Since N_2O_4 has been used safely on Titan II, Titan III, and Apollo, it is recommended that N_2O_4 be accepted as the Space Tug storable oxidizer.

2) The hazard level will remain critical until hardware build and approved detail operating procedures demonstrate the hazard is controlled.

DISPOSITION:

HAZARDS CATALOG
PART II - RESIDUAL HAZARDS

SYSTEM:	Propulsion	ITEM NO.	1.2
SUBSYSTEM:	Fuel, MMH	HAZARD CLASS	Critical
COMPONENT:	N/A	DATE	8/2/73

HAZARD DESCRIPTION:

Monomethyl hydrazine, MMH, presents fire and explosion hazards and is highly toxic. It can be ignited/exploded in air by spark or flame with varying violence of reaction. Health hazards include skin and eye burns from liquid or vapor, liquid absorption through the skin, and the toxic effects of vapor inhalation.

RECOMMENDATION:

1) Since MMH has been used safely in other aerospace applications, it is recommended that MMH be accepted as the Space Tug storable fuel.

2) The hazard level will remain critical until hardware build and approved detail operating procedures demonstrate the hazard is controlled.

DISPOSITION:

HAZARDS CATALOG
PART II - RESIDUAL HAZARDS

SYSTEM:	Propulsion	ITEM NO.	1.3
SUBSYSTEM:	Propellant Tanks	HAZARD CLASS	Catastrophic
COMPONENT:	N/A	DATE	08-04-73

HAZARD DESCRIPTION:

Mishandling of the Space Tug after propellants are loaded presents a fire/explosion hazard if shock loads would cause the tanks to rupture. A low grade explosion or fire ball would occur with possible loss of life and/or flight hardware and extensive damage to facilities.

RECOMMENDATION:

1. Establish and enforce rigid criteria/requirements for the design and operation of lifting and handling equipment.

2. The hazard will remain open until detail design and operating procedures meet requirements and adequate Danger Areas have been established.

DISPOSITION:

PROPOSED SAFETY OUTLINE FOR SEPTEMBER 17 PRESENTATION

- REVIEW SAFETY ANALYSIS METHODOLOGY
- ANALYSIS RESULTS SUMMARY
  - HAZARD IDENTIFICATION
    - INHERENT HAZARDS
    - UPDATED FMEA/SFP LIST
    - UPDATED OPERATIONS & MAINTENANCE SUMMARY
    - UPDATED SYSTEM SAFETY CHECKLISTS
  - HAZARD ANALYSIS
    - HAZARD CATALOG PART I
    - HAZARD CATALOG PART II
- SPECIFIC ANALYSIS RESULTS
  - DETAIL PRINCIPAL HAZARDS
  - ASSESSMENT OF CONFIGURATIONS
  - DESIGN & OPERATIONAL REQUIREMENTS

MARTIN MARIETTA

PROPOSED RELIABILITY OUTLINE FOR SEPTEMBER 17 PRESENTATION

- REVIEW RELIABILITY ANALYSIS METHODOLOGY
- RELIABILITY RESULTS SUMMARY
  - FAILURE MODES & EFFECTS SUMMARY
  - SINGLE FAILURE POINT SUMMARY
  - CONFIGURATION RELIABILITY PREDICTION
    - EACH SELECTED TUG CONFIGURATION
    - EACH SELECTED KICK STAGE CONFIGURATION
  - IDENTIFY SUBSYSTEM REDUNDANCY
  - IDENTIFY ALL ANALYSIS ASSUMPTIONS

MARTIN MARIETTA