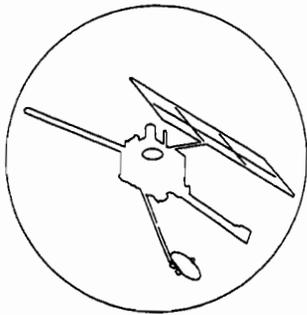


Mars Observer Loss of Signal: Special Review Board Final Report



November 1993

NASA

National Aeronautics and
Space Administration

Jet Propulsion Laboratory
California Institute of Technology
Pasadena, California

JPL Publication 93-28

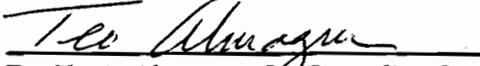
The research described in this publication was carried out by the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.

Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement by the United States Government or the Jet Propulsion Laboratory, California Institute of Technology.

CONCURRENCE



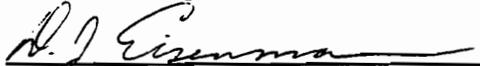
R. Rhoads Stephenson, Chairman
Deputy Assistant Laboratory Director, Technology and Applications Programs



Teofilo A. Almaguer, Jr., Recording Secretary
Member of Technical Staff, Hardware Assurance Division



Douglas E. Bernard
Technical Group Leader, Guidance and Control Section



David J. Eisenman
Deputy Manager, Flight Command and Data Management Systems Section



Thomas E. Gindorf
Manager, Reliability Engineering Section



Carl S. Guernsey
Member of Technical Staff, Propulsion Systems Section



Michael C. Lou
Group Supervisor, Applied Mechanics Technologies Section



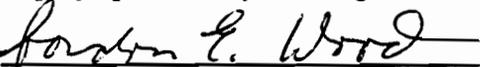
Duncan MacPherson
Consultant



Joseph L. Savino
Division Engineer, Electronics and Control Division



John P. Slonski, Jr.
Deputy Spacecraft System Engineer, Cassini Project



Gordon E. Wood
Member of Technical Staff, Telecommunications Systems Section



Larry W. Wright
Manager, Electronic Parts Reliability Section

ABSTRACT

Launched on September 25, 1992, the Mars Observer spacecraft was to conduct a global survey of the Martian surface and atmosphere. On August 21, 1993, Mars Observer was executing a sequence to pressurize the propulsion tanks in preparation for Mars Orbit Insertion three days later. As part of that sequence, the transmitter was turned off, and no signal has been detected since.

The Deputy Director of the Jet Propulsion Laboratory convened a Special Review Board to thoroughly investigate the causes and ramifications of that failure. The Board concludes that an unrecoverable failure occurred during the 14 minutes when the transmitter was turned off. The four most credible potential causes of the loss of signal are:

- (1) Loss of downlink or destruction of the spacecraft due to a breach of the Propulsion System,
- (2) Electrical power loss due to a massive short in the Power Subsystem,
- (3) Loss of the spacecraft computational function (both spacecraft computers prevented from controlling the spacecraft) in a way that could not be corrected by ground commands, and
- (4) Loss of both transmitters due to failure of an electronic part.

Additional analyses, simulations, and tests underway at press time may affect the relative credibility of these hypotheses.

These most credible potential causes, and the many other hypotheses that the Board examined, are discussed in the report. The report also presents findings, including recommendations that could have been implemented and that might have precluded the failure.

ACKNOWLEDGMENTS

The members of the JPL Special Review Board wish to thank the Mars Observer Project Office and JPL technical staff for their cooperation, perseverance, and dedication in providing briefings and documents, answering questions, and performing tests and analyses in support of the Board's objectives. This includes Martin Marietta Astro Space (Astro) employees who are members of the flight team at JPL in Pasadena, as well as Astro employees and management at East Windsor, New Jersey. We would also like to recognize the cooperation and support provided by the Astro internal failure review board.

CONTENTS

CHAPTER I. EXECUTIVE SUMMARY	1-1
CHAPTER II. INTRODUCTION	2-1
A. Board Charter and Scope	2-1
B. Briefings to the Board	2-1
C. Other Sources of Information.....	2-1
D. Report Organization.....	2-2
CHAPTER III. THE MARS OBSERVER MISSION.....	3-1
CHAPTER IV. DESCRIPTION OF MISHAP AND RECOVERY ACTIONS	4-1
A. Incident and Mishap Reports	4-1
B. Recovery Actions	4-1
C. Observables.....	4-5
1. X-Band Downlink Capability	4-5
2. X-Band Uplink (Command) Capability	4-6
3. Attitude Dynamics Considerations	4-10
4. Summary	4-11
CHAPTER V. SYSTEM AND SUBSYSTEM ANALYSES SUMMARIES	5-1
A. Systems, Test, and Operations	5-1
1. Spacecraft System Description.....	5-1
2. System Single Failure Points	5-2
3. Integration and Test.....	5-5
4. Operations and Sequence of Events	5-10
5. Verification Test Laboratory	5-17
B. Flight and Fault Protection Software	5-21
C. Command and Data Handling Subsystem	5-27
1. Description of Subsystem	5-27
2. Method of Analysis	5-29
3. Potential Failure Modes	5-29
4. Other Comments.....	5-30
D. Redundant Crystal Oscillator.....	5-32
E. Attitude Control	5-35
1. Description of Subsystem	5-35
2. Method of Investigation.....	5-39
3. Potential Failure Modes	5-40
4. How AACS Influences System Response to Other Faults	5-40
F. Power Subsystem Description	5-42
1. Primary Power	5-42
2. Potential "High-Side" Short to Chassis	5-43
3. Previous Power System Failures	5-43

G.	Telecommunications Subsystem	5-44
1.	Transmitting Functions	5-44
2.	Receiving Functions.....	5-45
H.	Propulsion Subsystem	5-46
1.	Description of Subsystem	5-46
2.	Method of Investigation.....	5-46
3.	Potential Failure Modes	5-50
4.	Influences of Propulsion Subsystem on System Response to Other Faults.....	5-50
5.	Fracture Mechanics Design of Bipropellant Tanks	5-50
I.	Structure and Mechanisms	5-54
J.	Electronic, Electrical, and Electromechanical Parts	5-59
1.	The Parts, Materials, and Processes Control Plan for Mars Observer	5-59
2.	Waivers Applicable to EEE Parts.....	5-60
3.	Parts List Review for Single-Event Effects (SEEs).....	5-61
4.	Failure Likelihood of the JANTXV2N3421 in the RXO	5-61
5.	Other Parts Issues	5-62

CHAPTER VI. METHODOLOGY FOR DEVELOPING, CHARACTERIZING, AND ANALYZING HYPOTHESES.....	6-1
A. Hypothesis Generation Methods.....	6-1
1. Board Processes	6-1
2. Fault Trees.....	6-3
B. Categorization of Hypotheses	6-3
1. Degree-of-Causality Method	6-3
2. Contribution-to-Anomaly Method	6-4
C. Candidate Hypotheses for Potential Causes of the Observed Anomaly	6-4

CHAPTER VII. CANDIDATE HYPOTHESES TO EXPLAIN THE LOSS-OF-SIGNAL ANOMALY	7-1
A. Liquid Oxidizer Upstream of Check Valves Causes Damage to the Pressurization System (C1).....	7-1
1. Liquid Oxidizer Upstream of Check Valves Reacts With MMH in Pressurization System (Reaction in Lines; C1A).....	7-1
2. Liquid Oxidizer Upstream of Check Valves Interacts With MMH in Fuel Tank (Reaction in Tank; C1B)	7-3
3. Liquid Oxidizer Upstream of Regulator Causes Impact Damage to Pressurization System ("Liquid Bullet"; C1C)	7-4
B. Burst of Bipropellant Tanks Due to Unregulated Pressure (Regulator Fails Open; C2)	7-5
C. Burst of a Bipropellant Tank With an Initial Flaw During MOI Pressurization (Flaw Bursts Tank; C3A)	7-8

D.	Burst of a Bipropellant Tank During MOI Pressurization After Having Been Weakened by Meteoroid Impact (Meteoroid Damages Tank; C3B)	7-10
E.	Rupture of Tubing During MOI Pressurization (Flaw Ruptures Line; C3C)	7-12
F.	NSI Expelled /Pyro Valve Failure (NSI Impacts Tank; C4)	7-13
G.	CIU Hardware Redundancy Control State Indeterminacy (CIU Indeterminacies; C5)	7-15
	1. SCP In Control (C5A)	7-15
	2. I/O Crossed /Not Crossed (C5B).....	7-18
	3. I/O Bus Select (C5C)	7-20
H.	SCP Software Problem (C6).....	7-21
I.	Miswired Pyros (C7).....	7-23
J.	Sequence Error (C9).....	7-30
K.	Skew RWA Stall (C10).....	7-32
L.	Loss of Exciter Frequency Reference (C11)	7-33
M.	Hardware/Software Conflict Preventing RPA Turn-On (C12)	7-35
N.	RPA Coil Single-Point Failure (RPA Coil Short; C13)	7-36
O.	RPA Overcurrent Detector Prevents Turn-On (RPA Overcurrent Protection C14)	7-39
P.	Erratic Activity on Critical CIU Hardware Interfaces (Erratic CIU Interface; C15)	7-41
Q.	Hardware Failure Preventing RPA Turn-On (RPA Control Failure; C16)	7-43
R.	System Response to Primary-Side Timing Loss (RXO Transistor Failure; S1).....	7-46
S.	Primary Power Failure (Power Loss; S2)	7-50
T.	Erratic RXO Output (S3)	7-54
U.	RPA (TWTA) Cathode Heater Support Failure (RPA Cathode Support Failure; S4).....	7-56
V.	Gyro Spin Motor Short (S5)	7-58
W.	Sun Sensor Head #4 Failure (S6)	7-60
X.	RWA Overspeed (S7).....	7-61
Y.	Meteoroid Impact (N1).....	7-62
Z.	DSN Inability To Detect Existing Downlink (DSN Detection Problems; N3)	7-63
AA.	Multiple Failures (N4).....	7-65
BB.	SEE-Created Problem (N6)	7-68
CC.	+10-Volt Interface Power Failure (N7)	7-70

CHAPTER VIII. ASSESSMENT OF THE HYPOTHESES.....	8-1
A. Hypotheses Summary	8-1
B. Assessment	8-2
C. Tests Performed or in Process	8-4

CHAPTER IX. FINDINGS.....	9-1
A. System Engineering	9-1
B. Propulsion System Pressurization Design.....	9-2
C. Primary Power Subsystem Ground	9-3
D. Fault Protection	9-4
E. Command and Data Handling Subsystem.....	9-5
F. Telecommunications Subsystem	9-7
G. Flight Hardware Heritage.....	9-7
H. Unidentified Single Failure Points (SFPs).....	9-8
CHAPTER X. OBSERVATIONS.....	10-1
I. TECHNICAL OBSERVATIONS	10-1
A. Redundant Crystal Oscillator (RXO).....	10-1
B. Command and Data Handling Subsystem.....	10-2
C. Integration and Test	10-2
D. Sequence	10-2
E. Recovery Operations	10-3
F. Mars Balloon Relay Experiment.....	10-4
II. PROGRAMMATIC OBSERVATIONS	10-5
A. Fixed-Price Contracts.....	10-5
B. Operations	10-5
C. Reliability.....	10-6
D. Documentation and Configuration Control.....	10-6
CHAPTER XI. GLOSSARY	11-1
APPENDIX A BOARD CHARTER AND MEMBERSHIP	A-1
APPENDIX B BRIEFINGS LISTING	B-1
APPENDIX C MO PROJECT INITIATION AGREEMENT	C-1
APPENDIX D JPL CONTRACT TASK ORDER.....	D-1
APPENDIX E ISA FOR LOSS OF SIGNAL	E-1
APPENDIX F MISHAP REPORT	F-1
APPENDIX G CAUSAL FACTOR: PYRO SHOCK.....	G-1
I. Description of Threat.....	G-1
II. Method of Investigation.....	G-2
III. Results of Investigation.....	G-2

APPENDIX H PYRO-INDUCED FAILURE MECHANISMS IN CIU	
HARDWARE	H-1
I. Introduction	H-1
II. Step 1: Squib Transient Current.....	H-2
III. Latch-up in CD4000 Circuits	H-4
IV. Step 2: Energy Coupling Mechanisms	H-8
V. Step 3: Latch-up in Critical CMOS Circuits	H-14
VI. The Magellan Incident	H-16
VII. Summary and Conclusions	H-17
APPENDIX I CAUSAL FACTOR: METEOROIDS	I-1
I. Environment Description	I-1
II. Critical Hardware	I-1
III. Method of Investigation.....	I-2
IV. Limitations of the Analysis.....	I-4
V. Results of the Investigation	I-5
APPENDIX J CAUSAL FACTOR: SINGLE-EVENT EFFECTS	J-1
I. Overview	J-1
II. Introduction	J-1
III. System Overview	J-2
IV. Environment	J-2
V. Calculation of Upset and Latch-up Rates.....	J-4
VI. Summary of SEU and Latch-up Results	J-6
VII. Conclusions.....	J-8
APPENDIX K PROPULSION SYSTEM ANALYSES	K-1
I. NTO Transport Mechanisms.....	K-1
II. Hydrodynamic Impact Damage (“Liquid Bullet”) Mechanisms	K-6
III. NTO/MMH Reactions in the Pressurization System	K-8
APPENDIX L FRACTURE MECHANICS DESIGN OF BIPROPELLANT TANKS	L-1
APPENDIX M MARS OBSERVER APPROVED SFP WAIVER SUMMARY	M-1
APPENDIX N RECOVERY COMMANDS	N-1
APPENDIX O TIME DELAYS TO TRANSFER TO LGA	O-1
APPENDIX P PYRO VALVE FAILURE MODES.....	P-1
I. Cluster Program Failures.....	P-1
II. Mars Observer Pyro Valve Evaluation	P-6

APPENDIX Q	STRUCTURAL ANALYSIS OF MARS OBSERVER TWTA CATHODE HEATER SUPPORT TUBE	Q-1
I.	Introduction	Q-1
II.	Information Gleaned From the Mars Observer TWTA Meeting	Q-1
III.	Analysis of the Cathode Support Tube.....	Q-3
IV.	Summary and Conclusions	Q-3
APPENDIX R	AACS SIMULATIONS	R-1
I.	RWA Overspeed Scenario (S7) Details	R-1
II.	IMU Motor Short Scenario (S5) Details	R-6
APPENDIX S	THE UNITRODE JANTXV2N3421 IN THE MARS OBSERVER RXO.....	S-1
I.	Origin of Concern Over the Unitrode JANTXV2N3421 in the Mars Observer RXO	S-1
II.	Description of the Unitrode JANTXV2N3421.....	S-2
III.	Internal Wire Connections.....	S-2
IV.	Failure Mode Mechanism	S-2
V.	Use of the JANTXV2N3421 in the RXO	S-4
VI.	Probability of Failure of a JANTXV2N3421 in the RXO.....	S-4
VII.	Other Commentary	S-5
APPENDIX T	PRESSURIZATION SEQUENCE.....	T-1
APPENDIX U	MARS BALLOON RELAY BEACON DETECTION CAPABILITY	U-1

TABLES

3-1.	Mars Observer programmatic assumptions versus realities	3-2
3-2.	Mars Observer reviews	3-5
5-1.	System test types	5-8
5-2.	Commands in pressurization block.....	5-11
5-3.	Spacecraft state at start of pressurization block minus 7 seconds	5-12
5-4.	State table for Mars Observer RXO when primary oscillator is selected by CIU	5-33
5-5.	State table for Mars Observer RXO when backup oscillator is selected by CIU	5-34
5-6.	AACS hardware components.....	5-35
5-7.	AACS modes.....	5-35
5-8.	Mars Observer angular velocities for selected scenarios.....	5-41
5-9.	Mars Observer angular velocities at which certain capabilities are lost	5-41
6-1.	Physical changes on the spacecraft during pressurization sequence	6-1
6-2.	Sources of energy on board the spacecraft	6-2
6-3.	Hypothesis categories.....	6-4
6-4.	Candidate hypotheses	6-7
7-1.	First radiated recovery commands	7-59
7-2.	Dual-unit failures creating observed anomaly	7-65
7-3.	Unit FIT estimates	7-66
8-1.	Hypotheses summary.....	8-3
8-2.	Tests performed or in progress.....	8-4
B-1.	Briefings to the Mars Observer Special Review Board	B-1
G-1.	Mars Observer system pyro test firing events, listed by approximate firing order and date.....	G-3
G-2.	Mars Observer flight pyro firing events, listed in firing order, system pyro shock response for information only	G-4
H-1.	Voltage induced by B-field in secondary loops for two distances between primary and secondary loops.....	H-10
H-2.	Single-point failure modes in the CIU module involving CD4000 logic circuits	H-14
H-3.	Logic conditions	H-15

I-1.	Mars Observer cumulative fluence.....	I-2
I-2.	Fluences contributing to weakening of the tank velocity (km/s).....	I-3
J-1.	Distribution of SEE-sensitive parts in Mars Observer subassemblies.....	J-2
J-2.	Maximum LET used for single-event latch-up testing	J-6
J-3.	Calculated soft error rates for various device types	J-7
J-4.	Expected number of soft errors in 14 minutes using upper-bound soft error rates	J-7
J-5.	Expected number of soft errors in 14 minutes using best-estimate soft error rates.....	J-8
M-1.	SFPs addressed in Mars Observer downlink loss-of-signal anomaly	M-2
M-2.	Mars Observer approved SFP waiver summary listing by subsystem	M-3
U-1.	MBR receiving station characteristics	U-1

FIGURES

3-1.	Mars Observer development schedule	3-3
3-2.	Mars Observer organizational roles	3-4
4-1.	DSN events just after onset of anomaly	4-7
4-2.	Time delays to transfer to LGA	4-9
5-1.	Spacecraft functional block diagram	5-3
5-2.	Integration and test flow used for bench-level testing	5-6
5-3.	Integration and test flow used for spacecraft-level testing.....	5-7
5-4.	Depiction of scripts active during T1A phase at the time of the anomaly	5-14
5-5.	Timeline of spacecraft downlink and DSN events.....	5-16
5-6.	VTL block diagram	5-18
5-7.	Flight software task activity block diagram	5-22
5-8.	General REDMAN response block diagram	5-24
5-9.	C&DH block diagram.....	5-28
5-10.	HGA offset from Earth line during pressurization.....	5-37
5-11.	Initial conditions at RPA Beam Off	5-38
5-12.	Monopropellant Subsystem.....	5-47
5-13.	Bipropellant elements.....	5-48
5-14.	Bipropellant tank pressures during launch preparation.....	5-52
5-15.	Bipropellant tank in-flight pressure telemetry data.....	5-53
5-16.	Mars Observer structural configuration	5-55
5-17.	Mars Observer spacecraft in cruise configuration.....	5-56
6-1.	Loss-of-signal fault tree	6-5

7-1.	Regulator schematic.....	7-5
7-2.	Relation of pyro valves to MMH tank.....	7-13
7-3.	Pyro bus Enable and Arm System	7-25
7-4.	Flight pyro harness testing	7-26
7-5.	Solar Array outer cruise position and mapping positions	7-27
7-6.	Solar Array deployed in partial mapping position	7-28
7-7.	Initial condition, both relays are off	7-36
7-8.	Pyro shock leads to internal debris, which leads to short across coil L2-B	7-37
7-9.	Send command to turn RPA-B on	7-38
7-10.	An example of a single-failure point in SCU that inhibits RPA Beam On.....	7-45
7-11.	LGA boresight deviation from the Earth direction	7-48
7-12.	Unfused power schematic.....	7-52
H-1.	Chassis current induced by pyro short	H-2
H-2.	A model of current flow from short in NSI induced by plasma to chassis	H-3
H-3.	Chassis and shield currents created by disruption of the squib bridge wire in laboratory simulation of Magellan hardware. Mars Observer used the same type of squib	H-4
H-4.	Latch-up characteristics of a CD4049 inverter triggered by $V_{DD} - V_{SS}$ breakdown mechanism	H-5
H-5.	Transfer characteristics of a CD4049 inverter	H-7
H-6.	Geometry of primary current loop from battery through chassis when squib shorts to case. Secondary loop geometries are of similar complexity	H-9
H-7.	Culprit and victim loops	H-11
H-8.	Loop-to-loop coupling model for Mars Observer pyro-induced chassis current with culprit details.....	H-12
H-9.	Loop-to-loop coupling model for Mars Observer pyro-induced chassis current with culprit and victim details	H-13
H-10.	SCP in control	H-16
I-1.	Mars Observer cumulative micrometeoroid fluence as a function of mass	I-3
I-2.	Meteoroid fluence for Mars Observer for different velocity bins	I-4
J-1.	Spacecraft block diagram with subsystems containing SEU/latch-up sensitive components.....	J-3
K-1.	Tank temperatures versus time.....	K-2
K-2.	Vapor pressure versus temperature, liquid nitrogen tetroxide.....	K-3
K-3.	Geometry of the Pressurization System upstream of the regulator	K-7
K-4.	Effects of blowdown of the helium tank.....	K-9

K-5.	Pressurization System plumbing layout.....	K-11
K-6.	Estimated pressure in filter FG-2 (reactants are 2.2 g NTO and 0.1 g MMH)	K-12
K-7.	Estimated line pressures for the oxidizer-to-fuel ratio = 2.5 reaction at "T" (reactants are 2.2 g NTO and 0.9 g MMH).....	K-12
K-8	Estimated line pressures for the oxidizer-to-fuel ratio = 1 reaction at "T"(reactants are 2.2 g NTO and 2.2 g MMH).....	K-14
P-1.	Detail of the thread of the passive initiator, showing erosion damage to the Ti-alloy thread and to the Inconel 718 thread	P-2
P-2.	Detail of eroded initiator and housing threads. In every case, the Ti-alloy thread is eroded at the top of a tooth and the Inconel at the opposite side at the root of the thread. Firing residue can be seen between the threads	P-2
P-3.	Pressure history from simulated pyro firing valve	P-4
P-4.	Pressure history from simulated pyro valve firing #2 using OEA initiators	P-5
P-5.	X-rays of pyro valves fired in Mars Observer pyro shock tests	P-7
Q-1.	Mars Observer TWT cathode and support structure.....	Q-2
Q-2.	Mars Observer TWT cathode mounting configuration	Q-2
R-1.	RWA S uncontrolled spin-up to 9000 rpm	R-2
R-2.	RWA X uncontrolled spin-up to 9000 rpm.....	R-3
R-3.	RWA Y uncontrolled spin-up to 9000 rpm.....	R-4
R-4.	RWA Z uncontrolled spin-up to 9000 rpm.....	R-5
R-5.	IMU spin motor short, RWAs at +6500, -6500, -6500 rpm (X, Y, Z, respectively).....	R-7
R-6.	IMU spin motor short, RWAs at +6500, -6500, +6500 rpm (X, Y, Z, respectively).....	R-8
R-7.	IMU spin motor short, RWAs at -6500, -6500, +6500 rpm (X, Y, Z, respectively).....	R-9
R-8.	IMU spin motor short, RWAs at -6500, -6500, -6500 rpm (X, Y, Z, respectively).....	R-10
S-1.	Probability of failure of a JANTXV2N3421 in the RXO.....	S-6

CHAPTER I

EXECUTIVE SUMMARY

Shortly after the Mars Observer (MO) loss-of-signal anomaly on August 21, 1993, the Deputy Director of the Jet Propulsion Laboratory (JPL) convened a Special Review Board to determine the most likely cause(s) of the failure and to recommend steps that could have or should have been taken to prevent this event. A 12-member Review Board was established and held its first meeting on September 1, 1993.

As the spacecraft approached Mars, it was necessary to repressurize the propellant tanks. This sequence occurred at Mars Orbit Insertion (MOI) minus 3 days and was scheduled to last 14 minutes. Prior to the sequence, the spacecraft had been operating normally, and there were no indications of any component degradation or imminent failure. The pressurization sequence involved turning off the transmitter, putting the Attitude Control System in Deploy Control (drift) mode, spinning up a redundant reaction wheel, firing 2 pyro valves to pressurize the propellant tanks, returning the Attitude Control System to normal cruise mode, and turning the transmitter back on. This was not anticipated to be a difficult or risky sequence. Unfortunately, the spacecraft signal has not since been received.

There was no direct observation of the spacecraft at the exact time of failure because the Mars Observer spacecraft transmitter was deliberately turned off during the pressurization sequence. This was done because the Traveling Wave Tube (TWT) had not been qualified to survive the pyro valve shock (that was part of the sequence) when turned on (hot).

Analysis of this anomaly was especially difficult because of the paucity of available diagnostic information. However, there are some in-flight observables of the system: a downlink carrier was never detected from the spacecraft's High-Gain Antenna (HGA) or the Low-Gain Antenna (LGA) after the anomaly. Also, the myriad recovery commands that were sent did not re-establish either of the downlink signals.

One of the first actions of the Board was to investigate whether a signal would have been detected if the spacecraft had been transmitting. There could have been problems with the Deep Space Network (DSN) ground receiving stations, or the spacecraft could have been at an attitude or attitude rate where the receiving stations could not receive its carrier for a long enough time for detection, or there may not have been enough time for the uplink commands to have been successfully received by the spacecraft.

As the Board's inquiries and analysis progressed, confidence developed that if the spacecraft had been capable of transmitting, one or more of the downlink carriers should have been detected, and at least some of the repetitively sent uplink commands should have been received by the spacecraft. For some of the failure scenarios, the spacecraft attitude would return to normal, the HGA would point at the Earth, and the downlink should have been established at the predicted time. For other scenarios, the attitude would be corrupted or drifting, and, in those cases, in order of likelihood: the

receiving stations should have detected a downlink signal from the LGA, established an uplink over one of two receiving LGAs, and finally detected a downlink on the HGA.

The members of the Mars Observer Special Review Board now conclude that the failure of the spacecraft was caused by an unrecoverable failure that occurred during the 14 minutes when the transmitter was turned off. The four most credible potential causes of the loss of signal are:

- (1) Loss of downlink or destruction of the spacecraft due to a breach of the Propulsion System (See the discussion of Hypotheses C1, C2, and C4 in Chapter VII.)
- (2) Electrical power loss due to a massive short in the Power Subsystem (See the discussion of Hypothesis S2 in Chapter VII.)
- (3) Loss of the spacecraft computational function (both spacecraft computers prevented from controlling the spacecraft) in a way that could not be corrected by ground commands (See the discussion of Hypothesis C5 in Chapter VII.)
- (4) Loss of both transmitters due to failure of an electronic part (See the discussion of Hypothesis C16 in Chapter VII.)

Additional analyses, simulations, and tests are in progress that may produce information which could affect the relative credibility of these hypotheses.

These most credible potential causes, and the many other hypotheses that the Board examined, are discussed in the report that follows. The report then presents findings which include recommendations that could have been implemented on Mars Observer, and might have precluded the failure. However, it is recognized that some of these recommended actions that could have been taken might not have been taken for programmatic reasons even if they had been proposed during development; this is particularly true of the Mars Observer Project, which emphasized maximum use of industry design and production practices.

CHAPTER II

INTRODUCTION

A. Board Charter and Scope

The Special Review Board for the Mars Observer Loss-of-Signal Anomaly was appointed by the Deputy Director of the Jet Propulsion Laboratory on August 30, 1993. The memorandum chartering the Board appears in Appendix A.

The Review Board charter is to:

- (1) Ascertain the most likely cause(s) of the Mars Observer loss of signal, considering all relevant design, fabrication, test, and mission operations data.
- (2) Recommend steps that could have or should have been taken to prevent this event.

The Review Board was also instructed to cooperate with other review boards, such as the NASA Failure Review Board, in order to minimize duplication of effort, but still maintain the independence of each board.

B. Briefings to the Board

Briefings to the Review Board were given by the Mars Observer Project Office; their JPL technical support organizations; their prime contractor, Martin Marietta Astro Space (Astro) in East Windsor, New Jersey; and selected subcontractors. A chronological listing of these meetings is presented in Appendix B.

C. Other Sources of Information

In the course of deliberations and identification of potential hypotheses, many specific topics for review and analysis were pursued by this Review Board and supported by the JPL Technical Divisions and the Mars Observer Project Office. These actions resulted in both reports and presentations to this Board. In some areas (such as pyro shock, propulsion, and power), specific hardware tests were scheduled (and some completed during the tenure of the Board) at JPL, the USAF Phillips Laboratory, and at Astro. In other areas, such as the Command and Data Handling (C&DH) and Attitude and Articulation Control (AACS) Subsystems, simulations and tests were run in the Verification Test Laboratory (VTL) at JPL.

In addition to analyses and tests, a comprehensive library of applicable Mars Observer documentation was assembled and reviewed by members of the Review Board. These documents included presentation and disposition material from Project-level and lower-level reviews, problem failure reports (PFRs), waivers, risk analyses, and interoffice memoranda.

In order to focus on specific subsystems or topics, teams (of one or two people) were formed within the Review Board, and the pertinent information from those reviews is included in this report.

An interface was created between the JPL Board and the board appointed by NASA headquarters. The JPL Review Board chairman attended a preliminary kick-off meeting at the Naval Research Laboratory (NRL), gave a status report to that board on September 30, and a final presentation on November 10. In addition, the NASA Board had six subsystem teams, each with a JPL representative from the Mars Observer Project providing support and information.

D. Report Organization

Chapter III gives a brief history of the Observer Program and the Mars Observer Project to provide a framework or context for the reader.

Chapter IV describes the mishap, summarizes the attempts to re-establish communication with the spacecraft, and explains the "observables," i.e., what is actually known about the spacecraft and what one can infer from the lack of success in recovering its signal.

Chapter V is tutorial in nature and describes the spacecraft system and its major subsystems. It provides the technical reader with the background, terminology, and detail to understand the discussion of the failure hypotheses in Chapter VII. It also explains the examination the Board made of the various subsystems in the search for possible failure modes. The general reader may wish to skip this chapter or refer to specific sections, as desired.

Chapter VI explains how the Board developed, categorized, and screened the hypotheses for the failure. A complete list of the hypotheses considered by the Board appears in Table 6-4 and can be used as a guide to sections the reader may wish to study in Chapter VII.

Chapter VII contains the hypotheses in an arbitrary order. It is not intended to be read as a novel; the Board suggests that the reader browse.

Chapter VIII summarizes all the hypotheses and indicates the Board's consensus categorization. The hypotheses in Category A are considered to be the most credible potential causes of the Mars Observer failure.

Chapter IX contains the Board's findings. These are referenced to the hypotheses, and recommendations are offered as to what could have been done (by the Project) or which could be done (for future projects) to avoid or minimize the risk from these potential causes of the failure.

Chapter X contains the Board's observations. These are items which are thought to be incidental to the actual cause of the failure but are weaknesses or concerns worth noting for future planetary projects.

CHAPTER III

THE MARS OBSERVER MISSION

The Mars Observer mission was recommended and developed by the Solar System Exploration Committee (SSEC) of the NASA Advisory Council from 1981–1983. Mars Observer was one in a series of robotic spacecraft missions to Mars, which began in 1964 with Mariner 4 and continued through the spectacular Viking missions of the late 1970's. Mars was selected by the SSEC as the highest priority planet for global scientific characterization. The Mars Observer spacecraft, orbit, and instruments were designed to maximize scientific return within a modest cost framework. Launched from the Kennedy Space Center in Florida on September 25, 1992, Mars Observer was the United States' first return to Mars in 17 years.

Originally called the Mars Geoscience/Climatology Orbiter to emphasize geology, geophysics, and climatology, the spacecraft was later renamed Mars Observer, although the global science objectives remained the same:

- (1) To determine the global, elemental, and mineralogical character of the surface material
- (2) To define globally the topography and gravitational field
- (3) To establish the nature of the magnetic field
- (4) To determine the time and space distribution, abundance, sources, and sinks of volatile material and dust over a seasonal cycle
- (5) To explore the structure and aspects of the circulation of the atmosphere

Mars Observer was to conduct a global survey of the planet's atmosphere and surface and monitor changes over the course of a Martian year (687 Earth days). Mars Observer was expected to provide a greatly improved perspective for planning future missions to Mars. This composite perspective of Mars would have been similar to the unprecedented perspective of the Earth that has been assembled from Earth-orbiting satellites, such as Landsat.

Project History

With the advice of SSEC, NASA developed a Planetary Observer program concept consisting of a series of low-cost, scientifically focused missions, and selected the first two missions: the Mars Geoscience Climatology Orbiter (MGCO) and Lunar Geoscience Orbiter (the Lunar Geoscience Orbiter was not approved). (The Project Initiation Agreement of November 1983 and the JPL Contract Task Order are included in Appendices C and D, respectively.) Congress approved the Mars Observer Project as a new start in fiscal year 1985. (For more detail on the early Mars Observer history refer to the study performed by Charles Polk.¹ This study

¹C. Polk, *Mars Observer Project History*, JPL Document 8095, Jet Propulsion Laboratory, Pasadena, California, December 1990.

addresses the progression of programmatic decisions and possible consequences for the Mars Observer Project.)

As part of the Planetary Observer mission concept, Mars Observer had basic programmatic assumptions that were altered by the realities of the Project implementation. A comparison of basic Mars Observer assumptions and how they relate to reality is presented in Table 3-1. It is clear that the realities of the implementation shifted from the baseline against which the Project was originally costed and scheduled. One of the most significant decisions in the Mars Observer history was the deletion of the integrated payload module. The payload module concept was developed to simplify and control interfaces with the spacecraft to minimize spacecraft design changes. A summary of the Mars Observer schedule is shown in Figure 3-1.

The Mars Observer spacecraft design was based upon communication and meteorological satellites that routinely circle the Earth. A mission ground rule was that maximum inheritance of the manufacturer's production capability should be retained. The spacecraft was designed and assembled under contract from JPL to RCA Astro, East Windsor, New Jersey. RCA was subsequently acquired by General Electric and became the GE AstroSpace Division. (This Division has recently been acquired by Martin Marietta.) The spacecraft was initially planned to be launched from the Space Shuttle, using an integral propulsion module. Later it was decided to develop a new upper stage for this series of missions, which was also thought to have commercial potential. This new stage is the Transfer Orbit Stage (TOS), which was built by Martin Marietta under contract to Orbital Science Corporation. A summary chart of Project responsibilities is depicted in Figure 3-2.

Table 3-1. Mars Observer programmatic assumptions versus realities.

Assumption	Realities
Focused science	Added imaging; payload used all spacecraft resources—no margins remained
Simple inherited instruments	High-heritage instruments unavailable
Experienced principal investigators	Several first-time investigators
Inherited Earth orbital spacecraft with minimal modifications	Design modified for more complex payload
Maximum use of contractor inheritances (hardware, personnel, procedures, and product assurance)	Changes to improve reliability; inheritance was violated
Spacecraft selection before instruments to "bound" and define interfaces	Instruments selected before spacecraft; payload module deleted (before spacecraft Request For Proposal released)
First in an "explorer-like" line item	Mars Observer is the only Planetary Observer spacecraft
Stable funding environment	Funding significantly reduced following Challenger accident

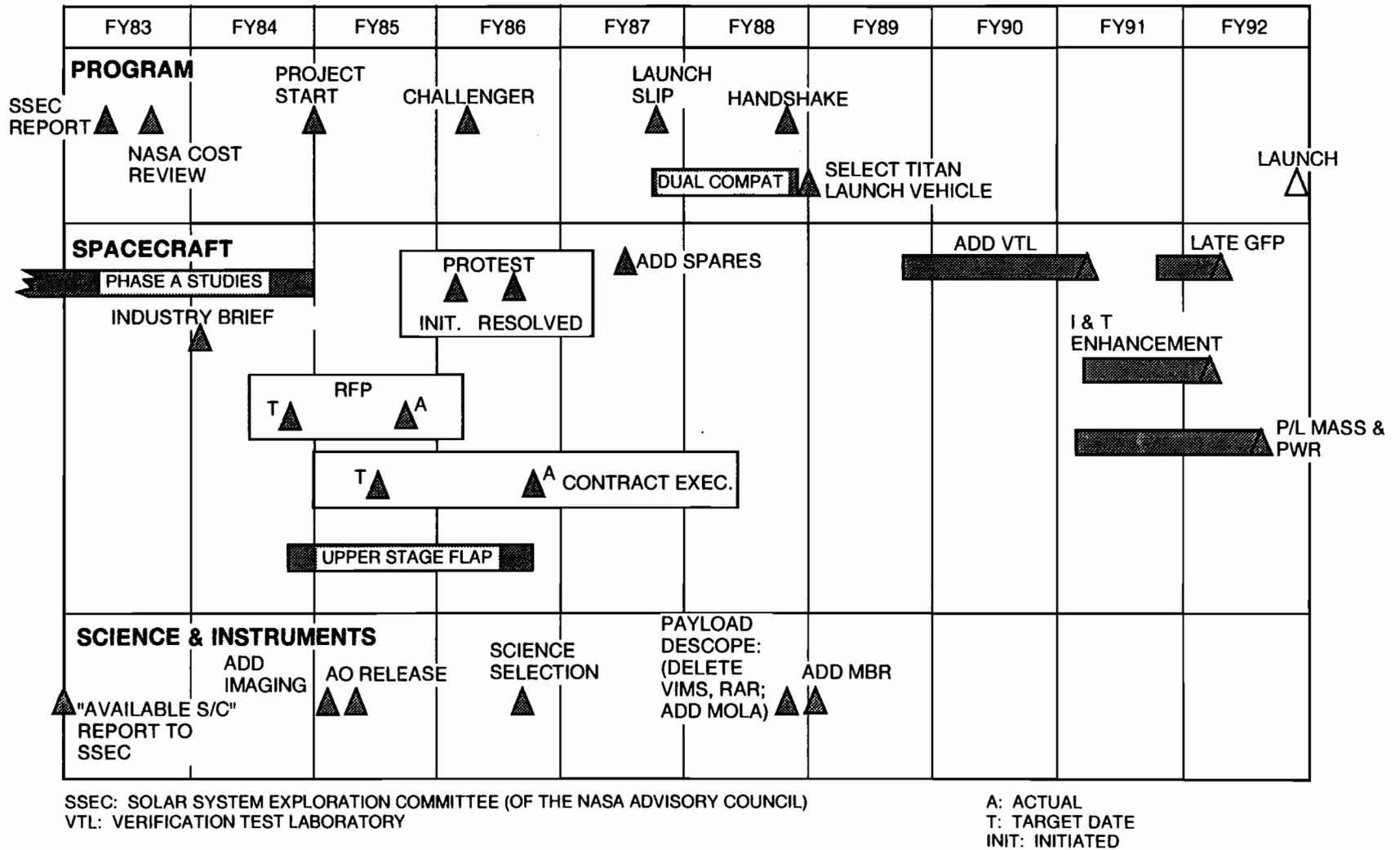


Figure 3-1. Mars Observer development schedule.

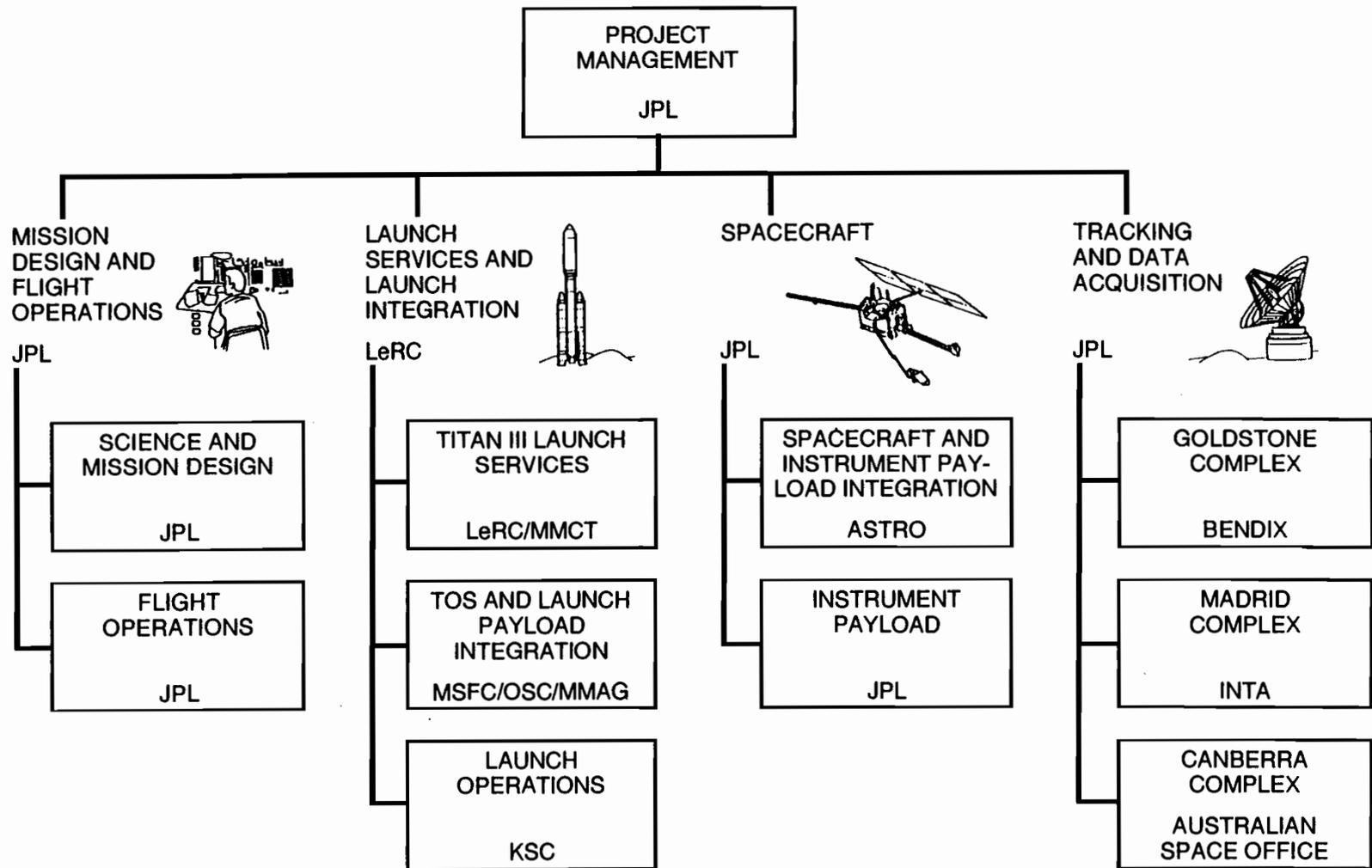


Figure 3-2. Mars Observer organizational roles.

The Challenger accident in January 1986 caused uncertainty as to whether (and when) the Shuttle would be available for launches. For about one year, the spacecraft had to be compatible with both the Shuttle/TOS and the Titan III/TOS. Finally, consideration of the Shuttle was dropped and the Titan III option was selected. On September 25, 1992, Mars Observer was launched to Earth orbit aboard an expendable Titan III rocket, provided by the Martin Marietta Aerospace Group, and then was boosted out of Earth orbit into interplanetary space by the first TOS.

During the course of the Project, a review program was conducted with technical and management personnel. The system-level review program is summarized in Table 3-2. These reviews were supplemented by the numerous subsystem-level preliminary and critical design reviews.

In late July 1993, 5.8 million kilometers (3.6 million miles) and 28 days from its encounter with Mars, the spacecraft was oriented to acquire its first image of the planet. Upon examining the image, scientists proclaimed that the atmosphere was clearer than it had been during any other mission, boding well for the mapping images to follow in the orbital phase.

Mars Observer was to arrive at Mars on August 24, 1993, at approximately 1:42 p.m. Pacific Daylight Time (PDT), when it would fire its 490-N engines to slow its speed and allow it to be captured into orbit around the Red Planet. The 28-min 50-s burn, delivering a velocity change of 761.7 m/s, would place the spacecraft in a 75-hour capture orbit around Mars, with a closest nominal approach of 3950 km at periapsis. Over a period of 3 months, the spacecraft's orbit was to be moved closer to the planet, transferring it from the initial 3-day elliptical capture orbit to a final near-circular 2-hour mapping orbit. The orbit would then be frozen in a Sun-

Table 3-2. Mars Observer reviews.

Review	Date
Spacecraft System Preliminary Design Review	12/86
Mission System Preliminary Design Review	2/87
Mars Observer 1992 Mission Re-Plan Review	7/87
Mission System Δ Preliminary Design Review	2/89
Spacecraft System Δ Preliminary Design Review	3/89
Preliminary Mission and System Review	5/89
Mission System Flight Sequence Critical Design Review	10/89
Spacecraft System Critical Design Review	3/90
Mission System Critical Design Review—Launch	10/90
Final Mission and System Review	1/91
System Test Readiness Review	3/91
Fault Protection and Operability Review ²	5/91
Mission System Critical Design Review—Encounter	12/91
Preship Review	6/92
MOS Launch Readiness Review	7/92
Launch Readiness Review	9/92
Mission Readiness Review	9/92

²C. Jones, *Mars Observer Flight Software Fault Protection and Operability Review Board Report*, JPL Interoffice Memorandum CC-CPJ-08-91, Jet Propulsion Laboratory, Pasadena, California, June 3, 1991.

synchronous 2 p.m. orbit that would provide the best lighting conditions for the mapping images. In December 1993, Mars Observer's seven science instruments would begin mapping the planet from an average altitude of 400 km.

About 68 hours before (and to support) the Mars orbit insertion maneuver, the spacecraft's transmitter was turned off in preparation for pressurizing the Propulsion System. (Pressurization is accomplished by releasing high-pressure helium through pyrotechnic valves into the NTO and MMH tanks.) After this event, at about 6 p.m. PDT on August 21, 1993, communications could not be regained with Mars Observer.

Mission operations for the Mars Observer Project were conducted at the Jet Propulsion Laboratory in Pasadena, California.

CHAPTER IV

DESCRIPTION OF MISHAP AND RECOVERY ACTIONS

A. Incident and Mishap Reports

On August 21, 1993, at 17:54 PDT,¹ after a planned 14-minute telemetry outage, the radio frequency (RF) signal from the Mars Observer spacecraft was not reacquired. The spacecraft operations team initiated an Incident/Surprise/Anomaly (ISA) report (Appendix E) to document this occurrence. On September 1, following 11 days of unsuccessful ground-based recovery activities, a Mishap Report (Appendix F) was filed with NASA Headquarters.

At the time of the anomaly, the spacecraft was executing a propellant pressurization sequence and was less than three days from its planned Mars Orbit Insertion (MOI). The pressurization sequence comprises the following functions (see Chapter V.A.4, Operations and Sequence of Events, for more details):

- (1) The active transmitter and its cathode heater ("filament") were turned off, along with the cathode heater of the nonactive transmitter;
- (2) The attitude control mode was set to "Deploy Control";
- (3) Two pyro-activated pressurant valves were fired on 5-minute centers to sequentially pressurize the oxidizer and fuel tanks;
- (4) The attitude control mode was returned to normal cruise control; and
- (5) The previously active transmitter was turned on.

One-and-a-half hours later, following unsuccessful signal acquisition attempts by multiple DSN tracking sites, a spacecraft emergency was declared.

B. Recovery Actions

A detailed list of all recovery commands transmitted to the spacecraft prior to September 22 is contained in Appendix N. The following listing functionally describes the commands that were sent to try to recover the downlink signal. Times shown are in UTC (Coordinated Universal Time) and are preceded by the day of year. (Day 234 was August 22, 1993; and PDT is 7 hours behind UTC.)

- | | |
|----------|--|
| 234/0509 | RPA Beam On commands sent six times each at the emergency (7.8 bps) and nominal (125 bps) rates. |
| 234/0819 | Go to Contingency Mode commands sent once each at the emergency and nominal rates. |
| 234/0945 | Commanding was initiated, but not completed, to stop the backup pyro valve open sequence about to execute on the spacecraft. The only command radiated was to change the Command Detector Unit 1 |

¹Day 234, 0054 UTC.

- (CDU 1) rate from 7.8 to 62.5 bps, the lowest rate for which the prebuilt “stop script” commands had been constructed. The remaining commands were aborted because they would not have reached the spacecraft in time.
- 234/1154 RPA Beam On and Go to Contingency Mode commands were resumed at 7.8 bps, but these would have had no effect if the previous command had been received since the spacecraft CDUs were set to 62.5 and 125 bps, respectively.
- 234/2037 CDUs 1 and 2 commanded to the 7.8 bps rate using uplink transmissions at 62.5 and 7.8 bps.
- 235/0009 Standard Control Processor (SCP)–processed discrete commands were transmitted to attempt to turn on first one and then the other RPA, using the HGA and then the LGA for downlink. Previous RPA Beam On commands had been SCP-processed software commands.²
- 235/1345 Commands initiated to begin methodically selecting telecommunications equipment in combinations of prime and backup units. This commanding began by repeating the Exciter-1/RPA-1/LGA and Exciter-2/RPA-2/LGA combinations before it was interrupted. As other strategies were developed, this methodical selection of various telecommunications combinations was interrupted and restarted several times.
- 235/2239 Backup Redundant Crystal Oscillator (RXO) Select commands, followed by RPA Beam On commands, sent multiple times.
- 236/0351 Engineering Data Formatter (EDF) Reset commands followed by RPA Beam On and Backup RXO Select commands.
- 236/0645 SCP-2 Control Select commands, followed by RPA Beam On commands, sent multiple times.
- 236/1030 Go to Array Normal Spin attitude control mode commands sent twice. This commanding was to recover from a three-failure scenario in which an attitude knowledge fault triggered the Contingency Mode, but in which RPA 1 had failed due to pyro shock and an RF switch failure (latent) prevented RPA 2 from being connected to the LGA. In this scenario, the spacecraft was transmitting over the HGA pointed at the Sun. The Array Normal Spin command would reorient the HGA to the Earth. Also, this command set contained commands to arm the Contingency Mode to enable it to be entered a second time, if necessary.
- 236/1315 Command Sun-Star-Init and Backup Pressurization Sequence initiation to place the spacecraft in the best posture for Mars orbit insertion (MOI), assuming the spacecraft had an unresolved downlink problem and its

² Commands sent to the Mars Observer spacecraft are of three types: (1) control interface unit [CIU] hardware commands, decoded by hardware logic in the CIU; (2) SCP discrete commands, decoded by SCP software and which perform a single definitive action; and (3) SCP software commands, high-level commands expanded by SCP software into a sequence of discrete commands, some of which are defined after the software evaluates spacecraft telemetry or the current prime status of redundant equipment.

- MOI sequence was going to execute as planned, but would execute from SCP-2.
- 236/1601 Beginning of an 8.5-hour command moratorium to avoid potential interference with the MOI sequence.
- 237/0034 Commands sent two times to select backup units for RXO, Clock Divider, I/O Bus, and SCP. The Clock Divider and I/O Bus commands were new, while the RXO and SCP Select commands were redundant to previous commands. In addition, spacecraft time in the EDF and SCP was set to the current time, and the star identification process was initiated.
- 237/0117 The methodical selection of combinations of telecommunications hardware was reinitiated. Exciter 2 was selected with RPA 1, and vice versa, while transmitting through the LGA. In addition, the Exciter-1/RPA-1 path via the HGA was commanded.
- 237/2204 Commands were sent to coordinate with, and possibly aid, the command loss time-out response that would have occurred if no commands had been received since the last known successful command transmitted at 232/2118. These commands were RPA Beam On, and Arm and Go Contingency Mode.
- 238/0203 Commands sent to set the outer cruise mission phase-latching relay to ensure that it was in the correct position. Testing in the ground VTL had indicated a problem potentially related to the state of the mission phase relays after a power on reset (POR). (It was not established that this actually was a problem, and it may have only been due to VTL initialization.)
- 238/0413 The methodical selection of telecommunications hardware combinations was reinitiated: Exciter 2 was selected with RPA 1, with downlink over the LGA.
- 238/0650 Commands sent to Arm Contingency Mode and initiate Array Normal Spin. (This was redundant to previous commanding.)
- 238/0737 Continuation of telecommunications hardware cycling: Exciter 1 was selected with RPA 2, with downlink over the LGA.
- 238/2200 RPA Beam On commands sent 10 times to the spacecraft location if MOI had not occurred, and 10 times to the location if MOI had been accomplished.
- 239/0529 Commands transmitted to put SCP-1 into Safe Mode, i.e., operating from its ROM code. SCP-1 power was cycled off and on, after which SCP-1 was put in control. These commands were sent multiple times to the flyby and Mars orbit positions.
- 242/0332 EDF Reset command transmitted, followed by RPA Beam On commands, on the theory that the SCP-1 was in Safe Mode but that the EDF was anomalous and preventing SCP-1 from executing the RPA Beam On command. These commands were sent once each to the flyby and Mars orbit positions.

- 242/1108 Start of 8-day, 10-hour command moratorium to allow the Command Loss Timer (CLT) to expire without potential restarts due to ground commanding.
- 250/2112 Command sequence to turn off SCP-1 (to remove possibility of SCP-1 and SCP-2 being simultaneously selected for control in the CIU), initiate Contingency Mode, and turn on the RPA Beam. The sequence was sent to the flyby position and consisted of the following commands:
RPA Beam On
SCP-1 Off and Go to Contingency Mode (sent multiple times at 7.8, 62.5, and 125 bps)
RPA Beam On (sent multiple times)
SCP-1 On and Select SCP-1 (sent multiple times)
- 252/0359 Repeat of the above sequence, transmitting to the Mars orbit position.
- 253/0436 Command sequence to disable RPA protection circuits: filament timer, helix overcurrent protection, and input power protection; command the RPA beam on; and re-enable the protection circuits. Each command was sent multiple times. The sequence was sent to the Mars orbit position.
- 253/1152 Repeat of the above sequence, transmitting to the flyby position.
- 257/2312 Command sequence to force the RXO to primary (to address a three-fault scenario where the backup side of the RXO failed, the primary side was acceptable but the switch-back logic had also failed), put SCP-1 into Safe Mode, and command the RPA beam on. Commands in the sequence were sent multiple times. The sequence was sent to the Mars orbit position.
- 258/1652 Repeat of the above sequence, transmitting to the flyby position.
- 260/0942 Command sequence to select Clock Divider 2, reset the EDF, and command the RPA beam on. Commands in the sequence were sent multiple times. The sequence was sent only to the flyby position, under the assumption that if the prime output of the RXO and/or Clock Divider 1 had gone away, MOI would not have taken place.
- 265/0220 Mars Balloon Relay (MBR) beacon transmitter commanded on (sent to determine if the lack of downlink was due only to failures in the downlink elements of the Telecom Subsystem). These commands were sent 83 times over a 7-day period, some to the Mars orbit position and some to the flyby position. NOTE: These commands had no effect, assuming that the previous commanding, beginning at 239/0529, successfully put SCP-1 into Safe Mode and in control. These MBR commands are not recognized when a SCP is operating with ROM code, which it does in Safe Mode.

Subsequent commanding through day 282 consisted of repetitions of previously sent commands to select Clock Divider 2, reset the EDF, and command the RPA beam on. From day 284 through day 302, these same commands were sent, along with commands to cycle SCP-1 power off/on and put SCP-1 in control, and commands to reconfigure the RF output switch.

Commanding from day 310 through 320 was intended to select the backup inertial measurement unit (IMU), set the catalyst bed warm-up time to zero, select Clock Divider 2, and select the backup mode controller in the Power Subsystem.

Subsequently, beginning on day 324, commands were sent to put SCP-2 into Safe Mode via power cycling and then put it in control. Commanding was also planned to repeat the MBR beacon transmitter turn-on sequence, this time using Preset I/O Logical commands, which can be used to produce the effect of the original MBR commands even when a SCP is operating in Safe Mode.

C. Observables

Analyses of this loss-of-signal anomaly are complicated by a complete lack of telemetry data. The primary observables are the apparent absence of any X-band downlink and the completely unsuccessful attempts to restore a downlink by use of ground commands described above.

This situation leads to legitimate questions about the ability to detect a weak or variable signal had one been present. What conclusions can be reached about the spacecraft attitude? Could the uplink commands have been successful even if the downlink was undetectable or missing?

To answer these questions requires communications link analyses with varying assumptions about spacecraft attitude and rates, coupled with ground-based actions to detect transient weak signals. A summary of such analyses is presented below. Refer to the timeline of Figure 4-1 for the correct juxtaposition of ground events.

1. X-Band Downlink Capability

The Mars Observer spacecraft may transmit a downlink at X-band through either a high-gain antenna (HGA) or a low-gain antenna (LGA).

The HGA is a 1.5-meter-diameter parabola with a Cassegrain feed and provides a nominal effective isotropic radiated power (EIRP) of about +83.2 dBm. The HGA is nominally boresighted on the +Y-axis of the spacecraft. Measurements from earlier in the mission indicate that the actual boresight was offset from the +Y-axis by 1.1° in the -X direction. The half-power beamwidth of the HGA is about 1.6° at the downlink X-band frequency.

The LGA is a choked, circular waveguide antenna that produces a broad beam centered at 30° from the +Y-axis in the +Z direction. The nominal EIRP of the LGA is +51.8 dBm with a half-power beamwidth of about 100°. The LGA provides useful coverage at angles up to 80° off boresight. The circumstances and associated times for which the LGA would be selected are shown in Figure 4-2 and are described in Appendix O.

At Earth, the DSN provides receiving terminals with 34-meter-diameter high-efficiency antennas. In addition, 70-meter-diameter antennas can be provided when required for special sequences or weak signal conditions. The application of these two types of antennas is shown in Figure 4-1 for the period just following onset of the anomaly. The noise temperatures of both antenna types are similar and vary moderately with elevation angle. For the link analyses herein, an X-band noise temperature of 20 K is assumed.

Normally the HGA is pointed close to the Earth line. When using the closed-loop receivers of the DSN, the receiving system is able to maintain lock for pointing errors up to about 4 degrees for signal levels prevailing at this time in the mission. When communications are required with greater pointing errors, the LGA would ordinarily be selected.

For very weak signals, detectability depends on special receiving apparatus and the operator's skill. The most sensitive detection equipment routinely available at the DSN complexes is at the spectral signal indicator (SSI). When the SSI is properly used, a signal present with a *carrier-power-to-noise-spectral-density* ratio of at least +10 dB·Hz should be readily visible if the signal persists for at least 10 seconds. This threshold of detectability can vary over a significant range, depending on the configuration of the SSI. During the search for the Mars Observer signal, the SSI was configured such that the threshold was usually in a range of ± 5 dB from the value above.

If the HGA is selected, and the pointing errors are very large, then the downlink performance is dominated by spillover of the primary feed pattern past the subreflector. If the SSI is utilized as described above, then the *presence* of an X-band downlink should have been detectable for pointing errors up to 28 degrees (33 degrees) for a 34-meter (70-meter) station if the signal persists above 10 dB·Hz for at least 10 seconds. For greater pointing errors, the required persistence time increases rapidly with signal detection becoming increasingly unlikely.

Conditions under which the LGA would have been selected are shown in Figure 4-2. Fault protection actions of Contingency Mode and Safe Mode are described in Chapter V.B. If the LGA is selected, the tolerable pointing errors are much larger. Utilizing the SSI, an X-band downlink is readily detectable for LGA pointing errors up to 80° (90°) for a 34-meter (70-meter) station. Obstruction by the spacecraft structure becomes problematic for large pointing errors with the LGA.

2. X-Band Uplink (Command) Capability

The DSN is capable of commanding Mars Observer via the 34-meter high-efficiency subnet only. The maximum uplink power is 18 kW (total), which is divided between carrier and command data in an optimum fashion. The 70-meter antennas have no capability for X-band command transmission. Commanding is possible only when the spacecraft has successfully acquired an uplink carrier and the uplink data rate is set to match that of the Command Detector Unit (CDU) in the spacecraft.

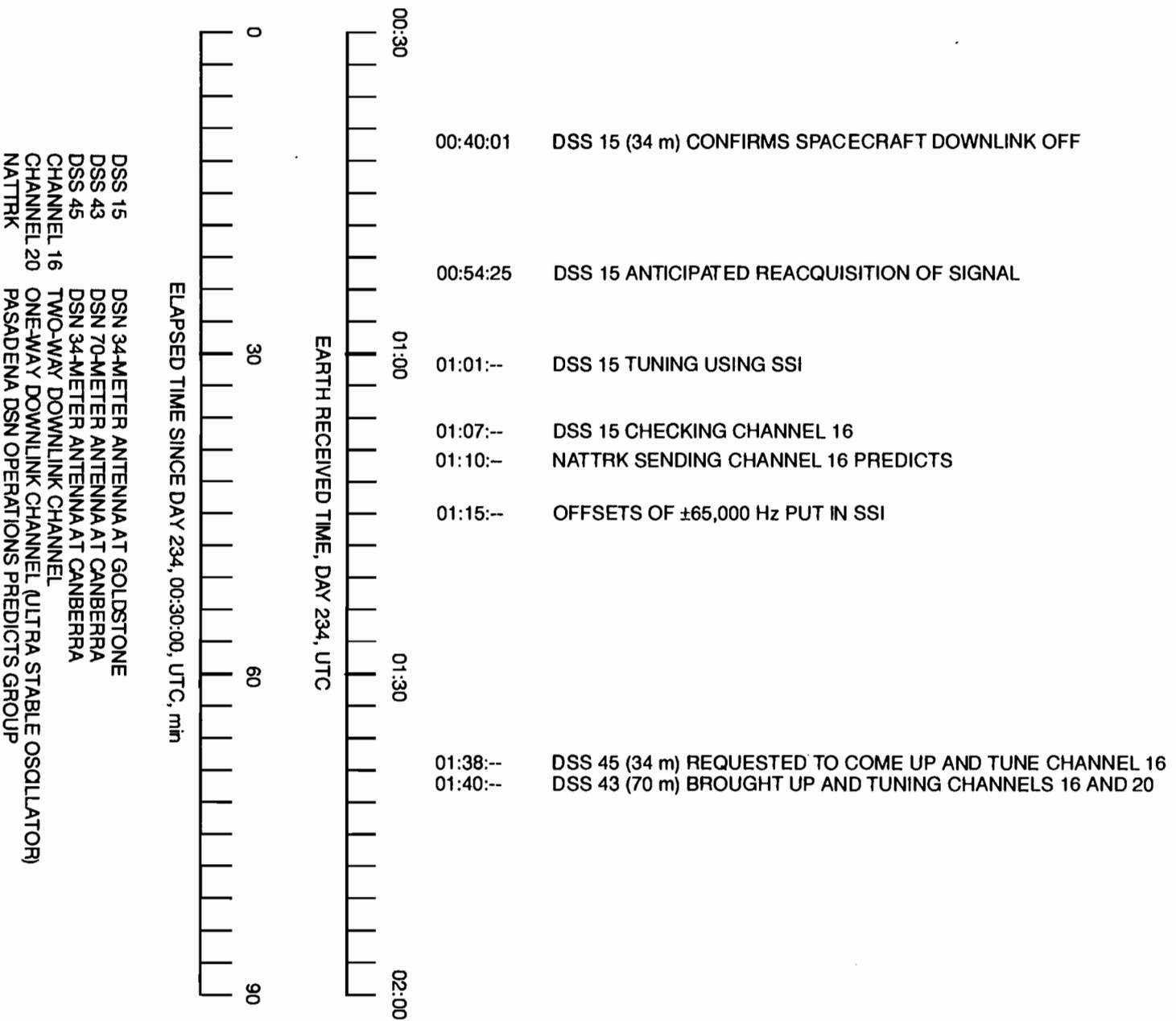


Figure 4-1. DSN events just after onset of anomaly.

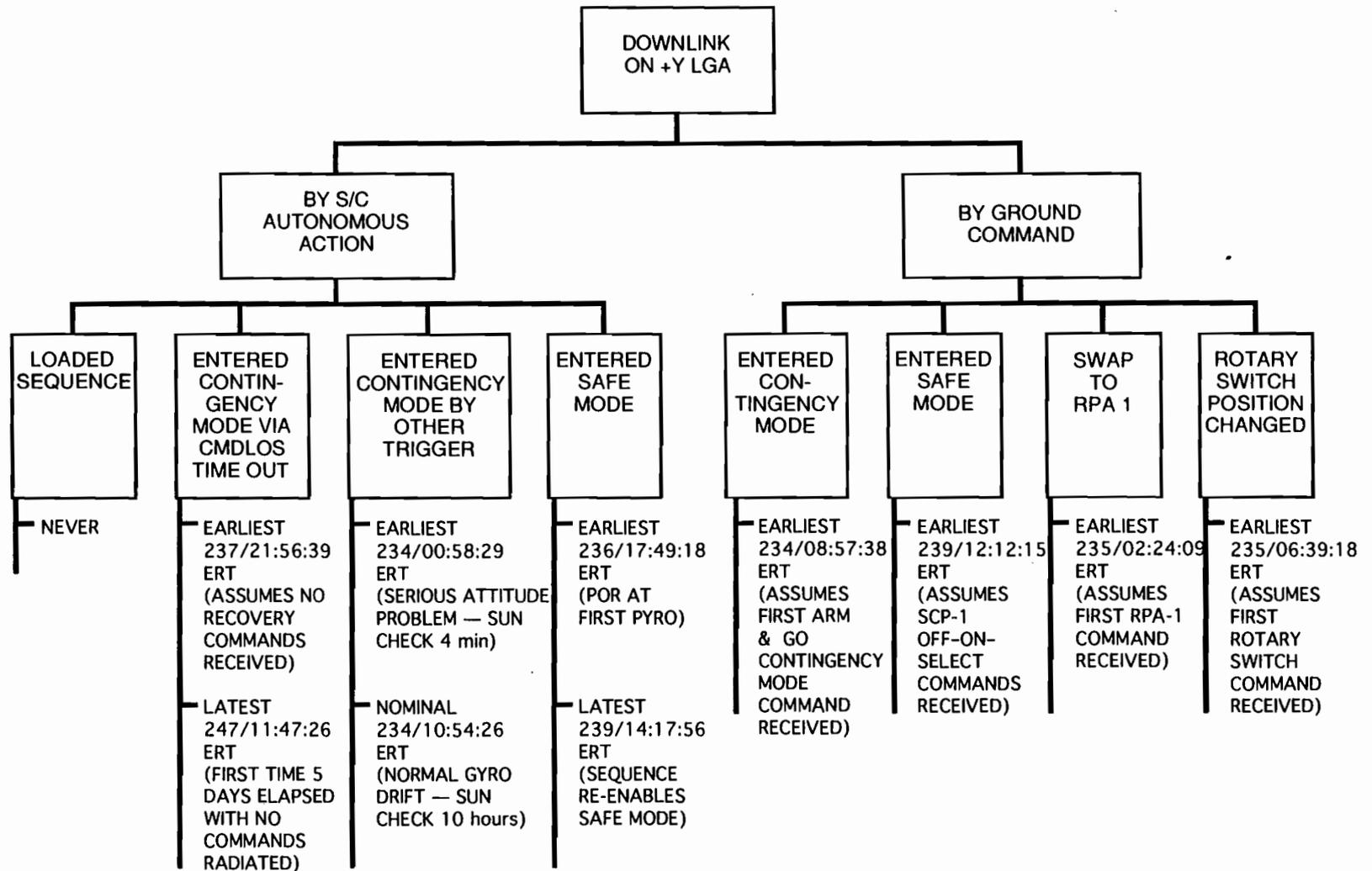
The Mars Observer spacecraft continuously operates two receivers and two CDUs. Commands may be received via any of three antennas that are continuously selected. A forward-hemisphere (+Y) receiving LGA is coupled to one of the two receivers, while the HGA and a rear-hemisphere (-Y) receiving LGA have uplink signals combined and coupled to the other receiver. Each of the receivers is uniquely identified with a CDU, and the two CDUs may be configured for different command data rates (see the Telecommunications Subsystem description in Chapter V.G).

Command *threshold* is an uplink signal level that will produce a *bit error rate* of 1×10^{-5} when detected on the spacecraft. The signal level required at threshold is variable, depending on the command data rate selected for the CDU. The following command link estimates have been computed for various command data rates and the Earth-spacecraft range on August 21, 1993, assuming proper receiver carrier acquisition and maintenance of proper pointing during the required command transmission interval. Recalling that the command data rate transmitted to the spacecraft must match the rate selected for the CDU for commands to be successfully received:

- (1) The HGA can receive commands at 125 bps for boresight offsets from Earth line of 1.4° or less.
- (2) The HGA can receive commands at 62.5 bps for boresight offsets from Earth line of 1.6° or less.
- (3) The HGA can receive commands at 7.8125 bps for boresight offsets of 4.0° or less.
- (4) For any orientation of the spacecraft within 80° of an LGA boresight, commands can be received at 7.8125 bps.
- (5) Either LGA can receive commands at 62.5 bps for boresight offsets from Earth line of 40° or less.

Since uplink commands did not establish a downlink, the following conclusions can be reached. Either:

- (1) Uplink commands are not being received due to failure of both receivers, CDUs, and/or antennas required to support the prevailing attitude; *or*
- (2) The uplink tuning profile has repeatedly failed to acquire a receiver to allow command detection; *or*
- (3) Commanding has not been at data rates that match those selected for the CDUs; *or*
- (4) Spacecraft attitude rates are sufficiently high to prevent successful demodulation of the command data stream while briefly above the threshold on any single antenna; *or*
- (5) The spacecraft is not properly processing received command data to effect the desired control.



RPA 2 AND HGA WERE SELECTED AT TIME OF PRESSURIZATION SEQUENCE. IT IS POSSIBLE THAT THE ABOVE EVENTS NEVER HAPPENED.

**Figure 4-2. Time delays to transfer to LGA.
(expected HGA AOS = 234/00:54:25 ERT).**

3. *Attitude Dynamics Considerations*

Many of the failure scenarios proposed have attitude time histories that fall into one of the following categories: (a) nominal attitude, (b) uncontrolled attitude, (c) high spin rate, (d) attitude does not matter, or (e) complex but analyzable attitude dynamics. The conclusions that can be drawn for each are discussed below.

a. *Nominal Attitude*

If the failure is in a portion of the spacecraft not required for attitude control (e.g., RPA), the nominal attitude sequence applies. The spacecraft would return the HGA to Earth pointing following the pressurization event, reestablish Array Normal Spin (ANS), proceed to perform MOI on schedule and in the correct direction, and eventually fall into Contingency Mode when the Command Loss Timer (CLT) times out, if not sooner. In this scenario, the LGA always covers the Earth, except when occulted by Mars. Since almost all recovery sequence commands would have been received, the only nominal attitude hypotheses that survive are those that postulate a failure that cannot be fixed by the commands that were sent.

b. *Uncontrolled Attitude*

If the attitude is uncontrolled, the initial angular momentum direction determines the resulting motion. Simulations indicate that the LGA will cover the Earth for more than 20 minutes at a time, a couple of times each hour. Since many recovery sequence commands would have been received, the only uncontrolled attitude control hypotheses that survive are those that do not autonomously establish a downlink, and that cannot be fixed by the commands that were repetitively sent.

c. *High Spin Rate*

One way to defeat communications with a working Telecommunications System is to spin the spacecraft so fast that the DSN cannot lock onto any signals it receives. Table 5-9 in Chapter V.E indicates what capabilities are lost at certain rates. Any hypothesis that can get the spacecraft spinning at more than $16^\circ/\text{s}$ perpendicular to the LGA boresight can explain all the observables. (See Table 5-9.)

d. *Attitude Does Not Matter*

In a number of scenarios, the spacecraft is assumed to be so severely damaged that all types of uplink and downlink are impossible. Primary power loss and Propulsion System breach fit in this category. Spacecraft attitude plays no part in the consideration of these failures.

e. *Complex but Analyzable Attitude Dynamics*

A number of functional failures have been postulated that result in complex but analyzable attitude-time histories. For most of these, the analysis showed that at least

an LGA carrier would have been detected had the postulated failure occurred. Even for the one exception, analysis shows that LGA downlink would have been very likely (Hypothesis S5, See Chapter VII.V). This exception was due to an unexpected interaction between the sequence and the fault protection software such that a Contingency Mode entry during RPA Beam On macro execution would result in cancellation of the macro, and the recovery action RPA Beam On command could not be guaranteed to have arrived before spacecraft power loss.

f. Other

Next consider those hypotheses that do not fall into any of the above categories. Some hypotheses are either not analyzable or they generate a huge array of possible attitude-time histories. In considering these, it may be helpful to consider the set of complex cases that have been simulated in the VTL and see what conclusions can be drawn.

In almost all cases that have been run, the LGA repeatedly comes close enough to the Earth line for a long enough period to allow a downlink carrier to be detected if one had been broadcast. The issues are: When does the spacecraft switch to the LGA (Figure 4-2)? When does it turn the RPA beam on? and Is it in danger of losing power due to an unfavorable attitude?

Any failure that both causes a switch to Contingency Mode upon resumption of ANS (which will terminate the RPA Beam On command) and an unfavorable attitude profile from a solar power point of view has the potential of losing spacecraft power before any RPA Beam On commands arrive. Some IMU failures discussed in the next section fall into this category.

Similarly, any failure that causes an unfavorable attitude profile from a solar power point of view, but for which the power alert causes a Contingency Mode entry (which will turn off the RPA), also has the potential of losing spacecraft power before any RPA Beam On commands arrive.

There are certainly pathological cases where the spacecraft attitude could point away from the Earth without any LGA-to-Earth viewing opportunities. Such scenarios are not considered credible.

4. Summary

To summarize, the following are known to be consistent with the observables:

- (1) Catastrophic damage occurring during the 14-minute planned communication outage
- (2) Very high spin rates, making it impossible to lock up on an existing downlink
- (3) Total primary power loss
- (4) Irrecoverable computation loss

- (5) Contingency Mode entry just after Go-ANS followed by an attitude-time history which leads to total power loss before any RPA-Beam On commands were received
- (6) Telecom downlink failure

Analysis indicates that the following are not consistent with observables:

- (1) Attitude control failure leading to uncontrolled attitude drift (plenty of LGA downlink opportunities)
- (2) Computational loss scenarios recoverable by uplink commands (plenty of LGA uplink and downlink opportunities).

CHAPTER V

SYSTEM AND SUBSYSTEM ANALYSES SUMMARIES

A. Systems, Test, and Operations

1. *Spacecraft System Description*

As shown in Figure 5-1, the spacecraft system comprises eight engineering subsystems plus the payload. The engineering subsystems are:

- (1) Structure, for primary and secondary structural elements
- (2) Mechanisms, which includes devices for deploying the HGA, Solar Array, Gamma Ray Spectrometer boom, and magnetometer boom
- (3) Power, including Solar Array and batteries
- (4) Telecommunications, which includes two redundant sets of X-band components in addition to three low-gain antennas and a high-gain antenna
- (5) Command and Data Handling, which includes two redundant control computers, two data-formatting computers, input/output buffers, pulsed and latching output relays, four tape-recorder transports and three tape-recorder electronic units, and data modulation units
- (6) Attitude and Articulation Control, which includes the star, Sun, horizon, and inertial sensors, plus reaction wheels, all of which are used by control algorithms in the C&DH control computer to control spacecraft attitude and rate
- (7) Thermal, which includes closed-loop controlled heaters, as well as blankets and radiators
- (8) Propulsion, comprised of monopropellant and bipropellant systems

The payload also includes a Payload Data Subsystem (PDS), which passes commands to the science instruments and formats science data. The system-level functional characteristics of the spacecraft are described below.

Attitude control is accomplished through three-axis stabilization using reaction wheels. Celestial references are sensed using Sun sensors, a star sensor, and, when in Mars orbit, horizon sensors. Thrusters are used to unload the reaction wheels. (There is no mode for three-axis control using thrusters except during trajectory correction propulsive burns.)

The Power Subsystem uses a multipanel Solar Array (four of six 4-m² panels are illuminated during cruise), controlled by a shunt regulator which operates on the lower panels, as the primary power source. Additional energy is available from two nickel-cadmium batteries, whose output is regulated with a boost voltage regulator. Battery state-of-charge is replenished with redundant charge regulators. The power bus is 28 V,

each load is fused, and two single-point hard grounds connect power return to the chassis.

Telecommunication is provided only at X-band, although a Ka-band downlink was included as an experiment. Downlink radiated power is provided by a 44-W traveling wave tube RF power amplifier (RPA). The primary antenna for up- and downlink is the 1.5-m-diameter high-gain antenna, but there are three additional low-gain antennas: two looking in opposite directions for uplink and one looking generally in the Sun direction for downlink. The redundant receiver-command detector pairs are always powered and connected to different antennas, while no more than one RPA is powered at a time. Uplink rates range from 7.8 to 500 bps in times-two steps. Engineering downlink ranges from 10 bps in the emergency mode to 2000 bps.

Attitude control, uplink command decoding, and stored command sequencing are performed by the software in a single computer, the Standard Controls Processor (SCP). The second SCP is running as a hot backup. Engineering data processing is provided in a separate processor, the Engineering Data Formatter (EDF). The second EDF is off (cold backup). Recorded data are stored using any of the four tape-recorder transports (via one of the three tape-recorder electronics units).

The Propulsion System includes a bipropellant system (nitrogen tetroxide and monomethylhydrazine) that operates in a blowdown mode during cruise and was to be pressure-regulated beginning at Mars orbit insertion (MOI). Also included is a dual-redundant monopropellant system (hydrazine) that operates in a blowdown mode. There are four 490-N main engines and an assortment of 22-, 4.5-, and 0.9-N thrusters.

2. System Single Failure Points

Except for one recently identified single failure point, all identified single failure points are internal to a single subsystem. That newly identified system single failure point is analyzed in detail in Chapter VII.Q. The following paragraphs summarize the analysis.

The failure scenario described in Chapter VII.Q begins with a hardware failure in the C&DH Subsystem that causes a spurious On command to be received continuously at either RPA Beam On control relay in the SCU. Then, as a result of turning off the filaments during the pressurization sequence, hardware logic contained in the SCU and RPA combine to prevent either RPA beam from being turned back on. The On command will permanently hold one RPA Beam On control relay in the off state through interlock circuitry in the SCU, while holding the other RPA Beam On control relay permanently in the on state.

This latter event generates a Beam On command, but it will not be responded to because logic in the RPA ignores Beam On commands until 209 seconds after the filament has been commanded on. After that, a new command is required, which would normally be generated by cycling the RPA Beam On control relay in the SCU from on to off to on. This cycling is impossible because of the failure, therefore the beam can never be turned back on.

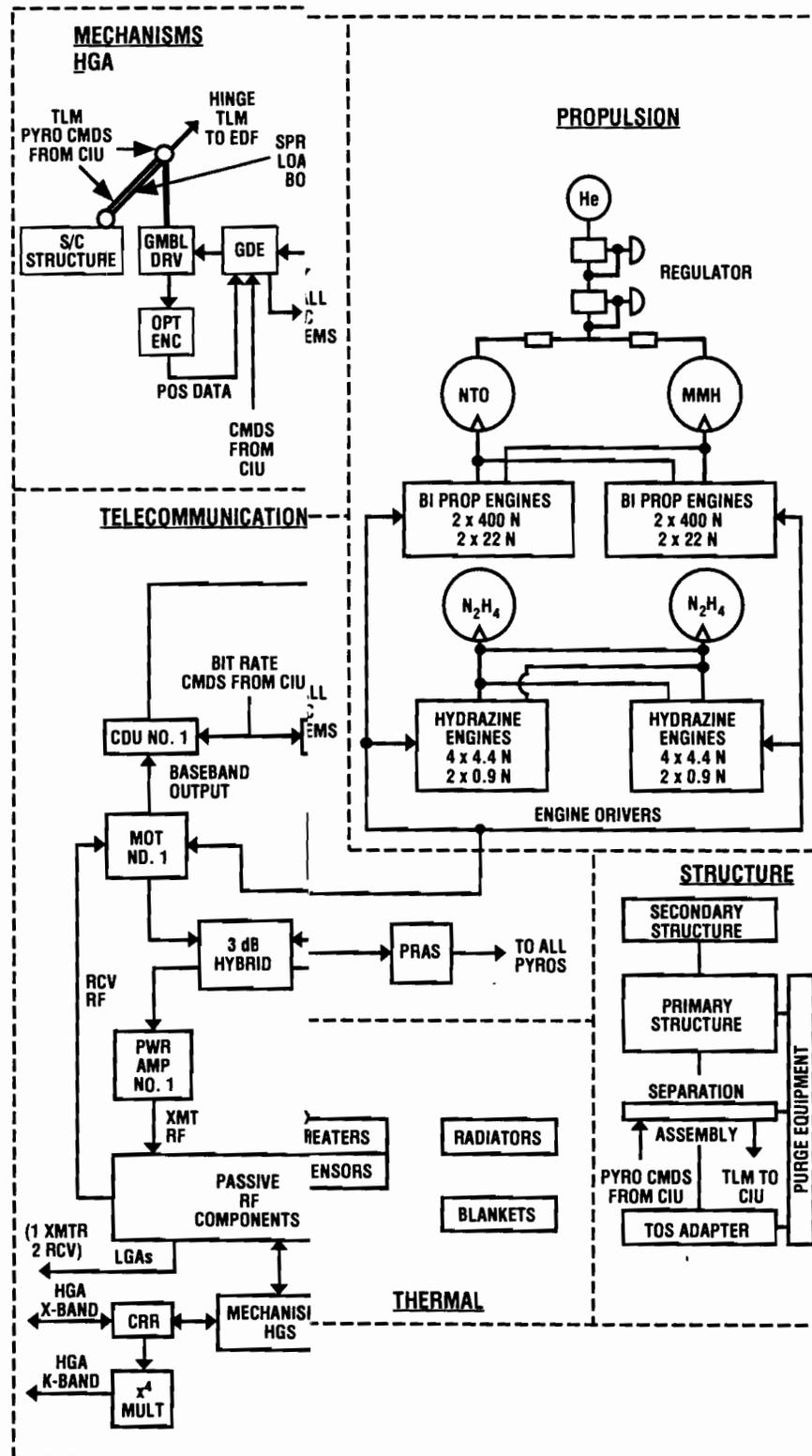


Figure 5-1. Spacecraft functional block diagram.

The period during which the failure could have caused the symptoms of the Mars Observer anomaly began on August 2 for failures causing a spurious RPA-2 Beam On command and at the start of the pressurization block for failures causing a spurious RPA-1 Beam On command. (On August 2, the spacecraft was configured from RPA-1 to RPA-2.) The end of the period of vulnerability was 209 seconds after the sequence commanded the RPA-2 filament back on.

It should be noted that the spacecraft was continuously vulnerable to this failure mode beginning at liftoff. Permanent loss of downlink would have resulted at the next filament-off event following the actual failure occurrence.

3. *Integration and Test*

The integration and test program planned for Mars Observer was typical for a spacecraft project. However, the test program actually executed was incomplete in some respects. Figures 5-2 and 5-3 illustrate the integration and test flow used for both bench- and spacecraft-level testing. Table 5-1 provides definitions for the various tests used.

Component- or assembly-level testing was performed prior to the system test program. A report by M. Trummel¹ shows that deviations from the environmental test and analysis requirements² were identified and a risk analysis was performed. This analysis showed that some deviations were considered technically unacceptable, or presented an estimated decrease factor in reliability, as compared with the processes required.³ For others, an estimated decrease factor could not be quantified. The added cost for full compliance with those requirements⁴ was considered prohibitively expensive and of unknown real value. The deviations were approved by Project waiver.

The bench integration test (BIT) activity (Figure 5-2) performed initial integration and test of components that had completed lower-level testing. BIT focused on the integration of components from the Power Subsystem, C&DH Subsystem, AACS, and PDS. BIT was also used to check C&DH components destined for use in the Verification Test Laboratory (VTL), and to test a subset of the functionality of the flight software.

The spacecraft integration and test activity (Figure 5-3) built and tested the spacecraft and payload in preparation for shipment to the Eastern Test Range (ETR). A battery of tests (Table 5-1) included electrical, functional (including flight software), interface and polarity, environmental (including thermal vacuum, electromagnetic compatibility, static and modal dynamics, sine vibration, acoustics, and pyrotechnic shock), deployment and articulation, mass properties, sequence, ground data system,

¹ M. Trummel, *Summation of Required Mars Observer Waivers to FPO 600-3 Requirements*, JPL Interoffice Memorandum 5217-89-003, Jet Propulsion Laboratory, Pasadena, California, February 23, 1989.

² *Payload Classification Product Assurance Provisions*, FPO document 600-3, Jet Propulsion Laboratory, Pasadena, California.

³ *Ibid.*

⁴ *Ibid.*

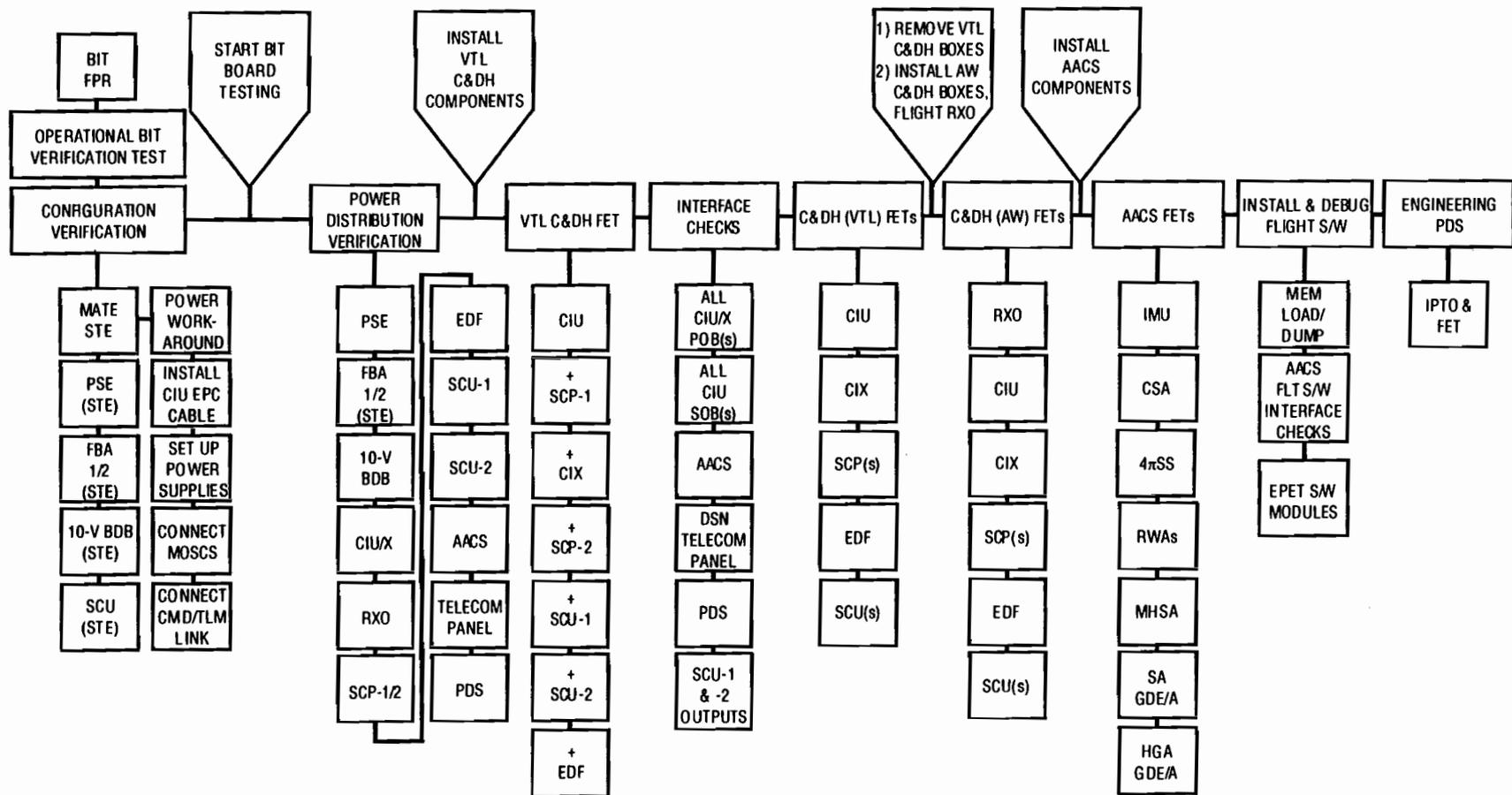


Figure 5-2. Integration and test flow used for bench-level testing.

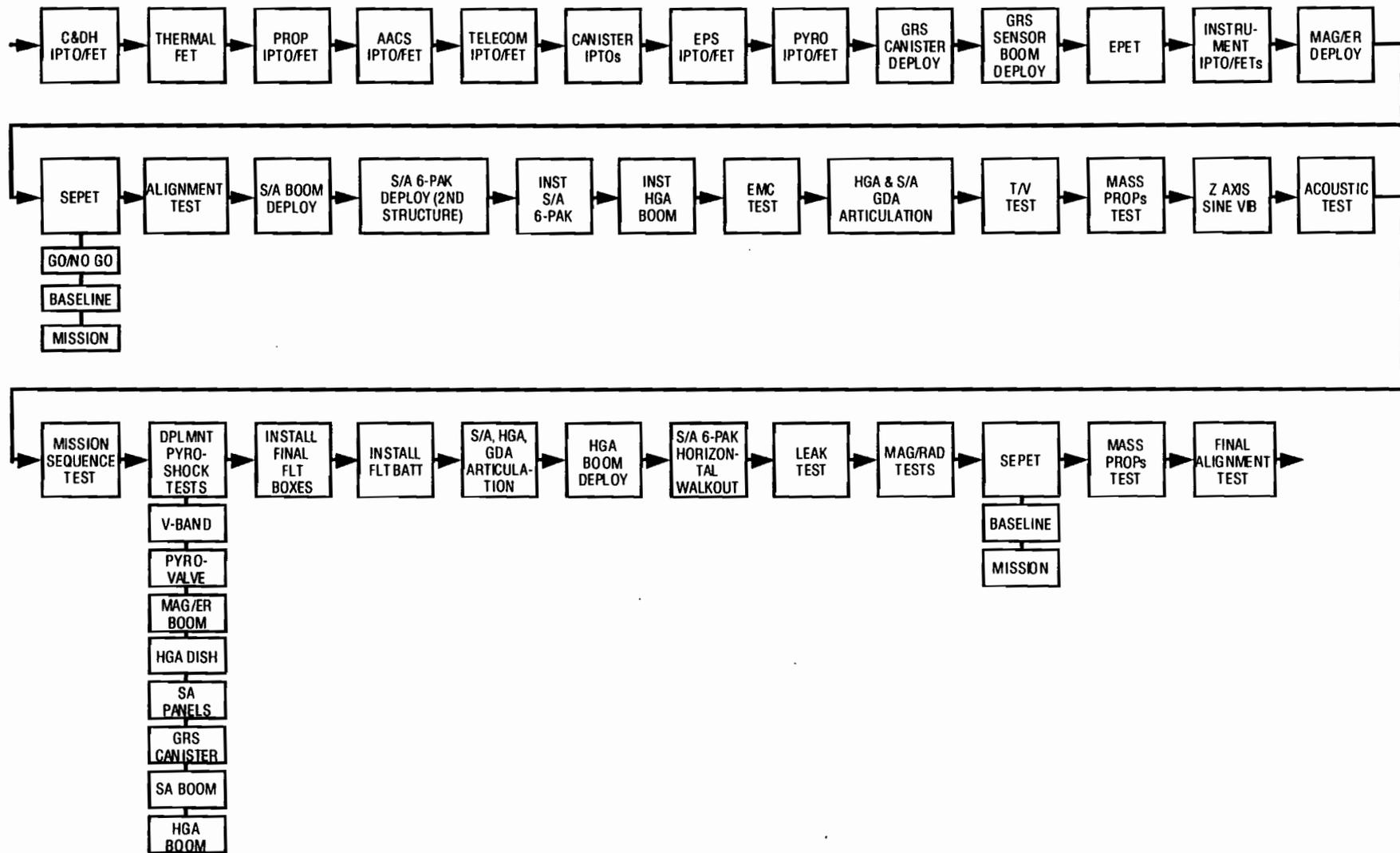


Figure 5-3. Integration and test flow used for spacecraft-level testing.

Table 5-1. System test types.

Test type	Purpose
Initial power turn on (IPTO)	Apply and verify safe initial power to spacecraft components
Functional electrical (FET)	Verify box and spacecraft functions and interfaces after initial integration
Electrical performance evaluation (EPET)	Verify functionality of flight software in spacecraft environment
Go/No Go	Demonstrate spacecraft aliveness by performing box-level functional electrical and command/telemetry tests
Baseline	Exercise a cross-section of tests performed during FET and EPET tests to demonstrate box function and system-level compatibility, and to provide data for comparison with previous box and system-level test data
Mission Sequence	Verify the baseline mission operability requirement by executing four sequences that represent spacecraft activity to be performed during the mission; these include (1) launch and cruise events, (2) maneuvers including MOI, (3) events for the transition from a cruise to a mapping phase, and (4) mapping and payload events
System electrical performance evaluation (SEPET)	Perform Go/No-Go, Baseline, and Mission Sequence tests
Polarity	Verify polarity consistency across all sensor-flight software actuator paths of the AACS
MOS Compatibility Sequence	Execute mission-critical flight sequences, including MOI and TCM-1, to verify MOS interfaces and procedures necessary to support flight operations, and demonstrate compatibility of JPL ground data system with the spacecraft
Thermal vacuum	Demonstrate spacecraft system operation in thermal vacuum environment and functionality with thermal margin
Electromagnetic compatibility (EMC)	Verify that radiated EMC from ground and onboard sources does not interfere with normal system operations, and that the system does not electromagnetically interfere with itself
Static load	Demonstrate structural integrity of the primary load path structure, and quantify analytical model accuracy
Modal	Measure primary and secondary structure mode frequencies and shapes through 50 Hz, and quantify analytical model accuracy
Sine vibration	Verify spacecraft system design and quality, and demonstrate system survivability when exposed to expected flight dynamic environment
Acoustic	Verify spacecraft system design and quality, and demonstrate system survivability when exposed to expected flight dynamic environment
Deployment	Verify that deployment mechanisms for Solar Array and boom, HGA and boom, GRS and boom, and MAG/ER boom perform as designed, and verify that there is no performance degradation due to environmental exposures

and DSN compatibility tests. Once the spacecraft was at ETR, a number of spacecraft, payload, and mission system electrical and performance tests verified post-shipment performance. Limited DSN and ground data system compatibility testing via spacecraft antenna hats was also completed.

Much system-level testing was performed using a spacecraft checkout station. The checkout station was used to send commands and display telemetry data. The station was a new implementation for Mars Observer and experienced hardware and software bugs during test. This increased schedule pressures and made testing difficult.

“All plugs out” spacecraft testing was very limited. With the ground support equipment (GSE) connected, the C&DH SCP flight software was not allowed to boot from read-only memory (ROM) and enter Safe Mode as intended in flight. The software always entered Safe Mode by transitioning through a GSE boot mode first. The C&DH controls interface unit (CIU) hardware-decoded command to restart the SCP was never tested or used without the GSE connected. Similarly, the SCP restart command via the simulated uplink channel was never tested in the VTL. As a result, a flight software design flaw that contributes to locking up the CIU uplink processor when the SCP restart command is sent was not discovered until VTL tests after the loss of signal. SCP restart is a basic but important function of the C&DH.

The pyrotechnic shock test was very limited, and was performed without propulsion plumbing connected to the test pyro valves. The result of this was to isolate the spacecraft from the major electrical and dynamic effects of the test, thus rendering the test nearly meaningless from a dynamics and EMI perspective.

A spacecraft-level test was not performed to check the system response and impacts of the primary-side failure of the redundant crystal oscillator (RXO) frequency output to the CIU, even though this potential failure was identified as a mission-critical single failure point at the time of the C&DH Subsystem CDR. RXO tests in the VTL were not complete enough to test the flight software for this potential failure.

Fault protection testing in the spacecraft environment was also extremely limited. The vast majority of this test activity was performed on the real-time application interactive debugger (RAID) simulator and in the VTL. In effect, no system-level fault protection test program was performed on the spacecraft. A major fault protection test program in the VTL was undertaken throughout the summer of 1992. The lateness of the VTL test program precluded fixing any problems discovered in the flight software program in ROM launched with the spacecraft. In hindsight, the fault protection testing was flawed in the area that handles failures of the RXO and CIU timing chain.

Post-launch, a potentially serious design flaw was discovered in the C&DH EDF flight software’s handling of error detection and correction (EDAC) of its memory. EDF EDAC is a basic and important function of the C&DH Subsystem.

4. *Operations and Sequence of Events*

a. *General*

The only pyro activities prior to pressurization were associated with launch and early cruise deployments. Three trajectory correction maneuvers (TCMs) were conducted during cruise: TCM-1 on October 10, 1992, TCM-2 on February 8, 1993, and TCM-3 on March 18, 1993. Science calibrations were conducted on the Magnetometer, the Gamma Ray Spectrometer, and the Thermal Emission Spectrometer. The principal anomalies experienced during cruise were due to failure of the attitude determination function, which caused entrance into Contingency Mode several times. A source of these anomalies was found in the flight code, which was modified to fix the problem. Another cause was some ground-selected parameters, which were found to be inappropriate and were corrected.

b. *Pre-MOI Activities*

MOI-related commanding began at MOI-19 days with the loading of star catalog and ephemeris data for the 22-day period ending at MOI+4 days. Propellant tank heaters were turned on at MOI-18 days. The sequence that would begin at MOI-7 days and include the propellant pressurization and MOI blocks was loaded at MOI-17 days. This sequence, known as T1, was broken into two segments, T1A and T1B, which contained the pressurization and the MOI block activities, respectively. The version of T1B loaded at MOI-17 days was based on preliminary trajectory predicts and was known as T1B (backup) because it would only be executed if ground commanding problems prevented loading the final version of T1B at MOI-4 days.

T1A and T1B were in sequencing memory, but were inactive during the last 10 days of the final cruise sequence, referred to as C13. The only activities during these 10 days were to configure the transponder on four occasions for delta differenced one-way ranging (Δ DOR) tracking passes and to alternately trickle-charge the two batteries once a day. T1A became active at MOI-7 days. Its initial activity consisted of activating a new star catalog and configuring the transponder prior to and after Δ DOR tracking passes. At MOI-4 days, the final version of T1B was loaded. T1B (backup) remained in memory, but would be canceled by the T1B (final) when it went active. The pressurization block activities began at approximately MOI-3 days with a sequence of commands to repack tape recorder 1. Following this, tape recording was begun and the pressurization block was initiated. The expected sequence of events from 234/0029 to 234/0130 Earth-received time (ERT) is included in Appendix T, and the full expansion of the events in the pressurization block is shown in Table 5-2.

It was noted that the original plan was to execute the block once for each pyro valve firing, pausing between firings for ground confirmation. Because the propellant pressurization was not performed shortly after launch as originally planned, and because concern about a regulator leak made it desirable to pressurize as late as possible before MOI, the block was modified during flight to include both primary pyro valve

firings in one block. Backup pyro valve firings were still to be accomplished one to a block and executed only if needed. The T1A sequence, therefore, included three pressurization blocks, the last two being optional.

c. *Spacecraft State Prior to the Start of the Pressurization Block*

A summary of the significant telemetered spacecraft state data is contained in Table 5-3.

Table 5-2. Commands in pressurization block.

Relative Time	Command/Event
0	MOT exciters 1 and 2 off
0m 1s	RPA 1 and 2 beams off
0m 5s	RPA 1 and 2 filaments off
4m 4s	Skew RWA on
4m 5s	Set AACS state to Deploy Control
4m 55s	Enable primary early cruise pyro bus
4m 55s	Enable backup early cruise pyro bus
4m 56s	Arm primary early cruise pyro bus
4m 56s	Arm backup early cruise pyro bus
5m 5s	Fire pyro valve 7
10m 5s	Fire pyro valve 5
10m 12s	(Set AACS state to Sun-Star-Init) ^a
10m 15s	Disarm primary early cruise pyro bus
10m 15s	Disarm backup early cruise pyro bus
10m 16s	Disable primary early cruise pyro bus
10m 16s	Disable backup early cruise pyro bus
10m 17s	Set AACS state to Array Normal Spin
10m 18s	MOT exciters 1 and 2 off
10m 19s	RPA 1 and 2 beams off
10m 22s	RPA 2 filament on
14m 22s	RPA 2 beam on
14m 23s	MOT exciters 1 and 2 off
14m 26s	MOT exciter 2 on
20m 17s	Skew RWA off
20m 18s	RWA X, Y, and Z on

^a Nonblock command.

Table 5-3. Spacecraft state at start of pressurization block minus 7 seconds.

AACS	State	Array Normal Spin
	Inertial Reference	Established
	Star Sensor A/B	On (both)
	Sun Sensor 1/2	On (both)
	Sun Sensor select	A
	Sun Ephem Monitor	Enabled
	Gyro 1/2/3	On (all)
	RWA X/Y/Z/S	On (all, except Skew)
MHSA	Off (all)	
C&DH	Telemetry Mode	Engineering
	Bit rate	2000 bps
	Control SCP	SCP-1
	SCP-1/2 MEOK	OK
	Safe Mode	Disabled
	Contingency Mode	Armed
	REDMAN	Enabled for all devices, except SA drive, HGA drive, and the MHSA Disabled for the IMU Status Word check (which includes checking for a gyro spin motor short)
	Active Scripts	6
	Command Loss Timer	93.3 hours
	RXO Mode	Primary
	CIU Bus	A
	CIU I/O cross-strap	Not cross-strapped
	CIX Bus	A
	CIX I/O cross-strap	Not cross-strapped
	DTR power	DTR 1 on; 2 and 3 off
	DTR 1 State	Record, 2 kbps
	EDF	EDF 1 powered and selected
XSU	XSU 1 powered and selected	
PDS	Powered; side A selected	
Telecom	RF Switch 1 posn	A (Rcvr 1 to +Y LGA; Rcvr 2 to HGA/-Y LGA)
	CDU 1 U/L rate	7.8125 bps
	CDU 2 U/L rate	125 bps
	Receiver Lock	In Lock (both receivers)
	Coherency status	Coherent (both transponders)
	USO status	Inhibited in MOT 1; Enabled in MOT 2
	Exciter status	MOT 2 exciter on
	RPA 1 status	Filament on; Beam off
	RPA 2 status	Filament on; Beam on
	RF switch 2 posn	A (RPA 1 to LGA; RPA 2 to HGA)
Propulsion	Thrusters	Disarmed and Disabled (all)
	Biprop Latch Valves	1-4 Open
	Monoprop LVs	Open, except for crossover valve
Power	Battery 1/2 State	100% (both)
	Battery Charger	Battery 1 Connected Only
	Batt 1 Chg Curr	0.775 amps
	Solar Array power	673 watts (power used, not capability)
Payload	Instrument power	MAG/ER on GRS on All other instruments off

d. Flight Sequence Load

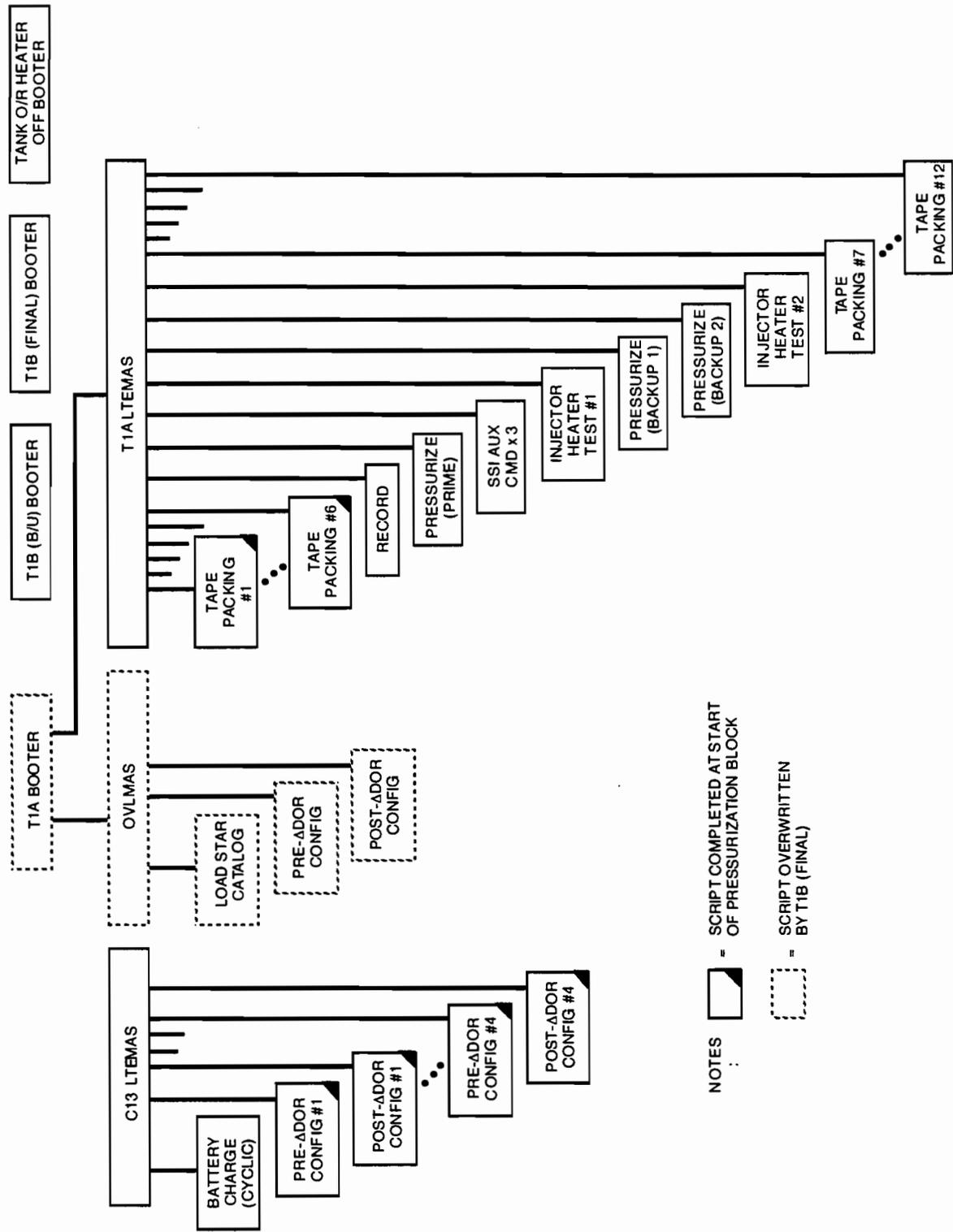
All event sequences are in the form of scripts, which are chains of commands separated by delta times. Several scripts can be executed simultaneously, each being initiated by a master script. Master scripts, in turn, are initiated by booter scripts, which execute at absolute spacecraft times following their loading into sequence program memory. Booter scripts are the only ones that can be directly initiated at an absolute time; all other scripts are referenced by relative time deltas to these absolute times.

The flight load uplinked at MOI-17 days contained two booter scripts, one each to initiate T1A and T1B (backup). T1A started two master scripts: OVLMAS, which ran from 229/1541 to 230/1821, and LTEMAS, which ran from 229/1541 to 234/2020. As mentioned, the pressurization activities were in T1A. The T1B (backup) script was to start at 235/1441 and execute MOI using the best parameters available at MOI-17 days. Another booter script, which would initiate the master scripts for T1B (final), was loaded at MOI-4 days. The booter scripts for both T1B sequences were to initiate at the same time, but the initial event out of T1B (final) would cancel the T1B (backup) script. (Because of onboard software logic, a script cannot be canceled until it is active.) A last booter script was loaded at the same time as T1B (final). This script was to initiate commands to turn off the propellant-tank override heaters shortly before the MOI burn. Figure 5-4 depicts the scripts that were active during the T1A phase at the time of the anomaly. There is an additional active script, initiated in the C13 sequence, that controls battery charging. This script is cyclic, restarting itself daily.

As seen in the figure, the OVLMAS master script started three scripts, all of which had completed by the time of the anomaly. These scripts activated a new star catalog and coordinated the transponder configuration during planned Δ DOR tracking passes.

The pressurization-related activities were initiated by the LTEMAS master script and were contained in nine scripts. The scripts controlled the following events:

- (1) Tape packing
- (2) Initiation and termination of tape recording
- (3) The prime pressurization block, which would open valves 7 and 5
- (4) An injector heater test
- (5) A backup pressurization block to open valve 8
- (6) A backup pressurization block to open valve 6
- (7) Another injector heater test
- (8) Post-pressurization tape packing
- (9) An auxiliary sequence to overlay each of the three pressurization blocks with a Sun-Star-Init command prior to the Array Normal Spin command. (The purpose of the Sun-Star-Init command is to initiate reacquisition of references had there been a loss-of-references condition at the time the AACS state was set to Deploy Control.)



NOTES
 :
 [Solid box with diagonal line] = SCRIPT COMPLETED AT START OF PRESSURIZATION BLOCK
 [Dashed box] = SCRIPT OVERRITTEN BY T1B (FINAL)

Figure 5-4. Depiction of scripts active during T1A phase at the time of the anomaly.

Note that the pressurization blocks utilized a “mission script” that is permanently in the sequence memory to turn the RPA beam off and on. This RPA beam off/on script had been used for cycling the RPA during TCMs 1–3. Cathode heater (“filament”) off commands were also used for TCMs 1–3, just as for the pressurization blocks.

e. Analysis of the Sequence and Sequence Load

All the stored sequence events leading up to the pressurization block did occur correctly and at their expected times. The spacecraft state observed in the last complete telemetry frame, sent 7 s prior to the planned downlink off time, was as expected. The actual time of downlink off, which would be due to the exciter off command in the pressurization block, was observed via the DSN receiver out-of-lock event on the ground. The out-of-lock time initially reported led to some ambiguity about whether the event was evidence of the SCP execution of the first command of the block or was due to the DSN turning off the uplink a round-trip light-time earlier. In Figure 5-5, the time bar at the top represents the time of events occurring at the spacecraft, and the time bar at the bottom represents events occurring on Earth. The time at which the DSN receiver first indicated loss of lock was 00:40:01 UTC, 2 s later than the expected time shown on the figure. This time closely approximates the time that the spacecraft downlink would have shifted from its two-way frequency to its one-way frequency, if the downlink were still present. The frequency shift by itself would have caused a receiver out-of-lock event at the DSN. The DSN did not check the one-way frequency for a signal, since none was expected to be there, so it could have been possible that the spacecraft transmitter was still on. However, inspection of the Link Monitor Control (LMC) log from the DSN showed that the actual time of transmitter off was 2 s later than originally reported. This works out to be 2.7 s less than a round-trip light-time prior to the time that the DSN receiver indicated out-of-lock. Therefore, the out-of-lock originated on the spacecraft and was probably due to the stored sequence executing as expected. The apparent 2-s delay between the spacecraft exciter off ERT and the DSN receiver out-of-lock is due to expected time lag in the receiver out-of-lock indicator. This anticipated time lag is always observed to be at least 1 s, which eliminates any question of whether there had been a swap to SCP-2, which has a 2-s built-in lag relative to SCP-1.

Additional confidence in the stored sequence correctness has been gained by examining the results of VTL simulations before and after the anomaly. The T1A sequence that included the anomaly time period was generated, then simulated and validated in the VTL weeks before. A minor change was introduced to the C13 sequence between that simulation and the T1A/T1B (backup) load, which caused the T1A/T1B (backup) load to be rerun through the ground-command-generation software. However, this did not result in any change to the T1A memory words as loaded in the SCP memory; this was verified by direct comparison with the previously generated load. As a final check, the actual T1A, T1B (backup), and T1B (final) loads have been simulated in the VTL after the anomaly. This simulation shows that nothing unexpected occurred, including the effects of the first 8 hours of recovery commanding.

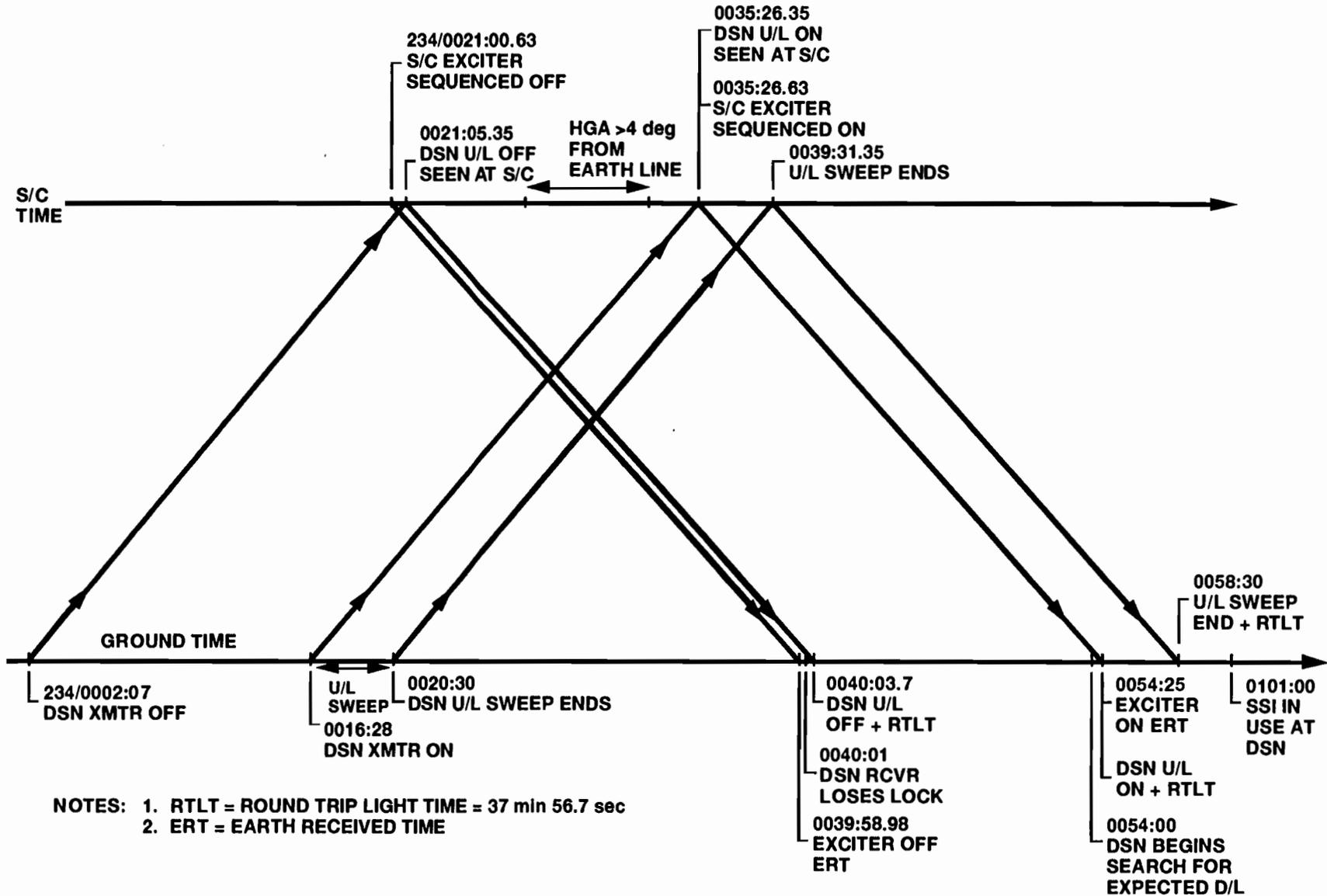


Figure 5-5. Timeline of spacecraft downlink and DSN events..

5. Verification Test Laboratory

The VTL is predominantly a C&DH and AACS simulator used to test sequences and flight software updates before they are executed on the spacecraft. Failure scenarios can also be checked with the VTL; however, this often requires careful test planning and analysis, VTL software (and sometimes hardware) tweaks, and more than one VTL run to properly simulate a complex failure scenario.

Figure 5-6 illustrates that the VTL is composed of a subset of spacecraft hardware units interfaced to the remaining configuration through a special interface unit to a VAX computer with peripheral devices. The spacecraft hardware is a mixture of flight and nonflight spacecraft components (NFSCs). These components and their status is as follows: SCP-1 and -2 are both NFSCs, the CIU is flight S/N 2, the controls interface extender (CIX) is an NFSC, the signal-conditioning units (SCU) 1 and 2 are both NFSCs, and the PDS is a single-string engineering model (EM). The EDF is predominately an NFSC, but does have four flight boards in the NFSC chassis. Instead of an RXO, the VTL uses a Wavetek function generator to simulate the 5.12-MHz clock signal required as input by the CIU. The NFSC and EM units are the same as the flight units in form, fit, and function, and do not have any outstanding engineering changes remaining to be incorporated. These units went through the same component-level test program as did the flight units. All NFSC or EM components were also verified on the spacecraft during system or bench integration test. The NFSC or EM units did not use flight-grade parts in their construction.

A command generator unit interfaces with the VAX computer and provides uplink commands to the CIU in DSN format at all rates and modes required by the mission.

The spacecraft hardware is interfaced to the VTL by means of an interface unit (IU). The IU appears to the spacecraft hardware as if it were the rest of the spacecraft. The IU performs the input/output (I/O) buffering, reordering, and time tagging of information transferred to and from the VAX computer and the spacecraft hardware. The IU also interfaces the Wavetek function generator to the CIU with the requisite 5.12-MHz clock signal. Special bus fault injection and monitoring circuitry is provided to capture, monitor, and modify I/O communications between the SCP and CIU/CIX. All CIU/CIX I/O events are reported to the VAX computer in this way, and not at the CIU/CIX external device interface. This means that if inputs to the CIU/CIX from the SCPs are working, but the CIU/CIX outputs to external devices are not, then the CIU/CIX I/O events are reported as working even when they are not.

All external device behavior is software simulated and is not actual hardware. The VAX computer provides the environmental modeling capability to drive and support the proper operation of the spacecraft hardware elements in the VTL. The level of modeling provided by these software models varies in detail and fidelity from area to area. Extensive modeling is provided for the CSA, SSA, MHSA, RWA, IMU, and star fields for attitude control. Moderate modeling is provided for the SA, gimbal drive electronics (GDE), and HGA articulation. Moderate modeling is provided for rigid-

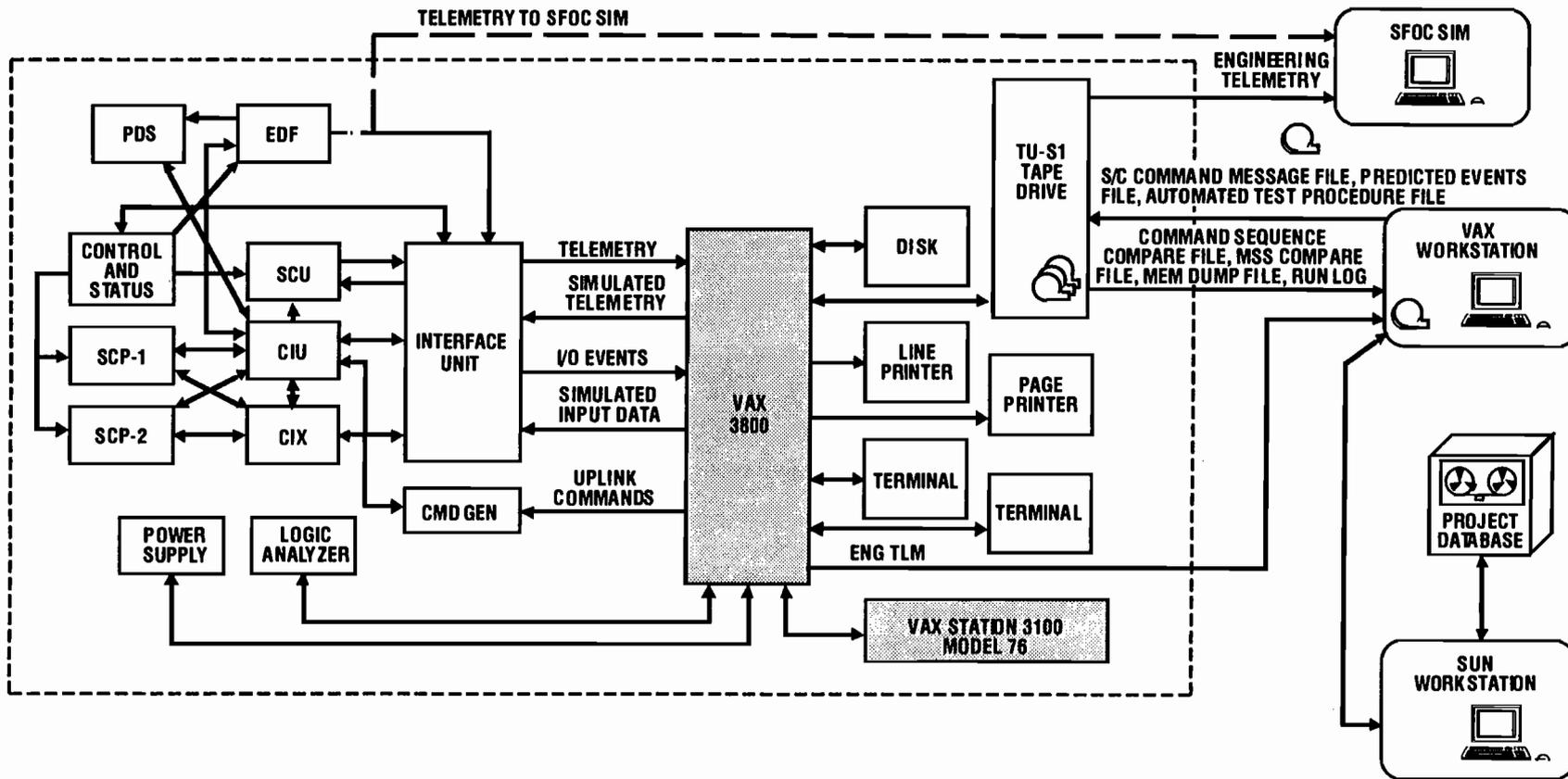


Figure 5-6. VTL block diagram.

body dynamics, and the SA is represented kinematically. Extensive modeling is provided for the DTRs and for telemetry decommutation. Moderate modeling is provided for command responses. Only very light or simple modeling is provided for the payload instruments. Moderate modeling is provided for the Power Subsystem functions of charge, current, and subsystem-status indicators. Moderate modeling is provided for the Propulsion Subsystem mono- and bipropellant fuel usage and thrust. Only light modeling is provided for pyro command verification and Telecommunications Subsystem (including RPAs) command verification. Light modeling is provided for temperature alarms. These models were developed by an Astro subcontractor in accordance with an official Project requirements specification. Some of the models were inherited and modified from the RAID system used to develop and verify flight software. The models were verified by a series of tests, predominantly AACS in nature, and run in the VTL and RAID. The results of these tests were analyzed by both Astro and its subcontractor. Additional verification was performed by testing flight software and sequences in the VTL during its development. During flight, numerous model errors were discovered and fixed. The models are sometimes updated to reflect data as observed in flight.

User interfaces through the VAX computer utilized for simulation setup and initialization, control (pause, checkpoint, resume, and time jump), and monitoring are provided by VAX workstations, terminals, and printers. Little graphical interface capability is provided.

The VTL System was verified in accordance with an official Project verification test program. However, these tests were not comprehensive, validating only user functions and not the information provided by the system. Numerous conflicts between JPL and Astro occurred due to misinterpretation of the requirements. The VTL was included in the program very late in the development cycle. The tight schedule to develop the VTL contributed to these factors and to a less-than-desirable verification test program. Consequently, many software and a few hardware errors in the IU and other supporting equipment were corrected during flight.

For running a sequence simulation, the main inputs to the VTL are the Spacecraft Command Message File (SCMF), VTL Predicted Events File (VPEF), Sequence of Events File (SOE), and SEQTRAN run log. The SCMF contains the uplink commands to be simulated and is the file used by the DSN for transmission to the spacecraft. The VPEF, which is a modified PEF for the VTL produced by the Planning and Sequencing Team (PST), is used to compare with and verify the simulated events and telemetry produced by the VTL. The SOE is used to compare with and verify the simulated status of key telemetry produced by the VTL. The SEQTRAN run log is used to compare and verify the simulated SCP command verification (CV) telemetry messages produced by the VTL. Comparison of the VPEF with simulated VTL events and telemetry is automated on the VTL. However, though supported by a good display system, comparison of the SOE and SEQTRAN run log with simulated VTL events and telemetry is performed manually by the VTL engineer. The primary products produced by the VTL simulation are memory dumps and the simulated events and telemetry. A test report is written to

accompany each simulation run indicating how closely the simulated and predicted events match. Memory dumps are provided to the Spacecraft Team (SCT) and the PST for analysis. Simulation and test requirements for each run are provided by the SCT. The initial conditions for the simulation are provided by using a checkpoint file from a previous simulation and a special initial conditions file modified by the SCT when required. Input, output, and status of the VTL hardware and software are under Project-level configuration control.

A number of differences between the VTL and spacecraft behavior, and previously unknown spacecraft behaviors, were discovered as a result of attempts to simulate failure scenarios and recovery commands in response to the loss-of-signal event.⁵ These are briefly mentioned here. The IMU 10-Hz clock behavior is not properly simulated for RXO and CIU failures. The SCP I/O capability is not lost when dedicated clock divider output fails. The CIU clock divider and similar failures are not simulated correctly. (The above differences were corrected after the loss-of-signal anomaly occurred to support failure hypothesis testing.) Execution of flight software after pause/resume may not be identical to uninterrupted execution, but this has minimal effect. The CIU uplink processor hang-up was discovered through testing of the SCP Restart command (this is a hardware-software interface design flaw). The behavior of external devices, CIU and RXO failure mode testing, is only as good as the fidelity of the software simulations. Monitoring simulation outputs at the SCP-CIU interface, not the CIU-external device interface, makes the simulation appear to be working when it may not be.

⁵ S. Krasner, *Differences Between VTL, Spacecraft I&T, and Flight Environment* (NASA Failure Review Board Request #C20), JPL Interoffice Memorandum SCT-93-614, Jet Propulsion Laboratory, Pasadena, California, October 8, 1993.

B. Flight and Fault Protection Software

The flight and fault protection (FP) software is complex. It executes in two SCP 1750A computers (one prime and one hot backup) and two EDF 1750A computers (one prime and one cold backup). The SCPs intercommunicate by simple interfaces via the CIU, and the EDFs transfer status and telemetry data to the SCPs. The SCP software design uses an interrupt driven commercial multitasking operating system and message-passing queues for intertask communications at its core. Interrupts used to control software operation include those for telemetry data input from the EDF, uplink command input, timing inputs for IMU operation, and a main 10-Hz timing input used to drive a cyclic executive program. The cyclic executive controls the remaining software functions, including time-critical sensor readings, spacecraft timekeeping, Contingency Mode control, attitude control and maneuvering, command and status processing, stored sequence (script) processing, and spacecraft redundancy management, which is the prime vehicle for fault protection operations. A memory single-event-upset (SEU) scrubbing program executes in the background to the cyclic executive to correct bit errors. The software is executed from RAM, and a ROM-resident Safe Mode program to place the spacecraft into a known safe state is available. A block diagram of the flight software task activity is shown in Figure 5-7.

Both SCPs are loaded with identical software and run in parallel. The primary SCP controls the spacecraft, acts on faults, and issues commands to the spacecraft. The backup SCP runs stored sequences with a 2-s delay, so if the primary fails, the backup will take control and not miss sending any commands from the sequences. The SCP flight software detects degraded performance of spacecraft components either from directly sampled data from the component via the CIU or from telemetry provided to the SCP from the EDF. SCP redundancy-management (REDMAN) software responds by switching to redundant spacecraft elements. REDMAN filters fault indicators to reduce the likelihood that transient fault indicators will result in inappropriate activation of the fault protection response. However, failed sensor indicators are not screened out. The fault detection software acts upon multiple, consecutive samples of data from the respective subsystem. REDMAN configures spacecraft components autonomously in response to error reports from other flight software tasks. If a block-redundant spacecraft element is associated with a fault, the SCP flight software commands a switch to the redundant side of the block-redundant element. If the fault is not cleared by the element switch, the primary SCP assumes a bus fault and commands a bus switch. In some cases, if the fault is still not cleared, a control SCP fault is assumed and a SCP switch occurs. The primary SCP will cause a switch to the redundant SCP by withholding its "MEOK" heartbeat to the CIU. The redundant SCP will then become the primary SCP and vice versa. The new SCP will retry device swaps and, if the fault is still not cleared, the new SCP withholds its "MEOK" heartbeat to the CIU. The CIU will then restart both SCPs and cause both to enter Safe Mode, with the new SCP remaining in control.

Entry into Safe Mode by the new SCP can be disabled by ground or stored sequence command. In fact, Safe Mode entry was disabled at the time of the loss-of-signal

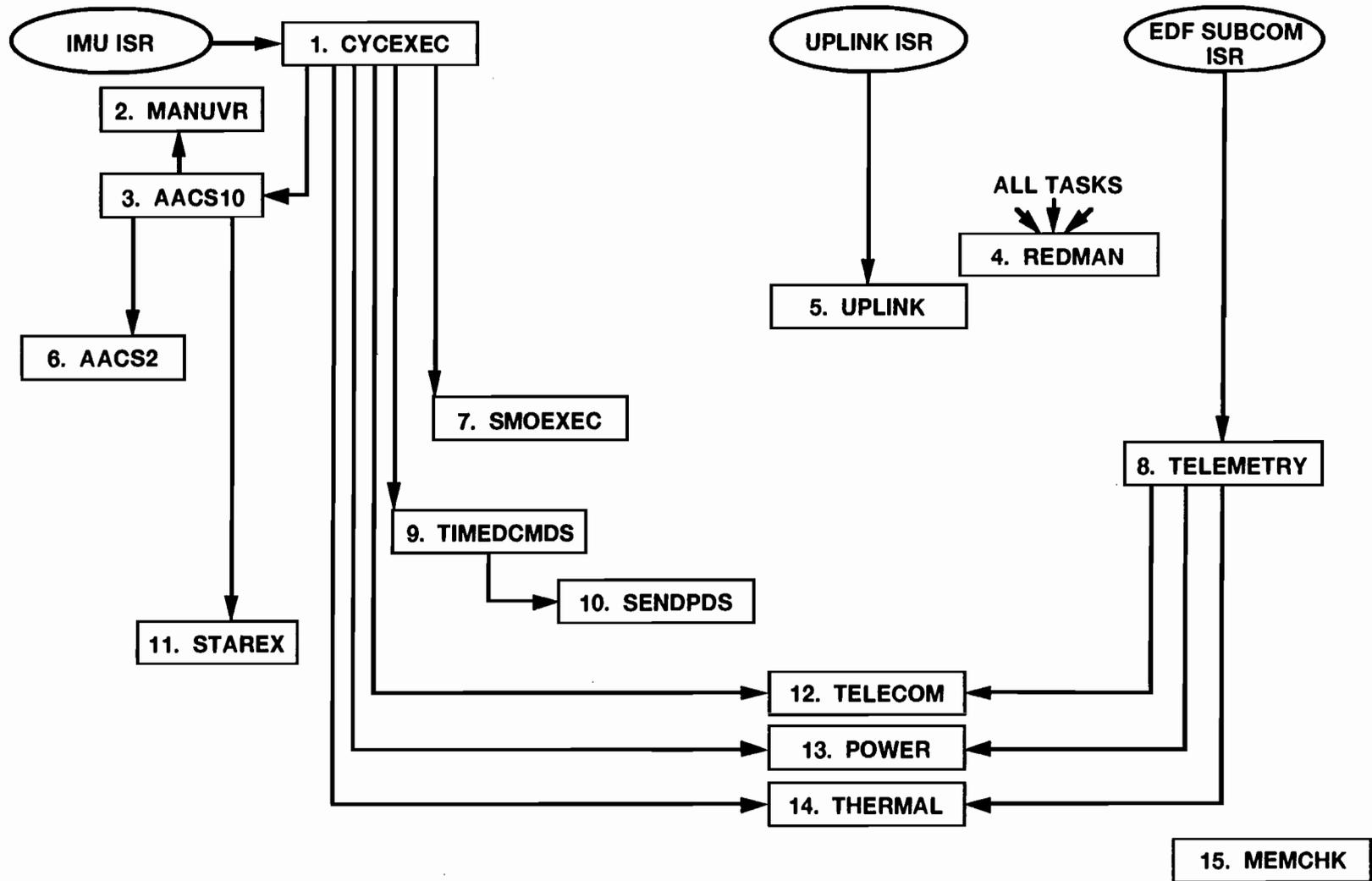


Figure 5-7. Flight software task activity block diagram.

anomaly. A block diagram of the general REDMAN response is shown in Figure 5-8. Note that this diagram only shows some of the REDMAN responses that are available.

The basic flight software, including redundancy-management design, was inherited from past Astro Satcom and Defense Meteorological Satellite Programs (DMSPs). It was extensively re-engineered for Mars Observer. New 1750A computers were utilized. Application code was written in JOVIAL (J73) and some assembly language was used. RAID, acquired from the U.S. Air Force, was enhanced to perform flight software build testing and was the major tool for flight software testing.

The flight software was tested on spacecraft hardware in the BIT environment in early 1991. However, BIT testing came after flight software Build 5, the version of SCP ROM code that was launched. Four system tests for Launch/Cruise, MOI/TCM, Cruise to Mapping, and Mapping were executed on the spacecraft. Two of these were run during thermal-vacuum testing. These were very valuable in wringing out I&T and command block problems. Limited Safe Mode tests were run on the spacecraft.

The VTL provided a C&DH hardware testbed for flight software checkout; however, it came late in the program for flight software development, and a reliably functioning VTL was unavailable until after the spacecraft was shipped to ETR in June 1992. The EDF was tested in the VTL. The VTL was needed for Safe-Mode and SCP-to-SCP verification. Fault protection software tests were run in the VTL from April to July 1992. Three-shift sharing of the VTL was required between the FP and MOS compatibility testing. The VTL was "debugged" during this time. More fault protection tests were performed through September 1992, using 12-hour-day, 7-day week schedules to finish the remaining FP tests.

There was a serious lack of system-level FP system engineering. No single person was responsible for this area. Additionally, no attention was given to possible undesirable interactions between the FP software and stored sequence execution. This was noted in Project-level system reviews.

A design flaw in the way the SCP software interacts with the CIU hardware upon processing the SCP Restart command was discovered by VTL testing during recovery attempts after the loss-of-signal anomaly. The SCP Restart command hangs up the CIU uplink processor, which causes its associated SCP to be forever uncommandable. Because of this finding, this command was subsequently never sent to the spacecraft.

Review indicates that use of the SCP Restart command as a means of effecting Safe Mode entry was never tested prior to launch via the radio frequency link as it was intended to be used in flight. The GSE was always plugged into the spacecraft CIU, and this caused entry into a special GSE mode rather than the normal Safe Mode. This contributed to masking the SCP Restart design flaw mentioned above.

The SCP REDMAN response to a failure of the primary-side RXO frequency output was discovered to be incomplete only after the loss-of-signal anomaly. This appears to

REDUNDANCY MANAGEMENT: (REDMAN) CONFIGURES SPACECRAFT DEVICES AUTONOMOUSLY IN RESPONSE TO ERROR REPORTS FROM FLIGHT SOFTWARE. ENABLED IN SAFE MODE, CONTINGENCY MODE AND EMERGENCY MODE.

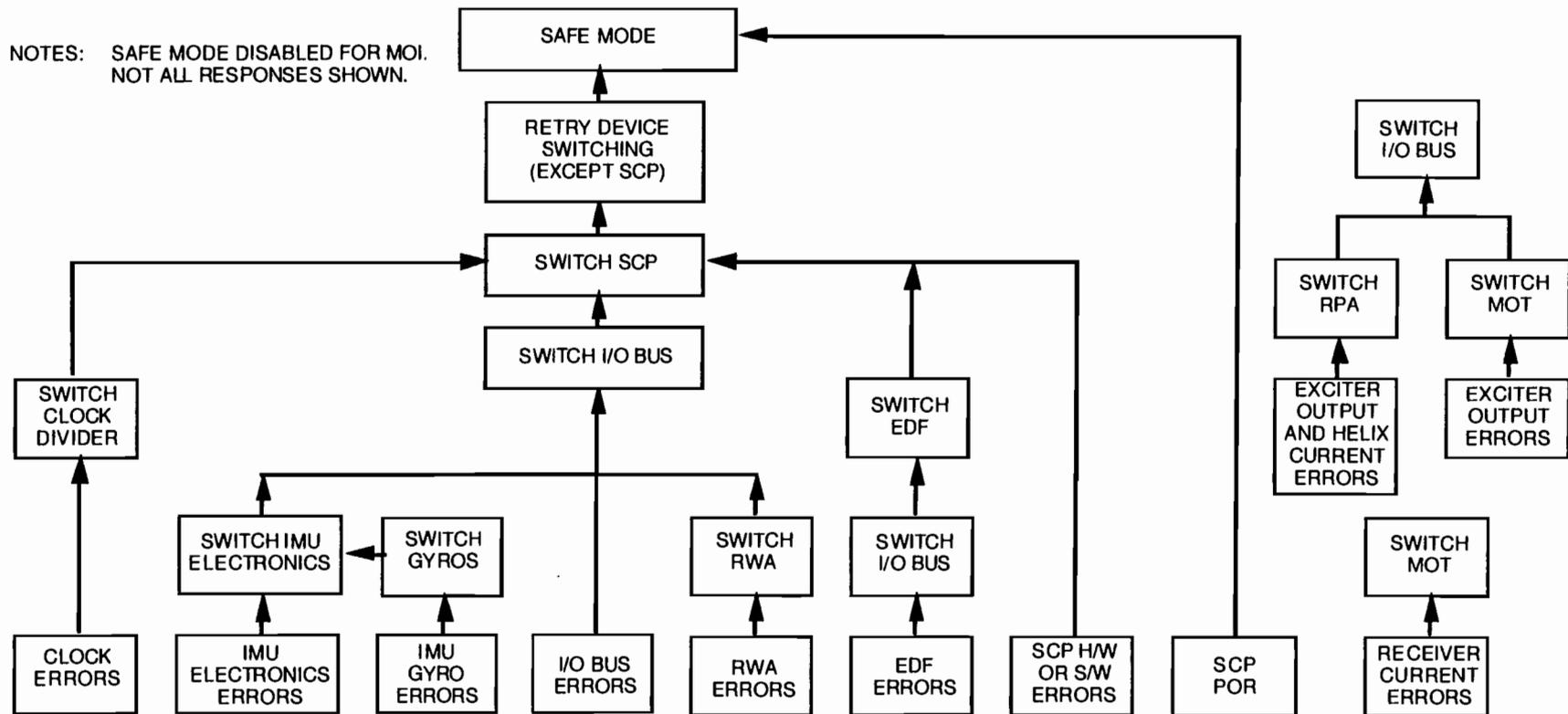


Figure 5-8. General REDMAN response block diagram.

be due to a lack of understanding either that this failure could occur or of the effects of this failure and the resulting software design and test deficiencies.

Post-launch, a potentially serious design flaw was discovered in the EDF flight software's handling of the EDAC—the software was correcting the wrong address. This error was fixed by an in-flight patch.

The gyro-motor-short FP software had been disabled since before launch. This fact was not widely known and was discovered by the Mars Observer Flight Team during preparations for MOI. Rather than make a change near MOI, this FP function remained disabled for MOI.

Entry into Contingency Mode (CM) does not guarantee that a downlink signal will be sent by the spacecraft. An undesirable interaction was discovered between the CM response and a sequenced STRPAN spacecraft expanded block which turns the RPA on. STRPAN begins by turning the RPA off and then delays about 4 min before turning the selected RPA on. If CM entry occurs before the RPA is turned on, the remaining STRPAN response is canceled. The CM response, detecting the RPA off, does not turn the RPA beam back on as was intended by the canceled STRPAN response. This design is certainly undesirable, and is possibly a serious flaw that prevented acquisition of telemetry in one of the hypothesized failure scenarios (gyro motor short).

Though it appears unrelated to the loss-of-signal anomaly, flight software entered CM a number of times during the mission due to attitude propagation errors. A JPL tiger team discovered two bugs in the star processing software, one of which had survived years of use in Earth orbit on other programs.

There is incomplete FP coverage. Examples include the RXO and gyro-motor-short potential failures. Generally, the FP approach is focused on low-level components and functions. There is limited functional level FP capability, although some is found in AACS maneuver mode software. In this sense, the FP software is not very robust.

Fault protection testing in the spacecraft environment was extremely limited in scope. The majority of this test activity was performed on the RAID simulator and in the VTL. In effect, there was no system-level fault protection test program performed on the spacecraft.

A major fault protection test program in the VTL was undertaken throughout the summer of 1992. The lateness of this test program guaranteed that any problems discovered would not be included in the flight software program in ROM launched with the spacecraft. Flight software testing relied heavily on the use of the VTL. The VTL fidelity to simulate the operation and failures of the RXO and CIU timing chain was inadequate.

Independent validation of the commercial multitasking operating system was not performed. Reliance was placed on vendor test results and experience. Any residual

problems were expected to be uncovered during the normal development process. The Project approved this approach. Experience by other users indicated it to be a stable and bug-free product. No problem was ever found, and no fix was ever required or made.

C. Command and Data Handling Subsystem

1. *Description of Subsystem*

The Command and Data Handling Subsystem (C&DH) is the complex brain of the spacecraft (Figure 5-9), and is composed of 23 assemblies (components or boxes) and 10 assembly types. These components are listed and described below.

The CIU receives and decodes uplink commands, including hardware-decoded commands that control critical subsystem functions such as SCP control and power off/on; directs data transmissions to one or both SCPs; receives data and control signals from spacecraft subsystems and provides them as inputs to the SCPs; sends data and control signals from the SCPs to spacecraft subsystems; provides clock signals to other spacecraft components derived from the RXO; provides common +10-V power to other spacecraft components to power their electrical signal interfaces; and is one-unit internally redundant (e.g., input/output buses and clock dividers), except for some critical selection and control functions.

The Controls Interface Extender (CIX) is an extension of the CIU, but is limited to serial and parallel input/output functions, and is one-unit internally redundant.

The Cross-Strap Unit (XSU) routes data between the EDF, DTRs, PDS, and MOTs; routes control and configuration commands to the DTRs; routes DTR playback data to the MOTs; convolutionally encodes and modulates data routed to the MOTs; controls the downlink data rate; and is one-unit internally redundant. This component is not required to achieve a downlink carrier.

There are three Digital (magnetic) Tape Recorders (DTRs). Each has eight record/playback tracks; starts record and playback on track 1 and automatically stops at the end of the tape on track 8; and two of the DTRs have a tape transport unit (TU) and an electronic unit (EU), and the third DTR has two TUs and one EU. This component is not required to achieve a downlink carrier.

The EDF collects spacecraft analog and digital telemetry according to predefined collection formats; maintains the primary spacecraft clock which is inserted into the spacecraft engineering telemetry; sends to the SCP EDF self-test messages and special telemetry messages that are used for spacecraft fault protection; uses a 1750A computer with a program in ROM, RAM-patching capability, and memory EDAC; and consists of two units—one is powered, the other is a cold (unpowered) backup. This component is not required to achieve a downlink carrier.

The Payload Data Subsystem (PDS) is the command and telemetry interface between the science payload and the C&DH; conveys spacecraft commands to the payload; distributes spacecraft time and timing to the payload; collects source packets from the payload; forms Reed–Solomon encoded telemetry transfer frames and provides them to the XSU; and is one-unit internally redundant, with one as a cold spare. This component is not required to achieve a downlink carrier.

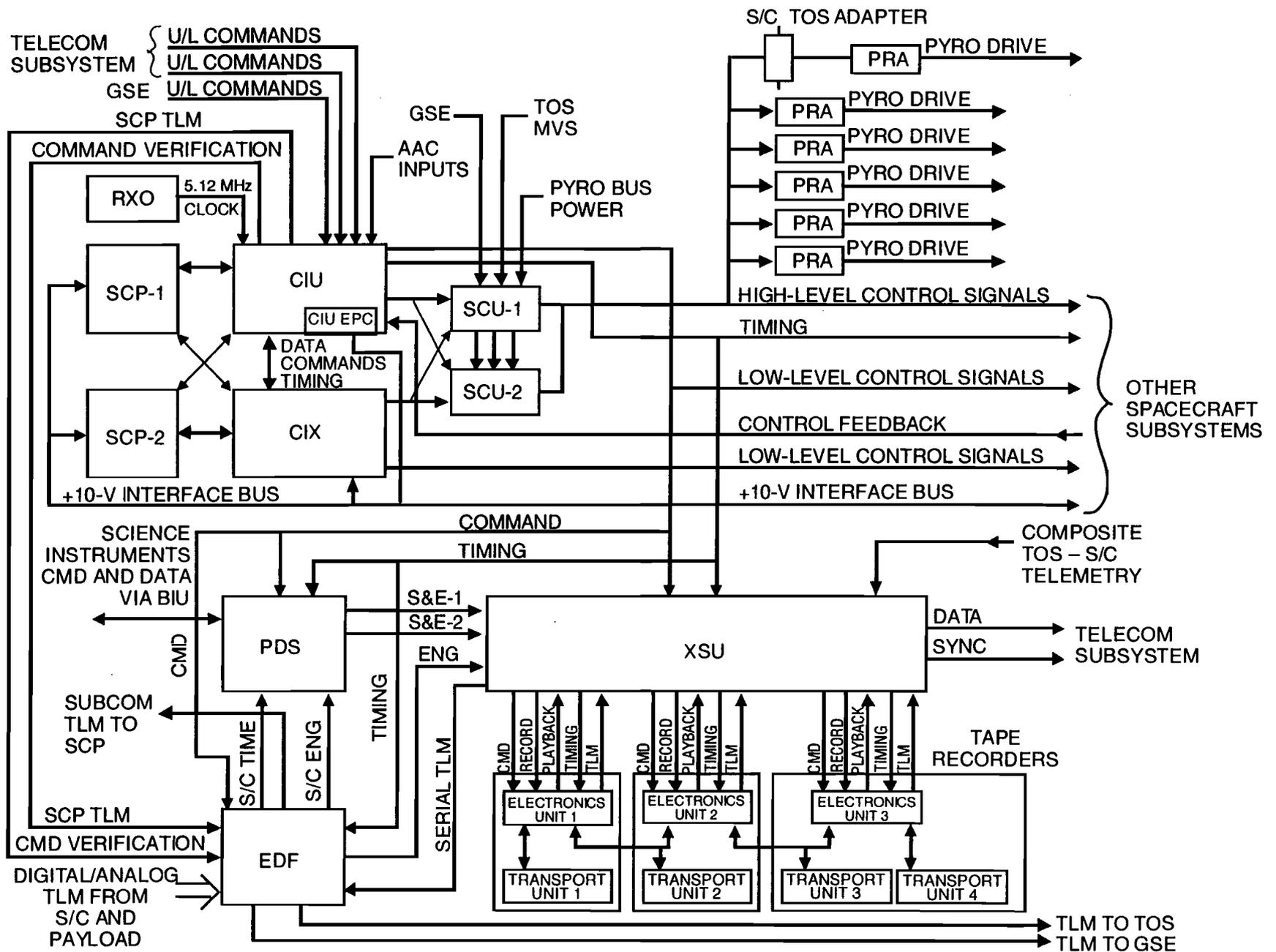


Figure 5-9. C&DH block diagram.

The Pyrotechnic Relay Assembly (PRA) provides commanded firing current to the electroexplosive devices; contains seven primary and seven backup firing circuits in each PRA; each circuit uses an inhibit nonlatching relay, with two series-inhibit latching relays in the SCU; contains five units, one of which separates with the TOS; and each unit is internally redundant. This component is not required to achieve a downlink carrier.

The Redundant Crystal Oscillator (RXO) provides a highly stable primary timing reference for the C&DH and the rest of the spacecraft, and is one-unit internally redundant with automatic switchover if the selected side fails. (See Chapter V.D for further details.)

The SCP is a reprogrammable 1750A computer; uses both ROM and RAM with memory EDAC; and contains two units—one is in control and the other is a hot backup. The SCP processes the flight software and redundancy-management functions described earlier in this report.

The Signal Conditioning Unit (SCU) contains most spacecraft relay functions. Each relay function is individually controlled by the CIU or the CIX. Relay functions include subsystem power switching, electroexplosive device enable-and-arm functions, thruster and engine valve control, and heater control. There are two units: one controls primary relay functions and the other controls backup functions. SCU-1 includes a special RPA beam on/off interlock to prevent both beams from being turned on simultaneously, and a special SCP power on/off interlock function to prevent both SCPs from being powered off simultaneously. All relay functions are separately powered at all times.

The C&DH design uses extensive redundancy and cross-strapping internal to components, and some external cross-strapping between redundant components. Although the subsystem design has extensive heritage from Astro Satcom and DMSPs, a few significant changes were incorporated for Mars Observer. The 1750A computer designs for the SCP and EDF were new. The EDF divider chains were substantially changed to convert from a time-division-multiplex to a quasi-packet telemetry scheme. The XSU-to-MOT interface was a new design for Mars Observer.

2. Method of Analysis

A combination of documentation review and VTL simulations was used. Design, analysis, and as-built documentation were reviewed, including performance specifications, schematics, assembly drawings, and some code listings. VTL simulations were used to understand subsystem responses to postulated failure scenarios, commands, and scripts, and to confirm flight software and fault protection responses. This was especially true for understanding the role that the C&DH played in the spacecraft system response to postulated failures.

3. Potential Failure Modes

There are potential single failure points that could explain the observed loss of signal. Some new ones were identified during this review. Most are credible but very

unlikely. These potential single failure points are discussed later in this report and are briefly summarized here.

Analysis now shows that a single failure of a suspect part (JANTXV2N3421 transistor) in the RXO can prevent the primary- or backup-side frequency source output of the RXO from being supplied to the CIU. This potential failure of the RXO had not been widely known or well understood. Analysis of an RXO primary-side output failure shows that REDMAN software in the SCP does not correct this failure, resulting in a partially functioning C&DH and many unanticipated and unintended system responses.

The CIU contains nonredundant critical control circuits. Potential critical control circuit failures caused by an internal part failure or perhaps induced by a pyro-firing electromagnetic spike have been identified.

Failure of the SCP in-control circuit such that neither SCP is selected can prevent effective spacecraft control. Failure of the input/output bus crossed/not-crossed circuit or input/output bus select A/B circuit such that neither bus is selected can also prevent effective spacecraft control. These potential failures are discussed in Hypothesis C5.

Failure of the backup RXO select circuit such that it is noisy or oscillating can compromise some or all primary and backup CIU clocks and prevent effective spacecraft control. This potential failure is discussed in Hypotheses S3 and C15.

Failure of the IMU select circuit such that it is noisy or oscillating can corrupt gyro data for all axes and result in loss of attitude control. This potential failure is discussed in Hypothesis C15.

A failure of the CIX output interface circuit (failed high) to the SCU RPA Beam On circuit or a failure of the SCU RPA Beam On power circuit (failed on) can prevent both RPAs from ever being turned on if the RPA filaments are off, which they were during the pressurization sequence. These potential failures are discussed in Hypothesis C16.

A potential failure in the +10-V power for CIU critical control circuits, including SCP in control, input/output bus crossed/not crossed, and input/output bus select A/B can also prevent effective spacecraft control. This potential failure is discussed in Hypothesis N7.

4. Other Comments

The loss-of-signal event caused the Flight Team to postulate potential failures and generate and test recovery commands not before tried. This resulted in discovery of a C&DH design flaw. The SCP Restart command was discovered not to function properly (during VTL testing). SCP Restart is a basic but important function of the C&DH CIU. Sending this command will hang up the interface between the SCP and CIU, resulting in the CIU being unable to send commands to the SCP through its dedicated, and only, uplink processor. This command was subsequently never sent.

It is highly improbable that a circuit error or failure in a C&DH component, an error in the wiring harness, or an error of the pyro firing sequence occurred that would have further deployed the HGA or SA, or produced a reverse order firing of pyro valves that could have contributed to the loss-of-signal anomaly.

The Board does not think that the PDS or science payload is involved with the anomaly.

D. Redundant Crystal Oscillator

The redundant crystal oscillator (RXO) provides timing signals that are distributed widely within the spacecraft. The signals are provided as 5.12-MHz square waves at two buffered outputs of the RXO. These outputs interface to two clock-divider chains in the CIU. The RXO outputs are the time base for generation of clock time within the spacecraft.

Internally the RXO consists of two ovenized quartz crystal oscillators, two power supplies, two buffer amplifiers, failure detection, and switch-over logic circuitry. In normal operation, all elements of the RXO are powered and available for immediate use.

The primary power supply provides power for the primary oscillator, the failure detectors, and the portion of switching circuitry that enables the RF signal to buffer A. The backup power supply provides power for the backup oscillator and the portion of switching circuitry that provides the RF signal to buffer B. The buffer amplifiers are powered by the spacecraft 10-V bus and are not dependent on the RXO power supplies.

Telemetry signals are provided from the RXO as follows:

- (1) A binary output level used to set a status bit indicating which side of the RXO is driving the two outputs
- (2) An analog output level to provide a calibrated measurement of the primary oscillator inner oven temperature
- (3) An analog output level to provide a calibrated measurement of the backup oscillator inner oven temperature

The failure detector circuitry examines the 5.12-MHz output power from each of the two oscillators and oven temperature from the primary oscillator only. Based on those three inputs the failure detector circuit controls the switch-over logic. All internal RXO control is autonomous, asynchronous, and has no latching or memory.

Selection of the RXO state (primary or backup) is performed by spacecraft command. The command is received by the RXO as a short between two wires in the RXO power connector. When shorted, the backup oscillator is selected. When there is an open circuit or the RXO is driven with a logical "one" level, the primary oscillator is selected. Regardless of which side is selected, the selection can be overridden by the internal failure detection circuitry if a failure should occur.

There are four 2N3421 transistors in the RXO, all from the suspect lot (Unitrode date code 8350). One 2N3421 is used as a series regulator in each of the RXO power supplies, and one 2N3421 is used as a power control transistor in each of the outer oven controllers.

The suspect transistors in the outer oven controllers are not a serious problem since a failure of either (or both) would not disable any functionality of the RXO. In such an

event, the inner oven controller would attempt to compensate for the loss of outer oven heater power. Even if the inner oven were unable to fully compensate, the oscillator would still provide valid outputs, although with a poorer frequency stability.

When power is applied to the RXO, it automatically switches to the backup oscillator, regardless of which oscillator side has been selected by the CIU. This happens because the primary oscillator oven temperature is initially cool and the failure detection circuitry senses a failure. The RXO will autonomously switch to the primary oscillator side, as soon as the temperature check is satisfied, if the primary oscillator has been previously selected by the CIU.

A failure of the power supply on either side of the RXO will terminate the RXO output from the corresponding buffer amplifier. This happens because the switching logic to route the signal to the buffer amplifier becomes unpowered on the failed side and no signal routing occurs.

The RXO internal fault protection results in a finite set of predictable states. The states identify which oscillator (primary or backup) is driving the two output ports. State tables for the RXO are shown in Tables 5-4 and 5-5 for selection of the primary and backup sides, respectively. Those tables have been augmented to show the resulting states when a power supply failure has occurred on either the primary or backup side. The tables define which oscillator is active in driving the output(s) and the status of the output buffer. When a buffer is marked "fail," there is no output signal provided to the corresponding clock divider in the CIU.

Table 5-4. State table for Mars Observer RXO when primary oscillator is selected by CIU.

Primary Amplitude	Backup Amplitude	Temperature Primary	Primary Power Supply	Backup Power Supply	Active Oscillator	Buffer A Out	Buffer B Out
OK	*	OK	OK	OK	Primary	OK	OK
OK	OK	Fail	OK	OK	Backup	OK	OK
Fail	OK	*	OK	OK	Backup	OK	OK
Fail	Fail	OK	OK	OK	Primary	?	?
Fail	Fail	Fail	OK	OK	Primary	?	?
OK	Fail	Fail	OK	OK	Primary	OK	OK
OK	Fail	*	OK	Fail	Primary	OK	Fail
Fail	Fail	*	OK	Fail	Primary	?	Fail
Fail	OK	*	Fail	OK	Backup	Fail	OK
Fail	Fail	*	Fail	OK	Backup	Fail	?
Fail	Fail	*	Fail	Fail	—	Fail	Fail

* State does not matter.

? Possible low-power output.

Table 5-5. State table for Mars Observer RXO when backup oscillator is selected by CIU.

Primary Amplitude	Backup Amplitude	Temperature Primary	Primary Power Supply	Backup Power Supply	Active Oscillator	Buffer A Out	Buffer B Out
*	OK	*	OK	OK	Backup	OK	OK
OK	Fail	*	OK	OK	Primary	OK	OK
Fail	Fail	*	OK	OK	Primary	?	?
OK	Fail	*	OK	Fail	Primary	OK	Fail
Fail	Fail	*	OK	Fail	Primary	?	Fail
Fail	OK	*	Fail	OK	Backup	Fail	OK
Fail	Fail	*	Fail	OK	Backup	Fail	?
Fail	Fail	*	Fail	Fail	—	Fail	Fail

* State does not matter.
 ? Possible low-power output.

E. Attitude Control

1. Description of Subsystem

The AACS on Mars Observer has hardware (Table 5-6) and software components that are used in different ways, depending on the AACS mode (Table 5-7).

Table 5-6. AACS hardware components.

Item	Full name	Description
CSA	Celestial Sensor Assembly	Slit-type star scanner with 6 slits (two sets of three). Honeywell. NR.
IMU	Inertial Measurement Unit	Three 2-axis spun-mass rate-integrating gyros. Any 2 out of 3 provide full 3-axis attitude change information. Honeywell IMU with Teledyne gyros.
MHSA	Mars Horizon Sensor Assembly	Horizon sensor for on-orbit operations. Barnes. NR.
4 π SS	4 π Steradian Sun Sensor	Five primary pairs of single-axis heads. Each head pair covers a $\pm 64^\circ$ by $\pm 64^\circ$ FOV. Taken together, the set of five pairs covers most of the celestial sphere, with known coverage gaps. Five additional head pairs provide redundancy. Adcole.
RWA	Reaction Wheel Assembly	Four wheels in a three-orthogonal plus skew configuration. Any 3 out of 4 provide full 3-axis attitude control. Astro.

Note: NR is used to denote "not required for establishing downlink."

Table 5-7. AACS modes.

Mode	Function	Hardware used
Sun-Comm-Power	Acquires and maintains Sun pointing, spins the spacecraft about the Sun line	RWA, 4 π SS, IMU
Sun-Star-Init	Same as above and initializes star processing	RWA, 4 π SS, IMU, CSA
Array Normal Spin (ANS)	Controls Solar-Array-normal axis to a commanded inertially referenced direction	RWA, 4 π SS, IMU, CSA
Inertial Slew/Hold	Controls to a commanded 3-axis attitude (and rate)	RWA, 4 π SS, IMU
Maneuver	Controls to a commanded 3-axis attitude during ΔV maneuvers; terminates burn upon completion	Thrusters, 4 π SS, IMU
Deploy Control	Attitude allowed to drift, RWAs kept above 200 rpm	4 π SS, IMU
Others	Sun-Stuck-Gimbal (to be used after Solar Array deploy), Mapping, CSA backup (for mapping), DSN ISH (launch day only), Launch Tach (launch day only), and Search (for mapping)	Various

AACS software involved in reestablishing the downlink includes hardware interface, attitude determination, RWA attitude control, Sun monitor, and momentum-unloading software. Additional AACS software is not required for downlink: star-processing, ephemeris, HGA and Solar Array gimbal drive, and maneuver control software.

a. Pressurization Sequence

Before the pressurization sequence began, AACS was in Array Normal Spin (ANS) Mode, spinning about the spacecraft Y-axis at a controlled rate of one revolution every 100 minutes. The Y-axis was Earth-pointed, allowing HGA communications. The phase angle of the spacecraft orientation about the Y-axis was uncontrolled—just the rate was controlled.

The spacecraft momentum at RPA Beam Off was $[-4.4, 7.4, -2.9]$ Nms about the X-, Y-, and Z-axes, respectively. The angular momentum magnitude was about 9 Nms.

The Deploy Control Mode came next in the sequence for AACS. In Deploy Control Mode, no attempt is made to control the attitude of the spacecraft. RWA control is only charged with assuring that all wheels are kept above 200 rpm. The skew wheel, which was off, is quickly (in less than 10 s) spun up to 200 rpm and held there. The other wheels, which had initial speeds in excess of 200 rpm, are allowed to coast down.

The spacecraft response to the cessation of control and the rapid skew wheel spin-up is shown in Figure 5-10, HGA offset from Earth line during pressurization. Note that this figure shows two scenarios: the nominal, planned sequence, and the situation if all attitude control is halted. The nominal response has the HGA deviating by about 18° from the Earth line during Deploy Control Mode, then rapidly returning to an error of less than 2° before the Beam On command.

Figure 5-11 shows the relative locations of the Earth, Sun, and total spacecraft angular momentum vector at the time of pressurization.

b. AACS Comments

Except during propulsive events, Mars Observer relies exclusively on reaction wheels for attitude control. Even though the thruster configuration would support a thruster-based attitude control algorithm, there is no thruster-only attitude control mode available. Any three wheels can provide attitude control (although the power requirements are higher and the angular acceleration is lower if the skew wheel is used). The reaction wheel redundancy management depends on a “passive wheel test,” which is disabled when in Deploy Control Mode, when wheel speeds are above 6000 rpm, or for small torque commands.

Attitude propagation for the period of interest is based on the IMU. The CSA is not used again until such time as the Y-axis pointing error is small and commanded array

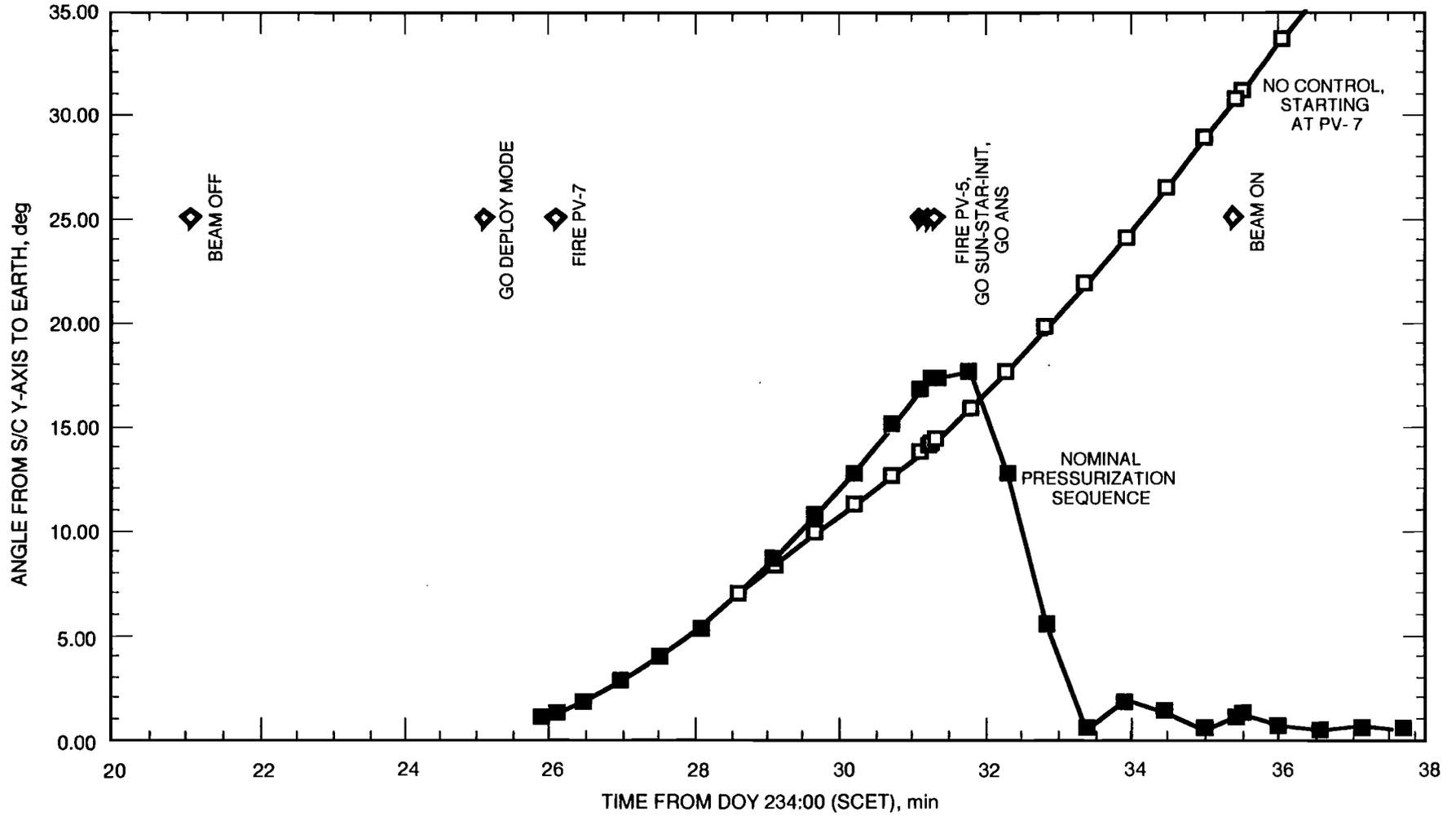


Figure 5-10. HGA offset from Earth line during pressurization.

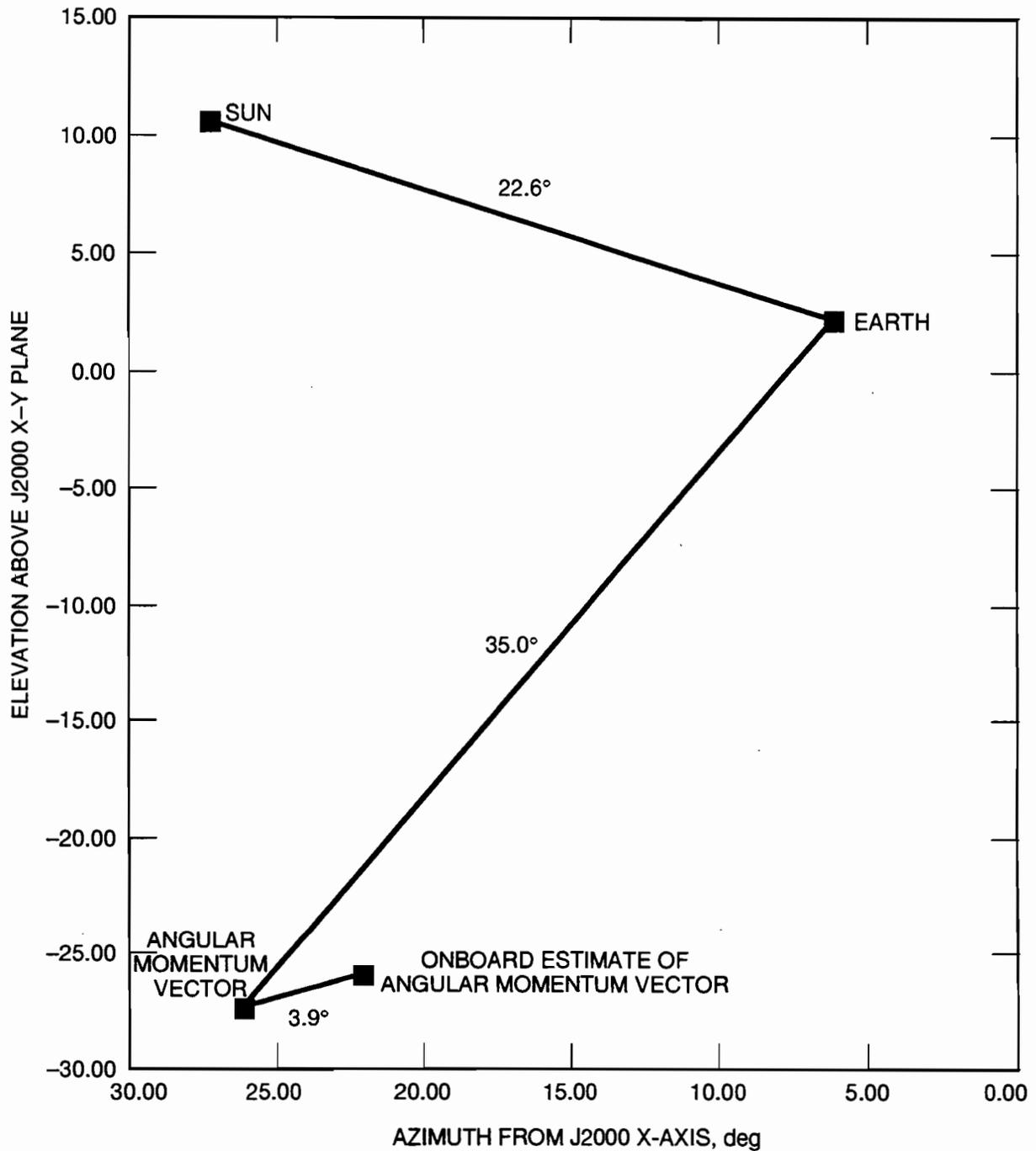


Figure 5-11. Initial conditions at RPA Beam Off.

normal spin has been established with accurate rates. The 4π SS is not used except as a check on the IMU-propagated attitude until such time as an attitude knowledge loss is declared. In that case, the spacecraft will use the 4π SS to search for the Sun, turn the Y-axis toward the Sun, and (if so commanded) try to reestablish inertial attitude knowledge using the CSA.

AACS fault protection is mostly redundancy management rather than functional fault protection. Low-level tests, such as the passive wheel test, are used to determine when to use redundant units, but there is no test for excessive attitude-control error for an unacceptable duration. This means that there are numerous failure scenarios in which attitude control is not maintained, but no response (e.g., enter Contingency Mode, enter Safe Mode, switch to LGA, or establish downlink) is triggered as a result.

A number of redundancy-management checks have been designed for the IMU. The most significant one with regard to mechanical gyro problems is the gyro co-axis miscompare. Since the redundant gyro channels are all active, there is a continuous check to make sure that the redundant axes agree with each other to within a tolerance. This check was enabled at the time of the anomaly.

2. Method of Investigation

Simulations were used as a primary means of determining whether a specific scenario met the observables.

The VTL includes the onboard flight software and simulated rigid-body spacecraft dynamics, and operates in real time. It was used to investigate the attitude-time history for those failure scenarios where the C&DH and Telecommunications Subsystems were working, but AACS failures were causing difficulty in antenna pointing. The scenario-by-scenario results are discussed in Chapter VII, but often the result was a conclusion that there was a very high likelihood of (at least) LGA coverage of sufficient duration and frequency that the scenario was inconsistent with the observables.

A dynamics-only simulation was used to augment the VTL in those cases where the flight software or real-time features of the VTL were not needed, such as a sudden and permanent cessation of control. When exercised, the dynamics-only simulation demonstrated ample opportunities for LGA communication to Earth (but very limited HGA opportunities).

In a number of scenarios, the spacecraft nutates uncontrolled about a fixed angular momentum vector. There is no purposely designed nutation damper on the spacecraft, but propellant slosh and appendage flexing provide a low level of damping. The nutation damping time constant was analyzed for several possible scenarios.⁶ The analysis shows time constants of about a year for spin rates up to $0.2^\circ/\text{s}$. The time constant drops to about 10 days for a spin rate of $7.5^\circ/\text{s}$. Since propellant slosh dominates, the damping analysis has high uncertainty, but is useful as a rough gauge of nutation damping.

⁶ S. W. Sirlin, *Passive Nutation Damping of Mars Observer*, JPL Interoffice Memorandum 343-93-374, Jet Propulsion Laboratory, Pasadena, California, November 5, 1993.

3. *Potential Failure Modes*

After investigating several possibilities, it appears highly unlikely that a single AACS failure can explain the observed initial and persistent loss of signal. Possibilities considered that do not explain initial and persistent loss of signal include:

- (1) “No-control” attitude drift (angular momentum vector known)—would give frequent opportunities of sufficient duration to see LGA and HGA downlink (DL)
- (2) Sun sensor locked on Mars—would give opportunities for LGA DL in the first hour or so after planned acquisition of signal (AOS)
- (3) Reaction wheel runaway—would give opportunities for LGA DL in the first hour or so after planned AOS
- (4) Reaction wheel stall—covered by redundancy management

Of all the functional AACS failures examined, the one that cannot be completely ruled out is a massive gyro spin motor short. This scenario is developed in Chapter VII.V. Note that no causal connection has been found between this type of failure and the pressurization sequence, and no such failures have ever been observed.

4. *How AACS Influences System Response to Other Faults*

The controlled or uncontrolled dynamics are of interest in many scenarios to help assess the likelihood of pointing the HGA or LGA in a manner that allows downlink or uplink. Table 5-8 shows the resulting spacecraft angular velocities for selected scenarios. The first entry shows the planned ANS spin rate. The next entry shows the eventual steady-state spin rate based on all the momentum in the wheels transferring to the spacecraft and increasing the spacecraft angular velocity. The remaining entries show the spacecraft angular velocities resulting from spinning up a single RWA to the absolute limit, spinning up all wheels to the preset RWA hardware speed limit, allowing a helium leak to spin up the spacecraft, and allowing the monopropellant thrusters to spin up the spacecraft.

Table 5-9 shows what capabilities are lost at various spacecraft angular velocities. For entries dealing with the LGA, the postulated rate is perpendicular to the antenna boresight. A rate above $16^\circ/\text{s}$ perpendicular to the LGA boresight is sufficient to prevent a downlink and a rate above $78^\circ/\text{s}$ will cause damage to the Solar Array.

In the case of a primary-side timing loss attributed to an RXO transistor failure, AACS would lose control of the RWAs, but would retain faulty information on the wheel speeds. As the wheels coast down and transfer their momentum to the spacecraft, the flight software will, in three out of four cases, trigger a momentum unload due to the sum of the correctly measured spacecraft angular momentum and the incorrectly measured wheel momentum. These wheel unloadings reposition the angular momentum vector, but this repositioning does not interfere with LGA communications. In the fourth case, there is no momentum unloading. Dynamic simulations show that there should be no additional unloadings for days—allowing good LGA-to-Earth viewing for all cases.

Table 5-8. Mars Observer angular velocities for selected scenarios.

Event	Rate, rad/s	Rate, deg/s	Rate, rpm	Period, min	Momentum, Nms
ANS spin	0.001	0.06	0.01	100	3
Flat spin at RPA Off momentum	0.003	0.17	0.03	35	9
One wheel at 9000 rpm (Y-axis)	0.014	0.77	0.13	7.8	41
One wheel at 9000 rpm (Z-axis)	0.027	1.55	0.26	3.9	41
Spin up all wheels to 6500 rpm: min.	0.021	1.20	0.20	5.0	63
Spin up all wheels to 6500 rpm: max.	0.028	1.58	0.26	3.8	83
Worst-case helium leak: 4000 Ns at 1-m moment arm about Y-axis	1.3	76	13	0.08	4000
Worst-case helium leak: 4000 Ns at 1-m moment arm about Z-axis	2.7	153	25	0.04	4000
Exhaust monopropellant on wheel unloads (worst case, all momentum in same inertial direction)	27	1528	255	0.004	40,000

Table 5-9. Mars Observer angular velocities at which certain capabilities are lost.

Event	Rate, rad/s	Rate, deg/s	Rate, rpm	Period, min	Momentum, Nms
Turn through 180° LGA beamwidth in 100 s (Arm and Go Contingency command time)	0.03	1.8	0.3	3.3	47
Turn through 180° LGA beamwidth in 40 s (Beam On uplink command time)	0.08	4.5	0.8	1.3	118
Turn through 56° HGA beamwidth in 10 s (minimum downlink detection time)	0.10	5.6	0.9	1.1	147
IMU software limit (Y-axis)	0.13	7.4	1.2	0.8	387
IMU software limit (Z-axis)	0.13	7.4	1.2	0.8	194
IMU hardware limit (Y-axis)	0.16	9	1.5	0.7	471
IMU hardware limit (Z-axis)	0.16	9	1.5	0.7	236
Turn through 160° LGA beamwidth in 10 s (minimum downlink detection time)	0.28	16	2.7	0.4	419
Structural damage (SA boom bending) ^a	1.4	78	13	0.08	2042

^a C.-Y. Peng, *Structural Capability Analysis for the MO Deployed Appendages Under Spin Induced Loads—GRS, MAG, and SA Subsystems*, JPL Interoffice Memorandum 3543:93:182:CYP, Jet Propulsion Laboratory, Pasadena, California, October 19, 1993.

F. Power Subsystem Description

The Mars Observer Power Subsystem is a direct energy transfer type. It provides a regulated 28-Vdc power bus to the spacecraft subsystems, where local conversion takes place.

1. Primary Power

The primary power source is normally the Solar Array. Other operation is by sharing with the batteries through the boost voltage regulator (BVR) or battery operation alone (boosted) to maintain bus regulation when array power is unavailable.

Solar panel capability is about 1000 W in cruise configuration and about 1500 W at perihelion in Mars orbit when panels 5 and 6 are deployed. A mode controller and a Partial Shunt Assembly (PSA) maintain bus voltage regulation within the capability of the array by diverting a portion of the available current. The two batteries can provide about 1600 W-h of energy, conservatively, and about 30 A to the bus at 28 Vdc through the boost voltage regulator. The batteries are charged by separate and redundant battery charger assemblies (BCAs) from the 28-Vdc bus.

Most elements of the primary power system are either block or functionally redundant.

a. Battery Charger Assembly

- (1) Separate charger for each battery, with an independent charge rate control
- (2) Primary and backup circuitry
- (3) 15-A maximum charge rate per battery, with a maximum total of 25 A

b. Power Supply Electronics (PSE)

- (1) BVR with five channels, any four will supply 24-A output
- (2) Redundant mode controller
- (3) Automated switchover to backup units for failure mode operations
- (4) Independent battery charge controls
- (5) 16 V/T limit curves (8 + 8 shifted) for battery charge control

c. Partial Shunt Assembly

- (1) 30 circuits, each capable of handling up to 5 A, nominally (2 A for Mars Observer)
- (2) Each circuit uses five transistors in parallel
- (3) Each circuit mounted on a separate strip
- (4) A common drive from the PSE; primary and backup

Although not a part of the Power Subsystem, organizationally, the pyros are electrically and redundantly "fired" directly from the two batteries: Side A from Battery 1 and Side B from Battery 2. Firing surges are thus not carried by the 28-V bus.

The primary system power return is tied directly to the chassis at two places (single-point grounds) with no isolation. This results in the system being vulnerable to a catastrophic high-side short to chassis, within the primary Power System, and also permits unintended current flow in the chassis under certain conditions.

This type of Power System grounding design has been used by the commercial aerospace industry for hundreds of Earth-orbiting spacecraft, but is not used on JPL-designed planetary spacecraft.

2. Potential "High-Side" Short to Chassis

There are three catastrophic "high-side" short to chassis (and therefore 28-V return) failure modes:

- (1) Solar Array only
- (2) Battery only
- (3) Both Solar Array and battery

In all cases, these shorts or overloads occur through failure of electrical insulation between Power System elements and the chassis. This electrical insulation is intrinsically not robust because of the requirement for a good thermal path as well as electrical isolation. Insulating thickness dimensions are very small (a few mil) and, as a result, there is considerable sensitivity to quality control during fabrication.

3. Previous Power System Failures

a. Mariner II (1962)

One of two solar panels was lost due to shorting to substrate. The mission was not lost because the remaining output was sufficient. This was the last time JPL designed a spacecraft without isolation between the primary power return and structure.

b. NOAA-I (1993)

Failure occurred because the total Solar Array output was shorted to chassis in the battery charger assembly when isolation between the electronics heat-sink and radiator failed. The three batteries provided about four hours of operation after the failure.

The Mars Observer failure is possibly due to a similar, although not necessarily identical, fault in the Power System electronics. To be consistent with the observables, it is necessary to sustain a short that overloads *both* the Solar Array and battery sources.

G. Telecommunications Subsystem

The Mars Observer Telecommunications Subsystem (“telecom”) is a unified X-band design that provides for all uplink and downlink communications with the spacecraft. Tracking is provided by the DSN with 34- and 70-meter stations at three signal processing complexes situated around the Earth. All critical elements of the Telecommunications Subsystem are block or functionally redundant to assure communications reliability.

The telecom design incorporates three LGAs and one HGA. Two of the LGAs are receive-only and the third is transmit-only. The HGA can simultaneously receive and transmit. It is the common practice of mission operators to select the HGA when the spacecraft attitude can be assured to keep the narrow beam pointed toward Earth (half-power beamwidth $\approx 1.6^\circ$).

1. *Transmitting Functions*

Telecom transmitting functions are fourfold: carrier generation, telemetry data modulation, ranging video modulation, and differenced one-way range (DOR) tone modulation. The downlink signal may be transmitted either through the transmit LGA or the HGA.

The downlink carrier is generated by exciters in the Mars Observer Transponders (MOTs). Only one of the two MOT exciters should be used at any time. The carrier frequency reference may be selected from three different sources:

- (1) The MOT receiver, if phase-locked, may be utilized to generate a downlink carrier that is phase-coherent with the uplink with a turnaround ratio of 880/749. Normally this source will automatically be selected whenever uplink phase-lock occurs. However, automatic switching can be disabled by command, resulting in a noncoherent downlink even when uplink phase-lock has been achieved.
- (2) Each exciter has a free-running crystal oscillator, known as the auxiliary oscillator, that can be utilized to generate the downlink carrier.
- (3) There is a single free-running crystal oscillator, known as the Ultra Stable Oscillator (USO), which is external to telecom, that can be utilized to generate the downlink carrier. This oscillator has better frequency stability than the auxiliary oscillators and is used to enhance the value of radio science data acquired during the mission.

Telemetry data are modulated on the downlink carrier in the exciters of the MOTs. The telemetry data stream is created by the C&DH Subsystem with coding and subcarrier modulation performed in the Cross-Strap Unit (XSU). A level-dependent interface is provided between the XSU and the exciters to affect different downlink telemetry modulation indices as required by the mission.

The demodulated ranging video signal described in the next subsection can be used to additionally modulate the downlink carrier. When this function is enabled, the uplink ranging code is turned around at the spacecraft, allowing two-way range measurements at Earth.

Finally, it is possible to modulate a pair of wideband sinusoidal tones onto the downlink carrier to enable DOR measurements upon receipt at Earth. The capability is used a small fraction of the time during the mission to provide for spacecraft navigation with enhanced accuracy. The DOR tones can be modulated simultaneously with telemetry and ranging, as link margins permit.

2. *Receiving Functions*

Telecom receiving functions are threefold: carrier tracking, command demodulation and detection, and ranging code demodulation.

Carrier tracking is performed by two redundant receivers in the MOTs that operate simultaneously and continuously. When the receivers are phase-locked to an uplink carrier, the resultant signal can be used to coherently excite the downlink to enable Doppler tracking.

Command demodulation is performed in two serial steps. First, the transponder receivers demodulate the uplink carrier to provide a command subcarrier to two redundant CDUs. The CDUs then demodulate the command subcarrier and perform bit synchronization. The synchronized serial data stream is provided to the C&DH. Uplink command data rates can be independently selected at each CDU from a set of rates, each being defined by $500/2^n$ bps, where n can range from 0 to 6 in integer steps.

Ranging code demodulation is performed internally to the MOTs and the resulting baseband ranging code can be used to modulate the downlink carrier for turnaround range measurements. The video noise bandwidth of the turnaround ranging channel is nominally 1.5 MHz.

H. Propulsion Subsystem

1. *Description of Subsystem*

The Mars Observer Propulsion Subsystem consists of the monopropellant and bipropellant elements shown schematically in Figures 5-12 and 5-13, respectively.

The monopropellant element is a conventional blowdown design of a type extensively used by Astro and other spacecraft manufacturers for nearly two decades. In this system, two hydrazine tanks supply propellant to any of 12 catalytic hydrazine thrusters. The thrusters are arranged in two redundant branches, each of which contains four 4.45-N thrust units and two 0.9-N thrust units.

The bipropellant element is a pressure-regulated propulsion system using four 490-N thrust main engines to provide ΔV and four 22-N thrust engines to provide thrust vector control (TVC). In normal operation, only two of the 490-N engines are operated at a time; the second pair provides redundancy. The gaseous helium (GHe) pressurant supply consists of a carbon-filament-wound tank with a maximum operating pressure of 4500 psia. Pressurant flow to the propellant tanks is controlled by a series-redundant hard-seat regulator. Mixing of nitrogen tetroxide (NTO) oxidizer and monomethylhydrazine (MMH) fuel vapors in the Pressurization System is limited by four parallel-redundant check valve assemblies.

Prior to the loss of signal, the pressurant tank was isolated from the regulator by normally closed pyro valves PV-7 and PV-8 to make the Propulsion System more robust to regulator seat leakage. In addition, the MMH tank was positively isolated from the NTO tank and Pressurization System by normally closed pyro valves PV-5 and PV-6. This eliminated the risk of forming bipropellant reaction products during cruise which have been observed to lead to regulator leakage and check valve sticking on other spacecraft.

2. *Method of Investigation*

The primary method of investigating potential propulsion failure modes was to compare the Propulsion Subsystem design heritage to Mars Observer mission requirements and to compare the Mars Observer design with spacecraft that have successfully met similar mission requirements. A group of technical specialists studied these issues and reached the following conclusions regarding the bipropellant element.

- a. *How do the Mars Observer mission propulsion requirements differ from those of the spacecraft upon which its heritage is based?*

The Mars Observer Bipropellant System heritage relied heavily on the design and qualification of the Integral Apogee Boost Stage (IABS), which was developed concurrently with Mars Observer by Astro. Another, essentially concurrent, Bipropellant System development at Astro was the Dual Mode system for the Series

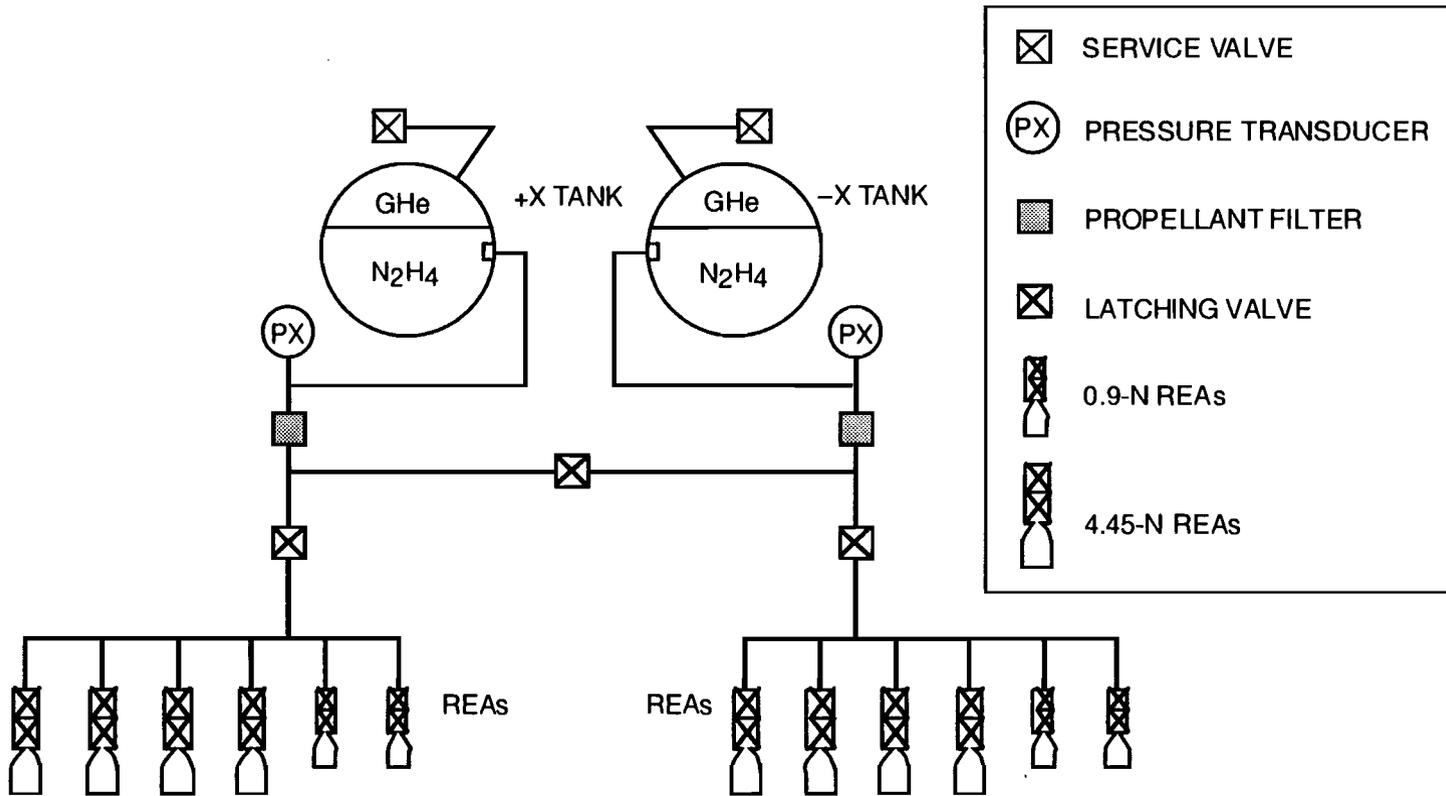
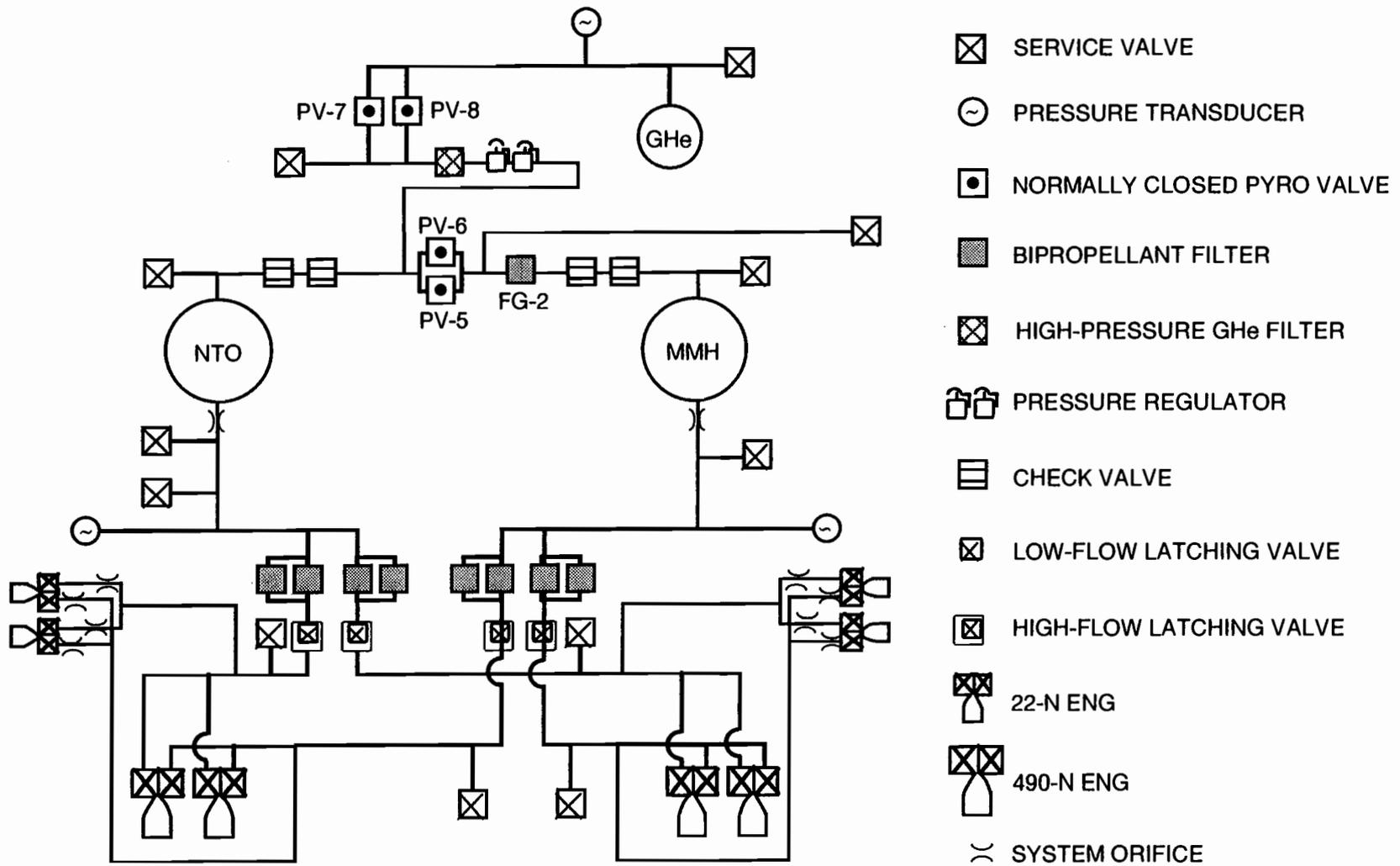


Figure 5-12. Monopropellant Subsystem.



- ☒ SERVICE VALVE
- ⊖ PRESSURE TRANSDUCER
- NORMALLY CLOSED PYRO VALVE
- ▒ BIPROPELLANT FILTER
- ☒ HIGH-PRESSURE GHe FILTER
- ⊞ PRESSURE REGULATOR
- ▢ CHECK VALVE
- ☒ LOW-FLOW LATCHING VALVE
- ☒ HIGH-FLOW LATCHING VALVE
- ⊞ 22-N ENG
- ⊞ 490-N ENG
-) SYSTEM ORIFICE

Figure 5-13. Bipropellant elements.

5000 spacecraft. These developments were the first experiences Astro had with developing a pressure-regulated Bipropellant System; with the exception of tankage, the components used had a high degree of heritage in communication satellite applications. The communication satellite application differs from the Mars Observer application in one key respect: Bipropellant systems used on communication satellites are only required to provide regulated tank pressures for one to two weeks after launch. After that, the Pressurization System is normally isolated from the pressurant/propellant tanks to preclude regulator leakage and/or reaction of propellant vapors. For example, new builds of the IABS system provide for isolation of the pressurant tanks by a latching valve. This design feature was absent from the Mars Observer Bipropellant System design. Only one communication satellite has been identified that was required to operate for a long period in a pressure-regulated mode: INTELSAT 603. This spacecraft was inadvertently put into the wrong orbit and was pressure regulated for 797 days until it was rescued by the Space Shuttle. INTELSAT 603 experienced leakage through both seats of a series-redundant hard-seat regulator beginning shortly after launch, and suffered a stuck-closed check valve during its first apogee maneuver.⁷

b. *How does the Mars Observer Propulsion System design differ from designs that have met similar requirements (e.g., Viking and Galileo)?*

The Viking Pressurization System design differed from the Mars Observer design in that the Viking propulsion design maintained the Pressurization System temperatures at or above propellant tank temperatures, making condensation of propellants in the Pressurization System highly unlikely. The Mars Observer Pressurization System was allowed to be much colder than the propellant tanks, allowing the possibility of condensation in the Pressurization System. The Viking design provided for three activations and two isolations of the regulator from the pressurant tank to mitigate the risk of regulator leakage, while Mars Observer had no isolation capability. The Viking design did incorporate a hard-seat regulator design similar to that used on Mars Observer, and at least one orbiter experienced excessive regulator leakage believed to be due to the deposition of reaction products of NTO and MMH vapors on the regulator seat.

The Galileo Propulsion System incorporated a soft-seat regulator design and very low-leakage check valves to minimize the potential for failures such as those seen on Viking. In addition, Galileo incorporated a parallel-redundant regulator, which is positively isolated from both the pressurant supply and propellant vapors until it is activated, and fault protection to autonomously isolate the primary regulator if excessive leakage is detected. The Galileo Propulsion System has operated in pressure-regulated mode since October 1989 with no evidence of leakage or other pressurization anomalies. None of these design features were incorporated into the Mars Observer spacecraft.

⁷ R. P. Prickett and L. S. Virdee, *Maximizing INTELSAT 603 Orbital Maneuver Life—Unique Factors*, AIAA Paper 93-2519, June 1993.

A secondary means of investigation was fact-finding trips to Astro and the vendors who manufactured the check valves and regulator. Telephone conversations with the pyro valve manufacturer yielded information on pyro valve failure history. Significant information exchanges also took place with the Lyndon B. Johnson Space Center, White Sands Test Facility, ESA/ESTEC, and the Mechanical Systems Panel of the NASA Mars Observer Review Board.

In concert with the NASA Board, extensive experimental efforts were initiated to quantify key issues that had to be evaluated to determine the credibility of the hypothesized failure mechanisms. These efforts are described in more detail in Appendices K and P.

3. Potential Failure Modes

As a result of the design comparisons and brainstorming activities described, the following potential Propulsion System failure modes were considered to be credible enough to warrant further investigation:

- (1) Line, component, or MMH tank failure due to NTO condensed in the Pressurization System
- (2) Bipropellant tank failure as a result of failure of both seats of the regulator to regulate tank pressure due to a common root cause
- (3) Rupture of the MMH tank or pressurant lines caused by structural failure of one of the pyro valves

These failure modes are described in more detail in Chapter VII, along with potential structural failures of propulsion hardware. Failure mechanisms that would require two independent failures following loss of communication with the spacecraft were not considered. Specifically, failure mechanisms of hardware that could not have been active during the pressurization sequence without an independent fault (e.g., bipropellant thrusters and the Monopropellant System) were not considered, although it was found that the ability of Mars Observer fault protection software to deal with some of these failure modes (stuck-on thrusters and stuck-on or -off main engines) was questionable.

4. Influences of Propulsion Subsystem on System Response to Other Faults

The only known propulsion influence on system fault responses is the catalyst bed warm-up time imposed before emergency reaction wheel unloadings.

5. Fracture Mechanics Design of Bipropellant Tanks

Safe lives of the bipropellant tanks were analytically determined on the basis of crack propagation analyses performed by Foster Engineering using the NASA/FLAGRO computer code. The initial crack sizes used in the analyses were established by cryogenic proof testing, radiography, and dye-penetrant inspections.

The analysis procedures and results were thoroughly reviewed, and it was concluded that the tanks had adequate safe-life margins for the Mars Observer mission. A summary of the review findings can be found in Appendix L.

Several weeks prior to the Titan III launch of Mars Observer, the bipropellant tanks were pressurized to a level of 285 to 315 psi (Figure 5-14). The tank pressures gradually decreased to a launch level of 250 to 260 psi, and then increased to 265 to 285 psi right after launch (see the in-flight telemetry data in Figure 5-15). During the 11 months of interplanetary transit, the pressures of the bipropellant tanks decreased to a level of 160 to 170 psi due to lower tank temperatures and greater ullage from three TCMs. The target pressure of the tanks for MOI pressurization was 260 psi, as controlled by the regulators. The fact that neither a rupture nor leak was detected during and after the launch events leads to the conclusion that structural integrity—including fracture mechanics design—of the bipropellant tanks was adequate for the Mars Observer mission. It is extremely unlikely that an error related to the design, analysis, fabrication, or quality control of the bipropellant tanks has caused the loss-of-signal anomaly. However, this does not preclude the possibility that one of the tanks was weakened, either by impacts of meteoroids or fragments of another failed Mars Observer component, and ruptured catastrophically during the MOI pressurization.

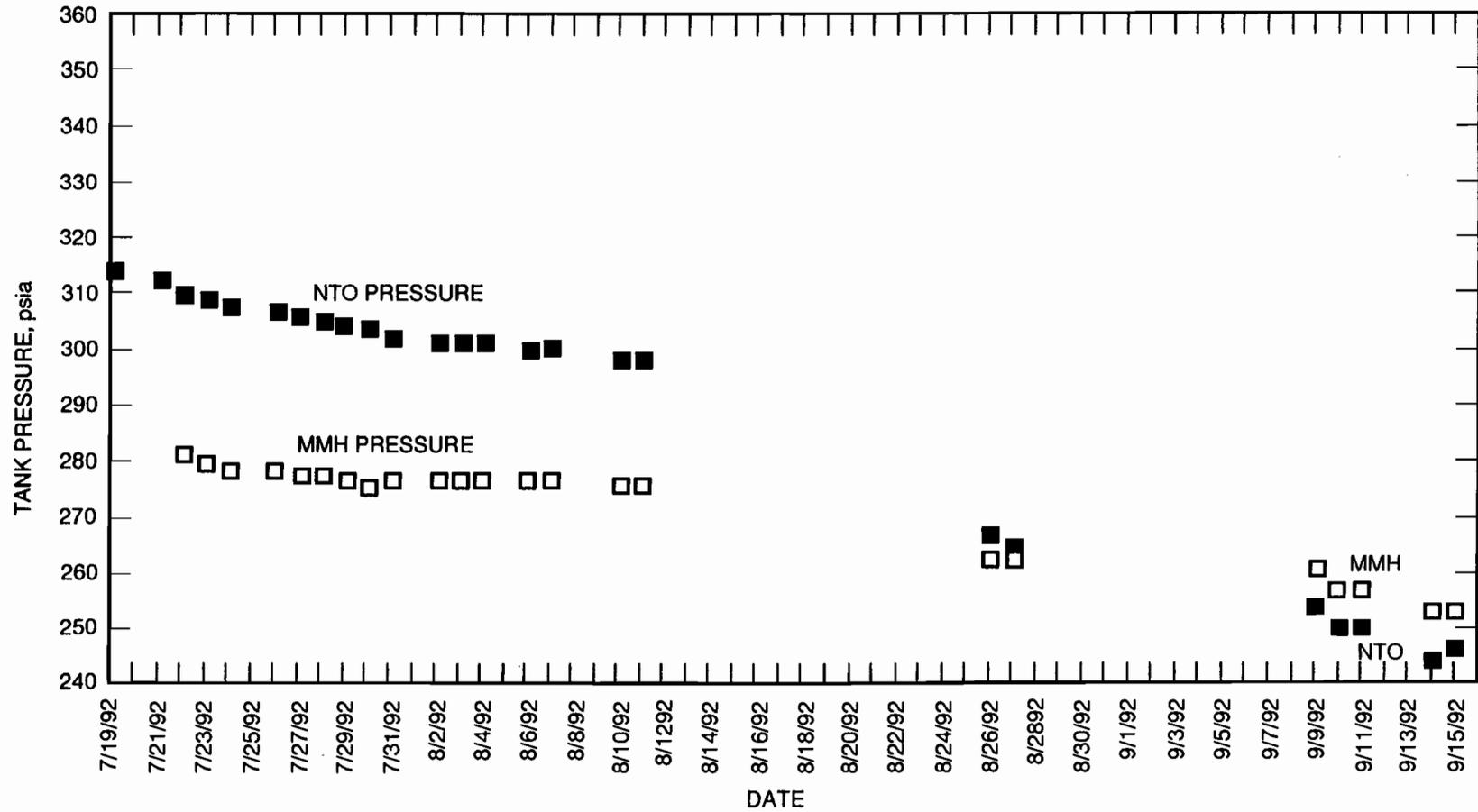


Figure 5-14. Bipropellant tank pressures during launch preparation.

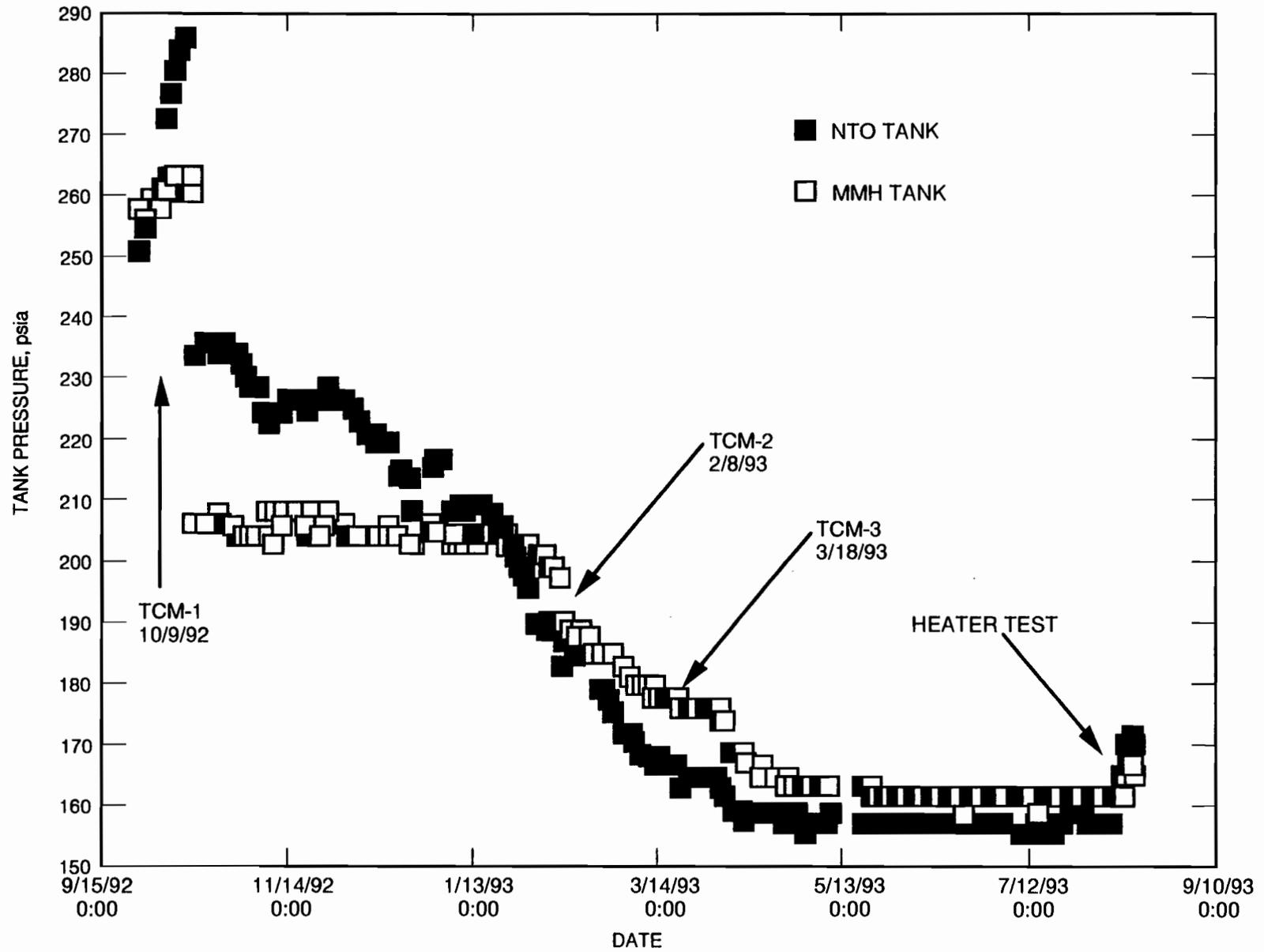


Figure 5-15. Bipropellant tank in-flight pressure telemetry data.

I. Structure and Mechanisms

The Mars Observer structural configuration is shown in an exploded view of the spacecraft (Figure 5-16). This structural design is conceptually inherited from the RCA/Astro Satcom-series satellites. The primary structure consists of a boxlike bus structure, with a central cylindrical shell running along the thrust axis of the spacecraft. The central cylinder utilizes a magnesium sheet-metal skin stiffened with rings. At the zenith panel, the central cylinder becomes conical and terminates in a separation ring that is the interface with the Transfer Orbit Stage (TOS) adapter. The central cylinder is joined to the bus structure by six radially placed aluminum honeycomb bulkheads. Two of these bulkheads are on each of the space and Sun sides to provide a trough area for stowage of the Solar Array (SA) and HGA booms. The other two bulkheads are on the +X and the -X sides, respectively.

The bus structure is comprised of all-aluminum honeycomb sandwich panels. The six side panels (the panels on the +Y and -Y sides are each divided into two half panels) and are connected by rivets and bolts to each other and to the bulkheads. Top and bottom panels (the nadir and the zenith panels) close off the box and provide lateral support to the side panels. The bus structure dimensions are 2.2 m by 1.6 m by 1.4 m high. The MMH and NTO tanks are flange-mounted inside the central cylinder, with a portion of each tank protruding beyond the end of the cylinder. Most of the science instruments, such as the Pressure Modulator Infrared Radiometer (PMIRR), the Mars Observer Laser Altimeter (MOLA), the Mars Observer Camera (MOC), the Thermal Emission Spectrometer (TES), and the Mars Balloon Relay (MBR), are attached to the +Z, or nadir, panel. The Gamma Ray Spectrometer (GRS) is located on the +X panel. The Magnetometer (MAG), Celestial Sensor Assembly (CSA), and Electron Reflectometer (ER) are located on the -X panel. The electronic boxes are attached to the inside of the Y panels. The SA assembly consists of six hinged honeycomb panels and, in the launch configuration, is stowed on the +Y-axis of the bus. The HGA reflector and its two-axis gimbals are attached to the -Y side of the bus during launch. The spacecraft structure and the TOS adapter are protoflight hardware for a Titan III/TOS launch. A pyrotechnically actuated V-band connects the spacecraft to the TOS adapter, which is permanently mounted to the TOS upper stage through a bolted interface. The TOS adapter remains with the TOS upper stage following spacecraft separation.

Figure 5-17 shows the spacecraft in its cruise configuration. All appendages of the spacecraft—the HGA, GRS, MAG, and SA—are partially deployed.

The HGA Subsystem consists of a 1.5-m parabolic reflector dish, a gimbal actuator, and a two-link boom interconnected by a mid-boom hinge assembly. The two-axis gimbal system supports and positions the HGA. The wrist-hinge assembly connects the end of the outboard boom and the base of the gimbal drive system. The inboard boom is attached to the spacecraft bus through the inboard hinge and support brackets. The HGA mechanisms are capable of moving the reflector, gimbals, and booms from the stowed to the cruise and then to the final on-orbit mapping configuration. In the cruise configuration, the HGA is partially deployed, is supported at two points, and extends beyond the nadir panel.

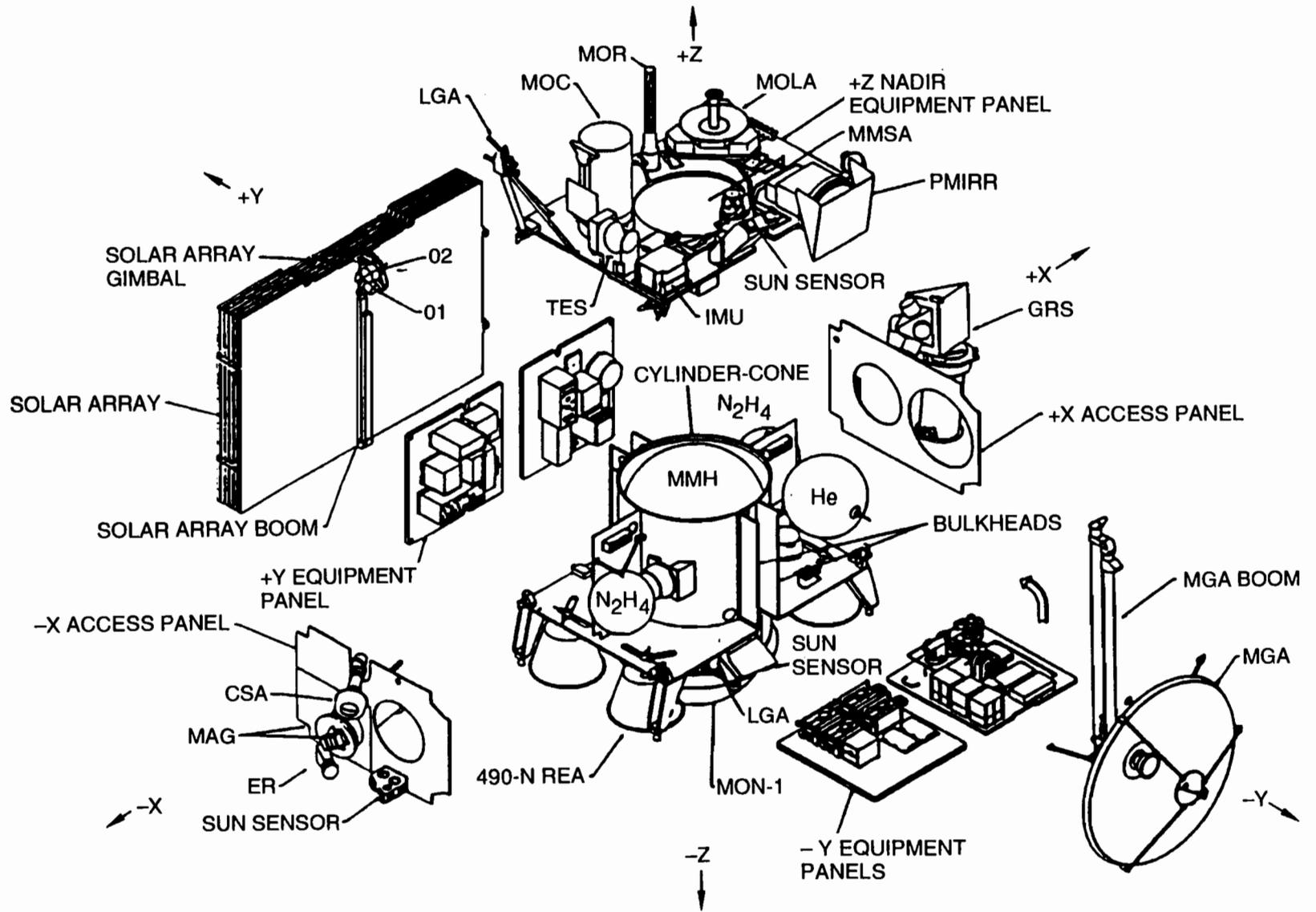


Figure 5-16. Mars Observer structural configuration.

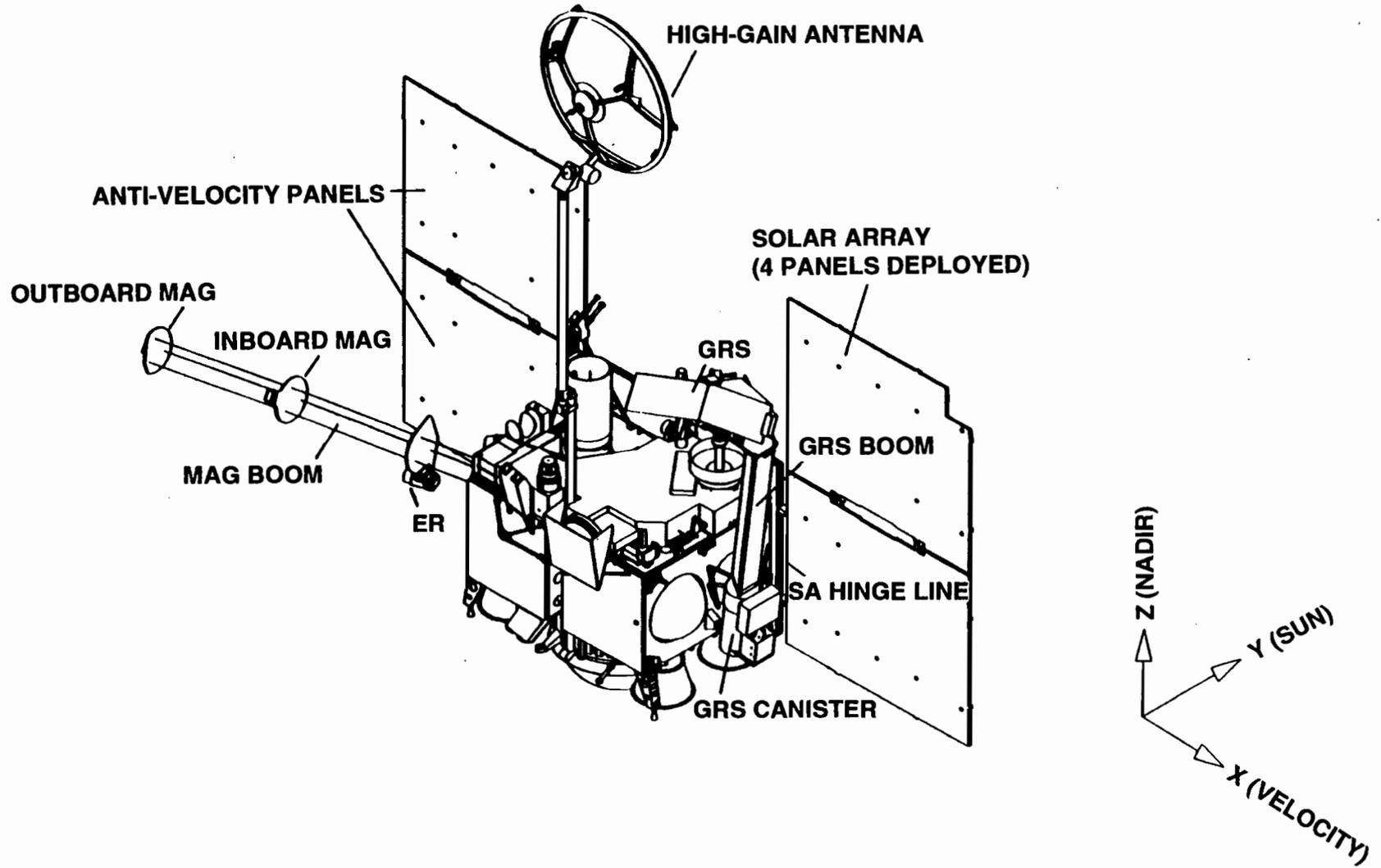


Figure 5-17. Mars Observer spacecraft in cruise configuration.

The GRS canister and boom assembly deploys the GRS sensor, utilizing a deployable truss boom controlled by a canister-deployment mechanism. The GRS instrument-mounting bracket is attached to an endplate at the boom tip. The central electronics assembly (CEA) is permanently mounted to the canister. The canister is attached to the +X panel, through a deployment hinge on the canister wall near its base and two latch brackets on the canister bottom. In the cruise configuration, the nominal boom extension is 1.587 m, measured from the top of the canister to the boom endplate. The boom will extend to its full length of 6 m in the mapping deployment.

The MAG canister and boom assembly consist of the canister housing, the drive mechanism, and a deployable boom that extends two magnetometer sensors and an ER. In the cruise configuration, the deployed boom length is 4.3 m, measured from the canister rim to the boom endplate. The outboard MAG is mounted on the end of the boom, and the identical inboard MAG is mounted 1.5 m from the boom's end. The ER is mounted 1.5 m from the inboard MAG platform towards the spacecraft. The boom is deployed using a canister-deployment mechanism. The canister fits into a cutout in the anti-velocity (-X) panel. The base of the canister is supported by four struts from the central cylinder of the spacecraft bus.

The SA, in the cruise configuration, has its four side panels deployed. The remaining two center panels are still attached to the +Y side panel with four shear ties. There are seven hinge-damper assemblies and four hinge assemblies. The inboard boom hinge-damper assembly interfaces with the bus structure and the inboard boom. The outboard boom hinge-damper assembly interconnects the booms. The interpanel hinge-damper and hinge assemblies interconnect the solar panels. There are a hinge-damper assembly and a hinge assembly on each hinge line. The SA panel system is supported and oriented by an SA gimbal drive at the tip of the SA boom. The SA boom is a two-link boom interconnected by an outboard boom hinge and attached to the bus via an inboard boom hinge. Both the gimbal and the booms are tied down to the bus structure and are not deployed in the cruise configuration.

The design loads for the Mars Observer spacecraft structure were governed by launch events and obtained from coupled loads analyses. Both the preliminary design and detailed Mars Observer structural design loads were generated by JPL using conservative upper-bound load prediction methods. The analytical model used to generate the loads was verified by a modal survey test of the spacecraft. The integrity of the primary structure was verified by test and analysis. All Mars Observer structural elements exhibited positive margins based on loads obtained from the verification loads analysis cycle. A postflight reconstruction analysis showed that due to an out-of-family Stage-1 fuel depletion burnout, the loads during that event exceeded the envelope of the predicted loads. A preliminary review of the increased stresses in the affected structural elements by Astro concluded that the launch loads did not exceed the structural capability.

After the loss-of-signal anomaly, a review of the Mars Observer structural design was conducted to identify hypotheses related to structural failures. It was concluded

from this review that failure of Mars Observer structures, other than the pressurized components of the Propulsion System, can be precluded as a likely cause of the Mars Observer anomaly. The reasons for this assessment include:

- (1) There was no indication of a structural failure during the Titan III launch events, which were unquestionably the most severe flight environment for the flight structures.
- (2) All appendages deployed and functioned as expected without any significant in-flight anomalies that can be potentially related to the loss-of-signal anomaly.
- (3) Mars Observer structures were designed to a set of very conservative loads established at JPL (even though postflight reconstruction of launch events indicated the loads imposed on some of the structures could be much higher than the verification loads analysis loads, all structures have sufficient margins to survive the flight environment).
- (4) The Mars Observer loss-of signal anomaly was inconsistent with any credible real-time or latent structural failure.

The Mars Observer Propulsion System includes five pressure vessels storing an extremely large amount of energy and contains hazardous propellant. A catastrophic failure of a pressurized component, including burst, rupture, and leakage of tanks and lines, could possibly lead to the observed Mars Observer anomaly. Based on this, Hypotheses C3A, C3B, and C3C have been developed and analyzed (see Chapter VII.C-E).

J. Electronic, Electrical, and Electromechanical Parts

Electronic, electrical, and electromechanical (EEE) parts per se are not a subsystem. EEE parts, however, are the fundamental building blocks used to implement most major functions required in a spacecraft. One of the basic requirements for achieving long spacecraft life is to use highly reliable EEE parts.

In support of the Special Review Board activities, the following EEE parts-related issues have been investigated:

- (1) Was the parts control plan well conceived?
- (2) Were there approved electronic parts waivers wherein the cause for the waiver might be related to the Mars Observer anomaly?
- (3) Were there parts that might exhibit a large number of single-event upsets (SEUs) or suffer catastrophic damage from a single heavy ion strike (single-event burnout or single-event gate rupture)?
- (4) What is the likelihood of failure of a JANTXV2N3421 Unitrode transistor in the RXO?
- (5) Specific questions regarding EEE parts used in particular subsystem applications.

1. *The Parts, Materials, and Processes Control Plan for Mars Observer*

The original edition of the Parts, Materials, and Processes Control Plan (PMPCP) for Mars Observer was prepared in early 1987 by RCA. The most recent edition of the plan⁸ was reviewed to determine, in general, how it would compare with the current JPL requirements for Class-A flight equipment.⁹

The PMPCP described a Grade 1 parts program suitable for Mars Observer and compared favorably with the requirements in Footnote 10. Although the PMPCP adequately covers the subject of heritage parts, it is possible that both JPL and Astro should have been more thorough in re-establishing the qualification basis of heritage parts.

A fundamental assumption from the beginning of Mars Observer was that there would be maximum use of heritage hardware for cost-saving reasons, and it was required that the electronic parts in that hardware be accepted based on heritage. Blanket waivers were used to accept all of the parts within each of four subsystems. The MOT was accepted from Magellan, while the MHSA, IMU, and CSA were accepted from DMSP. With the frame of reference being that heritage hardware would be

⁸ *Mars Observer Parts, Materials, and Processes Control Plan*, RCA document 2617508, Rev. E, RCA, September 16, 1991.

⁹ *Electronic Parts Program Requirements for Flight Equipment*, JPL Document 5357, Jet Propulsion Laboratory, Pasadena, California, November 21, 1990.

accepted, it is possible that the review of the qualification basis of heritage parts was less thorough than would have been the case for new designs.

2. *Waivers Applicable to EEE Parts*

The waivers applicable to EEE parts can be separated into three categories:

- (1) There were 196 waivers approved by JPL Electronic Parts Reliability and the Mars Observer Project Office. These waivers were considered to be low-risk with respect to being related to the Mars Observer anomaly and were not evaluated further.
- (2) There were 19 waivers rejected by both JPL Electronic Parts Reliability and the Mars Observer Project Office. These waivers by definition cannot be related to the Mars Observer anomaly because use was not allowed.
- (3) There were 34 waivers rejected by JPL Electronic Parts Reliability, but approved by the Mars Observer Project Office. These waivers were individually reviewed for level of risk and whether the parts might be related to the Mars Observer anomaly.

Among the 34 waivers rejected by JPL Electronic Parts Reliability, but accepted by the Mars Observer Project Office, five instances were found wherein additional investigation relative to the Mars Observer anomaly was justified. The investigation was hampered considerably by lack of an as-built parts list by subsystem for the spacecraft. The five instances are:

- (1) Teledyne, Type 412, DPDT, Nonlatching Relay—Parts of this type built prior to 1984 can fail to switch because the armature can become cold-welded to its stop while at rest. The vintage and all of the locations of the parts in the hardware are generally unknown. Investigation of the SCU has not found any relays of this type in locations that could be related to the anomaly. Investigation of the IMU found that the relays used were built subsequent to 1984 and would, therefore, be immune to cold welding.
- (2) Unitrode 2N4150 Transistor—On a Parts Advisory published by the NASA Parts Program Office, this transistor was identified as possibly having inferior wire bonds because it was built on the same manufacturing line as the JAN TXV2N3421 used in the RXO. Investigation determined that the 2N4150 was used only in the optical encoders associated with the HGA and SA gimbals. Neither of these applications could be related to the anomaly.
- (3) Microsemi Corp. JAN TXV1N821-1 Zener Diodes—These diodes failed destructive physical analysis (DPA) because of loose conductive particles. The disposition for the lot of parts was to use as is. Investigation found these diodes were used in a temperature sensor assembly in the Power Subsystem and determined that their failure could not be related to the anomaly.
- (4) LSI Logic LRH9600-MEU—This device is a custom error detection and correction (EDAC) chip used in the SCP and EDF. The waiver was written

because the device had not been optimally laid out and it had internal wires that crossed. The problem had been patched by carefully dressing the wires. It is very unlikely that the anomaly would have resulted from the sudden sagging of one of these wires to create a short.

- (5) Kemet, CKS06, 1- μ F, 50-Vdc Capacitor—The largest capacitance value qualified in this package size for military applications is 0.47 μ F. To obtain the 1.0- μ F value in this package size requires the use of a very thin dielectric layer between capacitor plates and greatly increases the probability of developing a short. These devices are used as noise filters on the 28-Vdc power lines in the IMU. Investigation found that a shorted capacitor in the IMU would result in the blowing of a fuse and that fault protection would switch to a redundant power supply. If this were to have happened, it would not have resulted in the Mars Observer anomaly.

3. Parts List Review for Single-Event Effects (SEEs)

There is no as-built parts list for the spacecraft and the Board has not succeeded in having one produced. A list of parts used in the Astro-built hardware was provided to the Board. Upon reviewing that list, the only device that had a high probability for SEU was the HS65C262RH random access memory (RAM) used in the SCP and EDF. These RAMs have been exhibiting SEUs in flight, and the errors have been corrected by EDAC. The only devices considered to possibly be subject to catastrophic effects (single-event burnout [SEB] or single-event gate rupture [SEGR]) were the power field effect transistors (FETs) used in the Power Subsystem. Analysis by the engineers cognizant of the Power Subsystem has shown that the maximum voltage that would be experienced by the power FETs is 38 Vdc, well below the 45-Vdc minimum voltage at which either SEB or SEGR might occur for these transistors.

Additional specific information related to devices used in the CIU, CIX, SCP, and CDU is contained in Appendix J. It is considered to be extremely unlikely that SEE is related to the Mars Observer anomaly.

4. Failure Likelihood of the JANTXV2N3421 in the RXO

There was a failure of a Unitrode JANTXV2N3421 transistor in a NOAA-I RXO on the launchpad at Vandenberg. The RXO in Mars Observer is similar to the RXO on NOAA-I and uses the same transistor from the same lot date code (8350). There was a great deal of speculation in the media about whether the Mars Observer anomaly resulted from failure of the RXO, which in turn was caused by failure of the JANTXV2N3421. Consequently, the failure investigations conducted by Astro, Goddard Space Flight Center, Hughes, and Aerospace, with respect to the JANTXV2N3421, have been reviewed extensively. The summary of this review is contained in Appendix S. The conclusion is that failure of a JANTXV2N3421 in the RXO, though unlikely, is not incredible. It is considered, however, to be extremely unlikely that a single JANTXV2N3421 failure would have resulted in the Mars Observer anomaly (see the discussion of Candidate Hypothesis S1 in Chapter VII.R).

5. *Other Parts Issues*

The Power Subsystem uses some large (1450- μ F) wet-foil capacitors, which might short to cause a large power drain. Investigation showed that capacitors of this type almost always fail by losing electrolyte, which in turn causes loss of capacitance and an increase in the dissipation factor. Capacitors of this type are very unlikely to short. However, if one of these capacitors, which are connected directly across the primary power supply, were to develop a low impedance short, the heat generated would cause the internal electrolyte to expand as a gas, thereby causing high internal pressure that could potentially cause a breach in the case with venting of the electrolyte and a likely increase in impedance. If the low impedance state exists long enough, the internal wire will probably fuse, causing an increase in impedance. The final state following a low impedance short is expected to be a path in which there will be at least a few $k\Omega$ of impedance. A test to experimentally demonstrate the outcome of a shorted capacitor has been proposed and will be conducted if suitable test samples can be acquired. A search for test samples is being conducted by William Baker of NRL.

CHAPTER VI

METHODOLOGY FOR DEVELOPING, CHARACTERIZING, AND ANALYZING HYPOTHESES

A. Hypothesis Generation Methods

1. Board Processes

The Mars Observer Special Review Board used various techniques to generate candidate hypotheses for the failure, being careful not to miss something by dismissing a possibility prematurely. In particular, at the outset of the investigation, the Board lacked confidence in the observables (see Chapter IV.C) and continued to study those hypotheses in which it might have been possible to detect a downlink. In fact, the analysis required to make that determination was frequently quite complex.

During and after the many briefings, the Board asked countless questions and analyzed the answers. All Board members freely proposed hypotheses for consideration throughout the investigation. The Board also studied recent failures of similar hardware, such as the NOAA-I RXO and power short events.

The Board systematically examined the sequence being executed during the pressurization block to determine which commands or components might have been in use for the first time or in a different way. The physical (not electronic) disturbances, or state changes, occurring during the pressurization sequence are given in Table 6-1. More information on the most violent of these disturbances, pyro shock, appears in Appendix G, and the possible electromagnetic interference effects from firing the pyros are described in Appendix H.

Table 6-1. Physical changes on the spacecraft during pressurization sequence.

Source	Change
Mechanical vibration/ shock sources	<ul style="list-style-type: none">• Pyro-shock events (see Appendix G)• RWA vibration or "squeal"• Check valve chatter or buzz
Electrical (not electronic) state changes	<ul style="list-style-type: none">• Loads turned off (Exciter 2, RPA-2 beam, and both RPA cathode heaters [filaments]; X, Y, and Z reaction wheel control)• Electrical pulse (EMI) from pyro firing (see Appendix H)• Loads turned on (skew RWA; X, Y, and Z RWAs upon resumption of control after exiting Deploy Mode; RPA-2 cathode heater [filament] RPA-2 beam, Exciter 2)• Solar Arrays drifting off-Sun (only about 10° change in nominal sequence)
Thermal changes	<ul style="list-style-type: none">• Thermal heating or cooling due to the electrical load changes above• Solar aspect angle changes during Deploy Mode (about 10° change)

For cases which might involve catastrophic physical damage to the spacecraft, the Board considered the sources of energy stored on board (see Table 6-2). Because the main sources of energy are in the Propulsion System and the battery (the Power System), the Board looked carefully for potential failures there.

A generic place-holder hypothesis for design and implementation errors was developed. All projects suffer such errors, and every effort is made to find and fix them prior to launch. Some software errors were discovered after launch, and several had been corrected prior to the pressurization sequence. The Board also studied the complex spacecraft interactions involving the hardware and software (and sometimes fault protection).

The Board reviewed known (documented and approved) Single Failure Points (SFPs), which are identified in Appendix M. This list was used as a source of clues for a cause of the failure, but since all spacecraft have traditionally approved SFPs, such as primary structure and propulsion tanks, few clues were found.

External influences that could have damaged the spacecraft were carefully studied. The spacecraft could have been struck by a meteoroid, but the probability of such an occurrence is very low (see Appendix I). Another external influence that could have affected the spacecraft is a single-event effect (SEE), such as a cosmic ray that penetrates the spacecraft and upsets or damages sensitive electronic parts (see Appendix J).

The Board considered the efficacy of computing the a priori probability of occurrence for each of the proposed hypotheses. After much discussion, the Board concluded that such an attempt is fraught with subjective judgment, inherently controversial, and in many cases not technically defensible. The Board's focus then became the degree of credibility based on causality, single- versus multiple-point failures, and failures of a similar nature on other spacecraft.

Finally, a fault tree was developed and refined, and is discussed in the next subsection.

Table 6-2. Sources of energy on board the spacecraft.

Source	Energy, joules (J)
Bipropellants (chemical)	6×10^9
Monopropellant (chemical)	2×10^8
Batteries (chemical)	7×10^6
GHe pressurant tank	3×10^6
MMH and NTO tanks (ullage volume)	2×10^5
Reaction wheels (four at 9000 rpm)	8×10^4
Pyro valve (booster charge)	6×10^2
Deployment springs (approximate totals: HGA, 50 J; Solar Array, 80 J; GRS, 30 J; MAG, 6 J)	1.6×10^2
NSI (one)	1.5×10^2

2. *Fault Trees*

Fault trees are very useful for logically connecting events and causes. The top level of the fault tree is the observed failure. In this case, the observed failure is composed of the union of the observables described earlier in Chapter IV.C. The fault tree adopted by the Board is shown in Figure 6-1.

For the purposes of this fault tree, multiple simultaneous failures are not considered credible unless a common failure mode can be identified. For example, the “regulator fails open” scenario requires both halves of the regulator to fail due to common contamination.

The fault tree was structured so that at the first layer below the top layer, the loss of certain functions by subsystem is shown. In addition, catastrophic system failure (physical damage) is called out at this level because the damage caused by the scenarios in this branch could affect any one or all of the subsystem functions.

For each subsystem, the subsystem specialists expanded the fault tree to include all failures considered worthy of investigation.

B. Categorization of Hypotheses

1. *Degree-of-Causality Method*

One technique for categorizing a hypothesis is to consider the degree to which the hypothesis can be causally tied to the events being executed on the spacecraft. The Board adopted three categories that are identified by the letters C, S, and N:

- (1) Deterministically causal (C)
- (2) Postulated causality through deterioration—the “straw that broke the camel’s back” (S)
- (3) Not causal (N)

This structure is primarily the result of the desire to seek causal relationships for all events. The focus in this type of investigation must initially be the identification of a deterministically and unambiguously causal event that leads directly to the observed anomaly, but it was evident early that the Board would be frustrated in its search for causality. The reasons for this are twofold: first, there is no obvious “smoking gun,” and second, the paucity of available evidence makes unqualified elimination of most of the abundant alternatives impossible.

The S-category hypotheses result from deterioration, a wear-out mode whereby a very small effect or disturbance can precipitate a failure. This “straw on the camel’s back” model provides a link to the sequence activity through effects that are too small to be directly causal. This situation is plausible and real, but some of the straws can be quite small. A list of “straws” (small changes) happening on the spacecraft is given in Table 6-1.

2. Contribution-to-Anomaly Method

This method was developed and used to categorize the many analyzed hypotheses to determine the leading potential causes for the failure (see Table 6-3). Credibility refers to the physics of the situation and to the degree to which the hypothesis meets the observables. Likelihood has to do with the a priori probability that the event would happen.

Table 6-3. Hypothesis categories.

Category A: Credible	The hypotheses in this category require vulnerability only at a single point, and have either been experienced on other spacecraft or have been shown to be plausible by analysis, test, or VTL simulation. These hypotheses cannot be rigorously proven to be the cause of the failure, but they are the most credible potential causes of the actual Mars Observer loss-of-signal anomaly.
Category B: Credible, but very unlikely	Analysis shows that these hypotheses are credible potential causes of the actual Mars Observer anomaly, but are very unlikely. In some Category B hypotheses, an error or oversight in the modeling or analysis is required to match the observables, but the complexities and uncertainties associated with the modeling and analysis make this a possibility.
Category C: Not credible	Analysis shows that these hypotheses are not credible, and the complexities and uncertainties associated with the modeling are not a concern. These hypotheses are not credible potential causes of the actual Mars Observer anomaly.

C. Candidate Hypotheses for Potential Causes of the Observed Anomaly

In the course of the Board's work, many possible scenarios were advanced to explain the observed anomaly; some of these scenarios could easily be rejected as incorrect, but those that could not be so readily dismissed were identified as hypotheses for potential causes of the anomaly. As a result, the terms "hypothesis" and "potential cause" are used interchangeably for convenience. All the identified hypotheses (even those that could not have caused the anomaly) have been retained. This approach seemed prudent because the demonstration of impossibility is complex and may rely on detailed, derived information for some hypotheses.

The Board considered the efficacy of computing the a priori probability of occurrence for each of the proposed hypotheses. After much discussion, the Board concluded that such an attempt is fraught with subjective judgment, is inherently controversial, and in many cases not technically defensible. The Board's focus then became the degree of credibility based on causality, single- versus multiple-point failures, and failures of a similar nature on other spacecraft.

The hypotheses listed in Table 6-4 represent the identified potential causes. The numbering and sequencing of the list, however, is arbitrary, and the list is not organized in terms of likelihood of occurrence. These hypotheses are also identified on the fault tree (Figure 6-1).

The hypotheses have been categorized into the three groups according to degree of causality, as defined above (C, S, and N). Three hypotheses on the list were deleted because they were generic placeholders; any time that a real example of a generic type of failure emerged, a unique hypothesis was created to cover it. These hypotheses are discussed in detail in Chapter VII (with supporting appendices and references). A summary of the analyses and an overall assessment are given in Chapter VIII. Table 6-4, which also shows the category assigned to each hypothesis, serves as a guide to Chapter VII for the reader.

Table 6-4. Candidate hypotheses.

Hypothesis	Category	Description
C1A	A	NTO liquid upstream of check valves reacts with MMH in lines
C1B	B	NTO liquid upstream of check valve reacts with MMH in MMH tank
C1C	B	NTO liquid upstream of check valves is "liquid bullet"
C2	A	Pressure in bipropellant tanks is unregulated
C3A	B	Burst of tank in normal pressurization due to flaw existing at launch
C3B	B	Burst of tank in normal pressurization due to meteoroid-created flaw
C3C	C	Burst of line in normal pressurization due to flaw existing at launch
C4	A	NSI expulsion and/or pyro-valve failure
C5A	A	SCP in control
C5B	A	I/O crossed /not crossed
C5C	A	I/O bus select
C6	B	Unidentified SCP software problem
C7	C	Miswired pyros
C8	—	Deleted (generic placeholder)
C9	B	Unknown sequence error
C10	C	Skew RWA stall
C11	C	Loss of exciter frequency reference
C12	C	Hardware/software conflict preventing RPA turn-on
C13	B	RPA relay short SPF
C14	C	RPA overcurrent detector prevents turn-on
C15	B	Erratic activity on critical CIU-hardware interface
C16	A	Hardware failure preventing RPA turn-on
S1	B	System response to primary-side timing loss (RXO)
S2	A	Total spacecraft power loss
S3	B	Erratic RXO output
S4	B	RPA cathode support failure
S5	B	Gyro-spin-motor short
S6	C	Sun sensor head number 4 failure
S7	C	RWA overspeed
N1	B	Meteoroid impact
N2	—	Deleted (moved to S5)
N3	C	DSN failure to detect existing downlink
N4	B	Multiple electronic parts failures
N5	—	Deleted (generic placeholder)
N6	B	SEE-created problem
N7	B	10-V interface power failure

CHAPTER VII

CANDIDATE HYPOTHESES TO EXPLAIN THE LOSS-OF-SIGNAL ANOMALY

A. Liquid Oxidizer Upstream of Check Valves Causes Damage to the Pressurization System (C1)

As discussed in Appendix K, there is a likelihood that a small quantity of nitrogen tetroxide (NTO) was transported by diffusion and permeation mechanisms to the coldest portions of the Pressurization System, where it subsequently condensed. Three hypotheses related to this phenomenon are described in this section.

1. *Liquid Oxidizer Upstream of Check Valves Reacts With MMH in Pressurization System (Reaction in Lines; C1A)*

Hypothesis

A portion of the accumulated NTO could have been injected into the fuel side of the Pressurization System. This is made more likely by the detailed configuration of the Pressurization System. If this occurred, the NTO would interact with liquid monomethylhydrazine (MMH) in the Pressurization System. NTO and MMH are hypergolic propellants and their reaction is very energetic (up to 6.4 kJ/g of reactants under stoichiometric conditions). Furthermore, MMH is an energetic compound that exhibits exothermic decomposition if exposed to high temperatures and/or catalysts. Depending on the rate of reaction and the amount of reactants, the Pressurization System tubing, fittings, or components could have ruptured. This would result in venting of helium (although at a rate limited by the flow restriction orifice in the regulator) and/or MMH into the interior of the spacecraft.

Consistency With Observables

As described in Appendix K, rupture of the Pressurization System downstream of the check valves may produce high angular rates adequate to preclude detection of a signal and will lead to massive MMH leakage. It is likely that spacecraft rates would at least preclude acquisition of an HGA signal at the scheduled time. Critical physical damage to the spacecraft might occur due to chemical attack by MMH on cable insulation, potting materials, and thermal blankets before acquisition of the signal on the LGA would occur (if it could occur at all given the possibility of very high angular rates).

Conclusion

The probability of failure occurring in accordance with this hypothesis depends on many factors, which are not presently well defined:

- (1) Quantity of NTO transported through the check valves. Issues include details of the check valve design and function, permeation rates through seat materials, and temperature gradients within the Pressurization System. Analysis and test results to date are described in Appendix K and indicate that quantities on the order of one to two grams of NTO would condense.
- (2) Final location of condensed NTO at the time of pressurization.
- (3) Fraction of condensed NTO swept into NTO tank after firing of PV-7 versus the amount available for interaction with MMH. Due to the geometry of the Pressurization System plumbing (Appendix K), it has been assumed that most of the NTO condensed in the Pressurization System would not have been removed by this method, although at least some of it should have vaporized and been carried to the NTO tank.
- (4) Reaction rates of NTO and MMH. This is strongly influenced by the ability of the hypergolic propellants to mix prior to ignition and is being evaluated experimentally.
- (5) Ability of MMH in the pressurization lines to sustain a decomposition flame after initiation by reaction with NTO. This phenomenon is energetically possible, but has never been observed, and many experts believe that it may be impossible due to the kinetics of MMH decomposition.
- (6) Ability of Pressurization System components to survive pressure spikes as a result of NTO-MMH interactions.
- (7) The time required for MMH liquid/vapor to inflict critical physical damage on the spacecraft. This has not been evaluated in detail, but tests of cabling exposed to propellants suggest that many hours might be required to produce serious damage.

Many combinations of possible events encompass these factors. The discussion in Appendix K describes scenarios that may be possible, and the ongoing attempts to quantify critical factors that affect the probability of failure. Based on the best available information, the pressures predicted in Appendix K may approach or exceed the burst pressure of the lines. An experimental program is underway at the U.S. Air Force Phillips Laboratory and JPL to attempt to reduce the uncertainties in the analysis of this scenario. The credibility level of this hypothesis is contingent upon the results of these ongoing tests.

Hypothesis C1A is Category A: credible.

2. *Liquid Oxidizer Upstream of Check Valves Interacts With MMH in Fuel Tank (Reaction in Tank; C1B)*

Hypothesis

Some of the accumulated NTO could have been injected into the MMH tank. If (and only if) the resultant reaction resulted in thermal decomposition of a large quantity of MMH could this result in rupture of the MMH tank.

Consistency With Observables

Rupture of the MMH tank would almost certainly cause multiple instances of critical physical damage to the spacecraft.

Conclusion

The probability of failure occurring in accordance with this hypothesis depends on a number of factors, including:

- (1) Quantity of NTO transported through the check valves. Analysis and test results to date are described in Appendix K and indicate that quantities on the order of one to two grams of NTO would condense.
- (2) Final location of condensed NTO at the time of pressurization.
- (3) Fraction of condensed NTO swept into NTO tank after firing of PV-7 versus the amount available for interaction with MMH.
- (4) Reaction rates of NTO with MMH.

However, the key factor is the ability of the MMH in the tank to sustain a decomposition flame after initiation by reaction with NTO. This phenomenon is energetically possible, but has never been observed, and many experts believe that it may be impossible due to the kinetics of MMH decomposition.

Analysis shows that unless a very fast reaction or decomposition flame occurs in the MMH tank, it would not be possible to rupture the tank under any credible conditions (including a failed open state of both check valves). Experimental activities are underway at the U.S. Air Force Phillips Laboratory to evaluate these key factors.

Until the results of these investigations are available, Hypothesis C1B is Category B: credible, but very unlikely.

3. Liquid Oxidizer Upstream of Regulator Causes Impact Damage to Pressurization System ("Liquid Bullet"; C1C)

Hypothesis

If the liquid NTO accumulated upstream of the regulator, firing of the high-pressure pyro valve (PV-7) at the start of the pressurization sequence could have accelerated the liquid to very high velocities, potentially causing failure of fittings in the Pressurization System when this "liquid bullet" impacted the elbow fitting in the plumbing. This rupture would lead to venting of the helium tank at a very high rate, and impart excessive attitude rates to the spacecraft.

Consistency With Observables

If the Pressurization System ruptured upstream of the regulator, very large angular accelerations and rates would probably be applied to the spacecraft. Based on the orientation of the hypothetical rupture, the spacecraft would probably be left rotating about the X- and Z-axes at a rate in excess of 90°/s. The initial spin-up would likely be about the X-axis. It is extremely unlikely that a downlink carrier could have been detected for rates above 16°/s.

Conclusion

The probability of failure occurring in accordance with this hypothesis depends on many factors which are difficult to define:

- (1) Quantity of NTO transported through the check valves. Analysis and test results to date (Appendix K) indicate that quantities on the order of one to two grams of NTO would condense.
- (2) Final location of condensed NTO at the time of pressurization. As described in Appendix K, it is possible that any condensed NTO was located just downstream of the high-pressure pyro valves.
- (3) Ability of high-pressure gas to accelerate a small slug of NTO without breaking it up into fine droplets.
- (4) Ability of Pressurization System lines and fittings to survive impact by an NTO slug propelled by high-pressure gas. These components are very robust, with burst pressures in excess of 35,000 psi.

Many combinations of possible events encompass these factors, but it is believed that item (3) would dominate the results.

The potential for impact damage could be larger in the unlikely event that both check valve assemblies failed open, but this is extremely unlikely. Two tests have been conducted using one and two grams of NTO in a flight-like plumbing configuration and no damage was observed. Because of the uncertainties in reproducing the flight system weld strengths, etc., and possible repeatability issues in the testing, this hypothesis cannot be totally eliminated, but it is extremely improbable.

Hypothesis C1C is Category B: credible, but very unlikely.

B. Burst of Bipropellant Tanks Due to Unregulated Pressure (Regulator Fails Open; C2)

Hypothesis

This hypothesis involves a near wide-open failure of both seats of the pressure regulator. This could be caused by the reaction of pre-existing contaminants in the regulator with NTO vapor over the one-year period between propellant loading and the MOI pressurization sequence. The products of reaction are hypothesized to either block the sensing port orifices of the regulator stages and/or fill the convolutions in the main bellows.

The regulator design is shown schematically in Figure 7-1. Blockages of the sensing port orifices would prevent the regulator stages from sensing increases in downstream pressure, thus preventing closure. Contaminants in the convolutions of the main bellows would lead to failure by mechanically jamming the regulator seats in the open position, where they had been for most of the flight.

A failure of this type might have been possible on Mars Observer in the presence of contamination levels that would not have a significant impact on a normal Earth-orbiting communication satellite. This is because the pressure-regulated operation of the communication satellite lasts only a few days to a few weeks; there would not be the opportunity for extensive interaction of contaminants with NTO vapors.

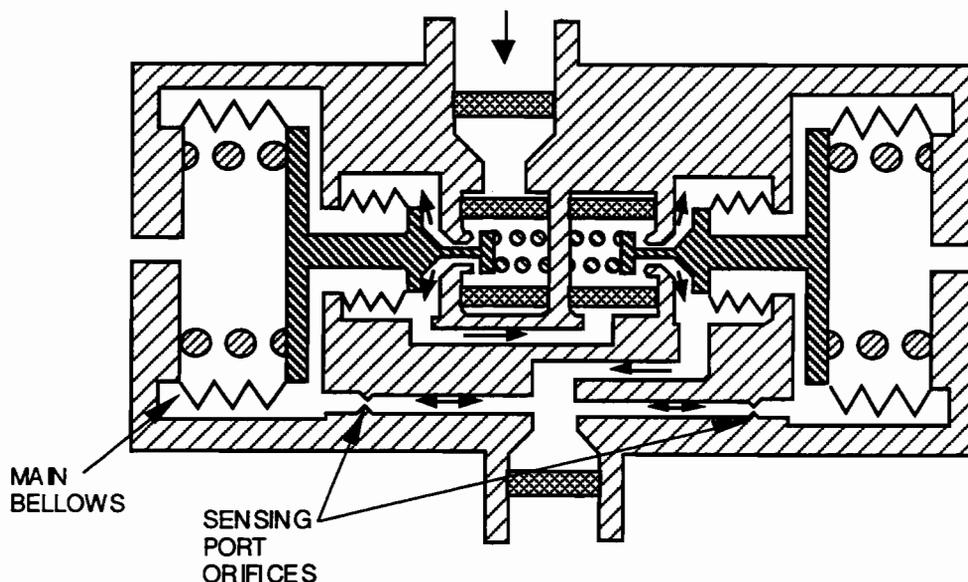


Figure 7-1. Regulator schematic.

Consistency With Observables

If the regulator failed in a nearly wide-open condition, the NTO tank would have burst approximately 30 s after the opening of PV-7. If the regulator failed in a partially open state, the propellant tank burst could have required several minutes. This would have led to critical physical damage to the spacecraft.

Conclusion

It will probably never be possible to determine whether the Mars Observer Propulsion System was sufficiently contaminated to cause such a failure, so this hypothesis cannot be ruled out.

The robustness of the basic regulator design is evidenced by the fact that the Space Shuttle program has 17 regulators of a similar design which have each seen continuous service exposed to NTO vapors for from 433 to 3803 days without experiencing such a failure. Although seven Space Shuttle regulators have been removed from NTO service due to leakage, none have exhibited wide-open failures.

However, this hypothesis is considered credible by virtue of the fact that similar failures have been observed:

- (1) A wide-open failure was seen in both stages of a regulator in the MMH side of the Space Shuttle Reaction Control System. In that case, the Pressurization System had been exposed to MMH vapors during operation and was subsequently exposed to air during servicing operations. Water vapor, carbon dioxide, and other contaminants reacted with residual MMH. When the regulator was returned to service, both seats failed in the open condition, leading to rupture of a burst disk in the Shuttle orbiter. Subsequent inspection found that "goeey, black deposits" had blocked the sensing ports of both regulator stages. While this failure occurred following MMH, rather than NTO, exposure, analogous deposits can occur when NTO reacts with appropriate contaminants.
- (2) One failure due to contaminant deposits in the main bellows was observed in a regulator removed from NTO service in a ground test operation at NASA's White Sands Test Facility. When the regulator was subjected to destructive analysis (after about a year of storage), extensive contamination of the bellows was evident and the bellows was found to be incompressible. This failure was probably due to contamination by service equipment and/or during storage.

One possible contributing factor is the use of Kalrez 1050 in the Futurecraft check valves used in the Mars Observer Pressurization System. This material is not considered to be long-term compatible with NTO and contains carbon black filler. No long-term compatibility testing has been performed, but it is possible that reactions between NTO, the carbon in this material, and traces of water or other contaminants could produce contaminant deposits. For this to occur, intermediate products, such as CO₂, would have to diffuse to the vicinity of the regulator.

The cleaning procedures used at Astro are brought into question by one event during this investigation. Four check valves were shipped to JPL for testing. Prior to shipment, Astro cleaned two of them and included cleaning results in the documentation sent with the valves. The cleaning tags showed a total absence of particulates, which is almost impossible. Subsequent testing at JPL showed that all four valves had substantial particulate contamination; they were re-cleaned before testing could proceed.

Another disturbing observation is that (as described in the Mars Observer Daily Activities Status Report for July 24, 1992) the hydrazine propellant loading cart was apparently contaminated with excess particulate and a "red powdery residue." While this would not be directly related to the potential contamination of the Pressurization System, this incident reflects at least one instance where inadequate precautions were taken in cleaning and inspecting service equipment used in servicing the Mars Observer Propulsion System.

Hypothesis C2 is Category A: credible.

C. Burst of a Bipropellant Tank With an Initial Flaw During MOI Pressurization (Flaw Bursts Tank; C3A)

Hypothesis

This hypothesis assumes that a crack-like flaw with a depth of more than 60 percent of the weld thickness exists in the weld in one of the bipropellant tanks. The flaw is not detected by the cryogenic proof test or during radiographic inspection and the follow-on dye-penetrant inspection used to screen cracks in the tank. The flaw is a part-through crack and grows to near-breakthrough size by the beginning of interplanetary cruise. The flaw does not grow at constant pressure during the 11-month cruise, and the pressure telemetry data indicate no tank leakage. When the tank is pressurized for MOI, the flaw grows from a part-through crack to a through-the-thickness crack without bursting the tank. However, the pressure regulator maintains tank pressure even in the presence of a through crack with the tank leaking. The flaw continues to grow due to stress corrosion in the NTO or MMH environment until the tank fails catastrophically.

Consistency With Observables

A catastrophic failure of one of the bipropellant tanks could lead to critical physical damage of the spacecraft.

Summary of Analysis

Traditionally, the crack sizes screened by nondestructive examination are specified for a 90-percent-probability/95-percent-confidence level of inspection reliability. However, it has been shown by extensive industry experience that the existence of a crack-like flaw of the stated size in any spaceflight tank is a rare event. Therefore, the probability of existence of a part-through flaw with a depth of more than 60 percent of the weld thickness after either cryogenic proof testing or radiographic and follow-on dye-penetrant inspections is a possible, but very unlikely, occurrence.

Fracture mechanics analysis was performed to determine the size and shape of a part-through crack in the weld that could become a through-the-thickness crack (i.e., break through) during MOI pressurization. Breakthrough of a crack is governed by many factors, including local plasticity, shear slips, ligament behavior, geometric nonlinearities, and stress intensity variations. Following a set of transition criteria and using the NASA/FLAGRO crack-growth computer program, the depth of the crack for breakthrough must be in a small portion of the range which is greater than 1.32 mm (0.052 in.) and with a depth-to-length ratio between 0.4 and 1.0.

Calculations were also performed to compare the leak rate from a through-the-thickness crack on the tank to the flow rate of the regulator. Based on a set of conservative assumptions, the leak rate through the crack is much less than the

regulator flow rate. This verified that the tank pressure has a constant pressure during MOI pressurization, even in the presence of a through-the-thickness crack.

Details of the above-mentioned analyses are in the document cited in Footnote 5 of Appendix L.

Conclusion

Industry experience and fracture mechanics analysis results indicate that this hypothesis scenario is almost impossible, but the complexities and uncertainties associated with the modeling of the growth of cracks require caution. Hypothesis C3A is Category B: credible, but very unlikely.

D. Burst of a Bipropellant Tank During MOI Pressurization After Having Been Weakened by Meteoroid Impact (Meteoroid Damages Tank; C3B)

Hypothesis

This hypothesis assumes that a meteoroid impacts a bipropellant tank during the 11 months of interplanetary cruise. The impact location is on a portion of the tank surface where the thermal blankets do not provide adequate protection against meteoroids of certain sizes and velocities. The impact does not cause an immediate burst of the tank, since the pressure telemetry data indicate that no tank leakage occurred during interplanetary transit, but it generates a flaw with a depth between 43 and 70 percent of the membrane thickness of the tank. The flaw does not grow at constant stress during interplanetary transit because its stress intensity is lower than the threshold for stress-corrosion cracking. When the tank is pressurized for MOI, the flaw grows from a part-through crack to a through-the-thickness crack without bursting the tank (the tank membrane is designed to have a leak-before-burst mode of failure). However, the pressure regulator maintains tank pressure even in the presence of a through-the-thickness crack with the tank leaking. The flaw continues to grow due to stress corrosion at constant stress in the propellant environment until the tank fails catastrophically.

Consistency With Observables

A catastrophic failure of the MMH tank could lead to critical damage of the spacecraft.

Summary of Analysis

Flaws can be generated when a tank is impacted by meteoroids. A flaw with a depth greater than 70 percent of the membrane thickness would have caused the tank to burst immediately. Since this did not occur during interplanetary transit, it is known that no flaw of this size or larger was formed due to meteoroid impact on the MMH tank. A flaw of depth less than 43 percent of the thickness does not result in an inner surface spall and such a flaw is assumed not to grow to failure during MOI pressurization. A meteoroid impact that creates a flaw with depth over 43 percent of the thickness results in an inner surface spall. It is conservatively assumed that all flaws with inner surface spall grow to failure during or following MOI pressurization.

A meteoroid impact on a tank surface, both with and without the protection of a thermal blanket, has been analyzed.¹ The flaw with a depth between 43 and 70 percent of the tank membrane thickness that is required to fit this scenario defines the range of meteoroid mass as a function of velocity. This mass, in turn, can be compared with the mission meteoroid fluence to calculate a probability of an impact of the type described in a unit area. This procedure has also been implemented (see Appendix I).

¹ R. Bamford, *Mars Observer Propellant Tank Meteoroid Protection*, JPL Interoffice Memorandum 3543-93-189, Jet Propulsion Laboratory, Pasadena, California, November 1, 1993.

The multilayer thermal blankets surrounding the tanks protect the tanks by changing an incoming meteoroid's form; this is a well-known meteoroid protection approach. These blankets provide more protection if they are held appreciably away from the tank surface, but protection is substantial even if the inner surface of the blanket is in contact with the tank. The protection mechanism is the pulverization and possible change in phase of a meteoroid by the blanket, with a resultant debris cloud that spreads the impact energy over a larger area. This spreading of energy minimizes or eliminates cratering and spalling, and tends to eliminate this potential scenario cause because the impact tends to either cause immediate tank failure or have no lasting effect. In the Mars Observer design, the portions of the bipropellant tanks that protrude outside the spacecraft bus structure are covered by loosely fitted multilayer thermal blankets. With the addition of a nadir panel tent (also made of multilayer thermal blankets) positioned several inches above its surface, the MMH tank is well protected from the meteoroid impacts that could cause this hypothetical scenario. As for the NTO tank, it is difficult to determine the spacing between the tank and its protective thermal blankets because of the lack of reliable information on how the thermal blankets are installed and how they behave in space. However, it is believed that the thermal blankets over the NTO tank tend to have an appreciable distance from most of the tank surface and contribute to adequate protection against the hypothetical meteoroid impacts on the tank.

Conclusion

This hypothesis scenario is assessed to be credible but the probability of occurrence is very low. However, caution is required in addressing the uncertainties related to the installation details of the thermal blankets over the NTO tank, as well as the complexities associated with modeling and analysis of (1) meteoroid fluence, (2) the consequence of a meteoroid impacting the tank surface, and (3) the effectiveness of thermal blankets as a meteoroid shield. Hypothesis C3B is Category B: credible, but very unlikely.

E. Rupture of Tubing During MOI Pressurization (Flaw Ruptures Line; C3C)

Hypothesis

The assembled propulsion lines had their highest vibration loading in the Z-axis direction during the Titan III launch since the integrated Mars Observer spacecraft underwent a ground-based sinusoidal vibration test only in the Y-axis direction. This hypothesis assumes that the combined effect of the mass supported by the tubing and a possibly more severe launch environment results in an undetected part-through flaw in a line growing to become a through-the-thickness crack during launch. This flaw is located in the unpressurized portion of the tubing between the high-pressure pyro valves and the check valves, and thus a leak cannot be detected by telemetry data during the interplanetary transit. When the pyro valves are fired for MOI pressurization, the flaw extends due to increased pressure. This allows helium gas to escape and leads to a secondary failure that could cause the loss-of-signal anomaly.

Consistency With Observables

Rupture of the pressurant line could lead to critical damage of the spacecraft and cause the Mars Observer anomaly.

Summary of Analysis

A structural analysis was performed to determine the probability of occurrence of this hypothesis.² A portion of line not pressurized during interplanetary transit was modeled using the NASTRAN finite-element computer code. Analysis results indicate that the maximum stress in the line is only 96.5 MPa (14 ksi) under the most conservatively estimated launch loads. At this stress level, the probability of a pre-existing part-through flaw in the pressurant line extending to become a through flaw is extremely unlikely.

Conclusion

Analysis shows that this hypothesis scenario is not credible, and the uncertainties associated with structural modeling of the fuel line are not a concern. Hypothesis C3C is Category C: not credible.

² P. Rapacz and S. Sutharshana, *Structural Analysis of MO Pressurant Line*, JPL Interoffice Memorandum 3542-93-320, Jet Propulsion Laboratory, Pasadena, California, October 28, 1993.

F. NSI Expelled/Pyro Valve Failure (NSI Impacts Tank; C4)

Hypothesis

In this scenario, one assumes that a NASA Standard Initiator (NSI) is ejected from the low-pressure pyro valve (PV-5), inflicting critical physical damage. As discussed in Appendix P, this is a failure mode observed during testing for the European Space Agency (ESA) Cluster spacecraft program.

The most obvious “target” for an ejected squib would be the MMH tank. As seen in Figure 7-2, one squib in PV-5 was pointed in the direction of the MMH tank. Other potential targets are the pressurant lines.

Consistency With Observables

If the MMH tank were ruptured, the resulting critical physical damage would be consistent with the observables.

The pressurant line that could be struck is downstream of the MMH check valves. If it were ruptured, massive MMH leakage which might lead to critical physical damage to the spacecraft would be accompanied by attitude rates which might preclude downlink. Such a rupture is less likely than MMH tank rupture since the NSI would have to follow a very particular trajectory, whereas, if it moved in a straight trajectory, it would have a high probability of striking the propellant tank.

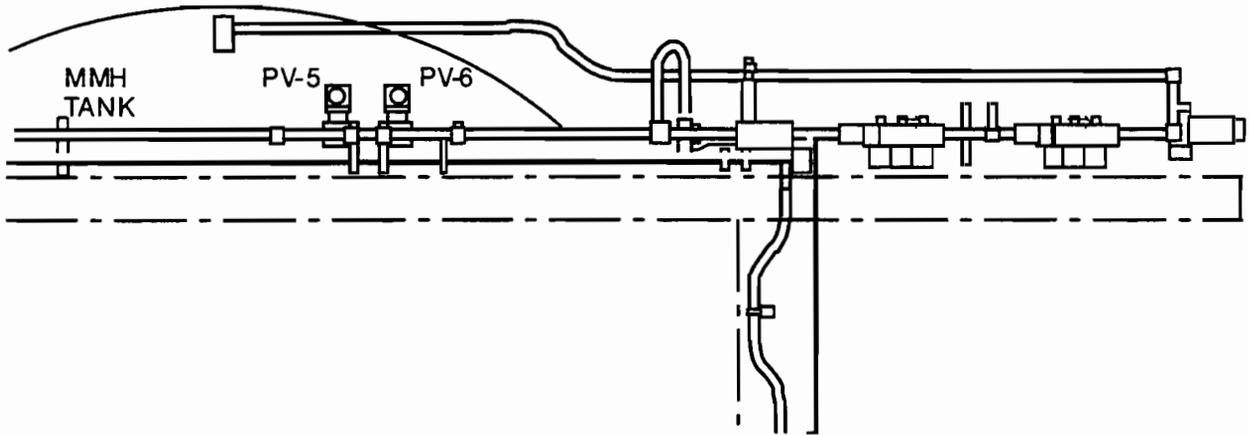


Figure 7-2. Relation of pyro valves to MMH tank (NSI axes are perpendicular to plane of drawing).

Conclusion

Based on the ESA data and x-rays of Mars Observer pyro valves discussed in Appendix P, it appears credible that one of the two NSIs in PV-5 may have been ejected at velocities as high as 200 m/s. One of these NSIs was directed toward the MMH tank. However, the NSI directed toward the MMH tank was not fired electrically; in all the Cluster tests in which an initiator was ejected, the electrically fired initiator was the one ejected. Furthermore, there are small differences between the initiators used in the Cluster program and the NSIs used in Mars Observer, which may have contributed to the initiator ejections in the Cluster program. However, it is impossible to dismiss this failure mode on the basis of available data.

An analysis has been performed to evaluate the damage that could be inflicted by an ejected NSI impacting the MMH tank.³ Results of the analysis showed that if the ejected NSI is moving at a velocity of 200 m/s, it is very possible that it will penetrate the tank wall upon impact and lead to a catastrophic rupture of the pressurized tank.

Hypothesis C4 is Category A: credible.

³ R. M. Bamford, *Effect of NSI Ejection on MMH Tank*, JPL Interoffice Memorandum 3543:93:183:RMB, Jet Propulsion Laboratory, Pasadena, California, October 26, 1993.

G. CIU Hardware Redundancy Control State Indeterminacy (CIU Indeterminacies; C5)

1. SCP In Control (C5A)

There are single failure points in the control interface unit (CIU) whereby a part failure or logic upset can disable critical control functions. In addition to this hypothesis, there are additional potential control logic upsets, from the same mechanism, that can cause adverse consequences with the CIU. They are: I/O Crossed/Not Crossed (C5B), I/O Bus Select (C5C), and RPA Lockup (C16).

Hypothesis

Pyro-firing-induced chassis current alters the state of the Standard Control Processor's (SCP's) control logic in the CIU.

Causal Connection to Sequence

Pyro electrical firing of propulsion valve NSIs during the pressurization sequence.

Anomaly Description

SCP control logic within the CIU is latched into one of four possible states so that neither SCP is in control. This halts effective command generation and results in no RPA turn-on and no attitude control. Changes in this control logic can occur due to EMI derived from induced chassis current.

Relevant Information From Recovery Activity

Ground commanding of SCP-1 power off was tried unsuccessfully, but no ground command is effective if neither SCP is in control.

Summary of Analysis

For pyro firing systems whose energy source has a path through chassis to its return side, it is possible to conduct some of the firing current through chassis. At NSI detonation, current is carried by plasma to the body of the device, then to the structure, and back to the source in parallel with the normal circuit return.

Connecting the primary system power return to chassis provides this path. When this chassis path exists, a large loop can be established that inductively couples energy to another loop that contains the control logic circuitry. With enough voltage and fast rise time, the logic state can be altered or the component destroyed.

Tests have shown that about 1 in 25 NSI firings produces chassis current exceeding 1 A when the electrical firing circuit is similar to Mars Observer's.

For this hypothesis, analysis using 2-A chassis current and 0.5-m spacing between the “culprit” and “victim” loops produces a voltage spike of 31 V at the control circuitry in the CIU. Part testing has shown upset probably at 12 V \approx 5 percent and at 30 V \approx 100 percent.

Conclusion

There have been thousands of NSI firings in space, yet there is only one known and analyzed anomaly that caused an electronic part upset or failure (Magellan 1990).⁴ Firing tests using actual NSIs with a simulated Magellan configuration yielded one voltage spike of 5 V at the part. However, the results are inconclusive because the number of firing samples was severely limited, and furthermore, it was not practical to simulate the entire Magellan electrical configuration.

In addition, the analysis is uncertain due to the complexity of the model and ignores the inherent EMI cancellation. Furthermore, the results of that analysis are very sensitive to spacing of the culprit and victim loops.

The actual configuration is critical, as the location of individual NSIs varies according to the specific device application.

For this scenario, there will be no attitude control following the fault. Analysis shows that the resulting spacecraft rotation with large angle nutation brings the solar panels into and out of view of the Sun in a pattern that results in complete battery discharge in approximately 22 hours. When the spacecraft motion later brings the solar panels sufficiently far back into the Sun, a spacecraft POR occurs. Upon POR, the latchup is cleared and the spacecraft comes up in Safe Mode.

The exact POR sequence depends on the exact voltage levels at which each assembly will be reactivated and cannot be predicted accurately without measurements of the flight hardware itself. As currently understood, as the spacecraft slowly rotates into the Sun, the primary power bus voltage will increase, allowing additional loads to come on line. These additional loads draw current, decreasing the bus voltage, causing loads to drop back off. The bus voltage continues to oscillate in this manner until the solar insolation is adequate to support all loads that are active for the associated bus voltage.

When the IMU is finally powered, it requires about a minute to spin up the gyro rotors. During this time, the (most likely saturated) gyro rate measurements are used to determine RWA control torques—resulting in large RWA torques on the spacecraft. In many (most likely most) cases, these undesired RWA torques will bring the solar panels away from the Sun, resulting in another loss of spacecraft power. In other cases, the

⁴ J. C. Arnett, *Recommended List of Documentation Covering the Magellan Squib Shorting Scenario*, JPL Interoffice Memorandum 5211-93-522, Jet Propulsion Laboratory, Pasadena, California, November 12, 1993.

RWA torques leave the spacecraft in the Sun when the gyro rotors are at full speed (and thus provide valid data), and Safe Mode attitude control will bring the Solar Array normal to Sun-point.

If the RWAs rotate the solar panels out of the sunlight, another opportunity will occur within an hour. Eventually, one of the POR opportunities should result in spacecraft recovery and safe mode control, which includes a "call-home" provision 65 hours later. That no such signal was received lowers the likelihood that this hypothesis is the cause of the Mars Observer loss of signal, but the spacecraft POR response is not yet well enough understood to draw that conclusion.

This scenario will be the subject of future VTL simulations; the results of those tests should give better understanding of the spacecraft POR response, but will never be conclusive since the actual flight hardware is not available for detailed measurements.

Refer to Appendix H for a detailed treatment of Hypothesis C5.

Hypothesis C5A is Category A: credible.

2. I/O Crossed/Not Crossed (C5B)

Hypothesis

Total loss of computational control capability.

Causal Connection to Sequence

Part latch-up caused by a pyro-firing-induced electromagnetic spike.

Anomaly Scenario

The I/O crossed and not crossed signal logic in the CIU is affected by the postulated electromagnetic spike such that neither SCP can access the CIU/CIX I/O bus, or both SCPs can access the CIU/CIX I/O bus.

Relevant Information From Recovery Activity

CIU hardware commands to switch to I/O bus B, and to turn SCP-1 power off were tried unsuccessfully.

Summary of Analysis

In the case where one assumes that both the I/O-crossed and the I/O-not-crossed logic signals are set (high), both SCPs would be able to read and write to both CIU/CIX buses. For read operations, input buffers on both bus sides would be enabled to both buses, but would contain the same data and thus would not cause a problem. Bus contention occurs for bus write operations, resulting in either no output or garbled output to the CIU/CIX buses. This also results in total loss of SCP control function, the inability to process commands (except CIU hardware commands), and loss of attitude control, creating a “no control” spin mode. Nor is control available to configure the telecom downlink and uplink. The “no control” attitude control mode analysis is described in Hypothesis C5A. With some uncertainty, the analysis shows that AACS pointing is good enough to allow uplink and downlink communication over the LGA after the anomaly. A solution to eliminate bus contention is to power off one SCP and command through the other. This was attempted late in the recovery commanding process with no successful outcome observed. Therefore, this I/O bus contention failure scenario is not consistent with the observables.

In the case where one assumes that neither the I/O-crossed nor the I/O-not-crossed logic signals are set (high), neither SCP would be able to write to either CIU/CIX bus. In addition, the CIU/CIX input buffers would not be enabled to either bus and both SCPs would receive all zeros on any buffer read. This results in total loss of SCP control function, the inability to process commands (except CIU hardware commands), and loss of attitude control, creating a “no control” spin mode. Nor is control available to

configure the telecom downlink and uplink. The “no control” attitude control mode analysis shows, with some uncertainty, that AACCS pointing is good enough to allow uplink and downlink communication over the LGA after the anomaly. However, though this is true and the command to switch to the backup I/O bus was tried, it is impossible to force the spacecraft to establish a downlink signal with this failure. This failure scenario is consistent with the observables.

Conclusion

The possibility of Hypothesis C5B occurring is of the same order as that assigned to Hypothesis C5A, SCP In Control—Category A: credible.

3. I/O Bus Select (C5C)

Hypothesis

Total loss of computational control capability.

Causal Connection to Sequence

Part latch-up caused by a pyro-firing-induced electromagnetic spike.

Anomaly Scenario

The I/O Bus Select A and B signal logic in the CIU is affected by the postulated electromagnetic spike such the neither I/O bus A or B is selected, or both I/O buses A and B are selected.

Relevant Information From Recovery Activity

CIU hardware commands to switch to I/O bus B, and to turn SCP-1 power off were tried unsuccessfully.

Summary of Analysis

The analysis for the assumed case where both I/O buses A and B are selected is similar to the case where both the I/O-crossed and the I/O-not-crossed signals are set. (See Hypothesis C5B.) In this case, the failure scenario is not consistent with the observables.

The analysis for the assumed case where neither I/O bus A or B is selected is similar to the case where neither the I/O-crossed nor the I/O-not-crossed signals are set. (See Hypothesis C5B.) In this case, the failure scenario is consistent with the observables.

Conclusion

The possibility of Hypothesis C5C occurring is of the same order as that assigned to Hypothesis C5A, SCP In Control—Category A: credible.

H. SCP Software Problem (C6)

Hypothesis

This hypothesis addresses a generic class of software problems caused by a design or implementation error present in the code of both SCPs. (See the discussion of Hypothesis N6 for a related class of software problems caused by a single event upset.)

The cause of the anomaly is a flaw in the design and/or implementation of the code: a logical error, erroneous constant, inappropriate instruction, etc. The triggering mechanism could have been a particular command in the pressurization sequence, or it could have been a chance alignment in time of nonsynchronous events among the software tasks, or it could have been a hardware fault triggering flawed fault-protection code. A number of scenario types can be postulated that could match the observed symptoms, but these can be generally grouped into two categories: flaws that cause “quiet” loss of SCP control and flaws that cause the SCP to issue spurious, destructive commands. The first type causes the SCP to be inoperative and unrecoverable, while the second type causes spacecraft system action resulting in physical destruction or in rates and/or attitudes that preclude downlink. The following scenarios give illustrative examples of these failures. In general, the scenarios fit the observables only in the cases where attitude control effects preclude the reception of ground commands or where there are unrecoverable physical effects.

Example A begins with SCP-1 withholding MEOK due to the hypothesized flaw. Control is transferred to SCP-2, which is experiencing the same flaw. However, because Safe Mode is inhibited (for MOI), it cannot withhold MEOK. It may be postulated that the flaw affects the SCP’s ability to generate commands to the SCU so it cannot turn the RPA beam on either via the stored sequence or ground commands.

Example B assumes both SCPs become locked in a tight loop not unlike the situation that happened to the attitude control computer on Magellan. In the Magellan case, there were two independent “watchdogs” which needed to be reset by the software. Only one of two “watchdogs” was serviced within the loop, so the anomaly was detected. In this Mars Observer scenario, the MEOK signal is generated within the postulated loop and is the *only* “watchdog,” so there is no onboard detection of the anomaly.

Example C consists of a program flaw that causes both programs to vector off into data words that are interpreted as instructions. This can result in rapid, unpredictable, and bizarre events —viz. runaway program execution (RPE). The RPE can result in gross alteration of code and can destroy sequencing and uplink command decoding routines. It could possibly leave the MEOK-generation software intact and settle out in a quiescent but uncommandable state.

The final example, D, involves a program runaway that has external hardware effects. This RPE causes spurious, destructive commanding to external attitude control

or propulsion equipment. Examples of commanding are thrusters or engines commanded on permanently or reaction wheels torqued in a random way. The results could range from uncommandability due to attitude to destruction of the spacecraft due to high rotational rates.

Consistency With Observables

Example A is not consistent with the ground-commanded recovery sequence, assuming that the SCP-1 Power Off/On and Select SCP-1 commands were received. These are CIU hardware-decoded commands, and would force SCP-1 to undergo a power on reset, which would initiate ROM program execution followed by transferring control back to SCP-1. (It is very difficult to conceive that the ROM code would be flawed and experience the same anomaly that the RAM code experienced.) Ground commands to SCP-1 would turn the RPA beam on and provide a downlink over the LGA. The one exception to this recovery scenario's success is if the flaw affects attitude control and the spacecraft attitude and/or rate preclude getting the SCP-1 Power Off/On and Select commands into the spacecraft.

The consistency of example B is identical to that of example A. Barring extreme problems with the spacecraft attitude or rate, the command to power SCP-1 off and on would have enabled subsequent commands to produce at least an intermittent downlink.

Example C is consistent with the observables only if the SCP-1 Power Off/On and Select commands were not received.

Example D fits the observables. The question of whether the SCP is able to process command bits properly is moot, since uplink lock either cannot be attained or the spacecraft has suffered unrecoverable physical damage.

Conclusion

That a software flaw caused the initial and continued loss-of-downlink anomaly is not impossible, but it is nearly impossible given the ground recovery commanding. Commanding of the pressurization pyro functions was, of course, not previously done in flight. However, the only new code used consisted of data words, which would not normally cause looping or other program control anomalies and these data words would not be involved in ROM operations. With respect to a hardware fault triggering flawed code, all fault protection code has been run in the VTL, which reduces the possibility of undetected flaws in RAM code. Adding in the differences between ROM and RAM code makes this failure mode even less possible. This leaves a chance alignment of software operations that had previously been transparent to each other. For this to have happened with no prior symptoms during ground test is highly unlikely, although not impossible. Hypothesis C6 is Category B: credible, but very unlikely.

I. Miswired Pyros (C7)

Hypothesis

Undetected design, integration, and test error.

Causal Connection to Sequence

Pyro firing.

Anomaly Scenarios

Assuming that the pyro-valve firing order is reversed, PV-5 (low pressure) fires before PV-7 (high pressure) leading to an unintended and increased level of oxidizer and fuel mixing and a potential explosion.

The HGA inboard boom and/or wrist hinge pyros fire instead of one or both of the expected pyros. This either partially or fully deploys the HGA into the mapping position, resulting in the HGA pointing away from Earth in an orientation off Earth point.

The Solar Array gimbal-support and center-panel-release pyros fire instead of the expected pyros. This deploys the Solar Array into a partial mapping position such that the Solar Array does not point at the Sun, but rather in a position along the $-Z$ -axis, and the batteries begin to discharge.

Relevant Information From Recovery Activity

Attempts to configure downlink communications on the LGA were tried unsuccessfully.

Summary of Analysis

The following analysis activities were undertaken:

- (1) The pyrotechnic electrical system was reviewed
- (2) The system I&T activity, including pyro simulator test, pyro shock, and deployment tests, was reviewed
- (3) The pressurization sequence was reviewed in some detail
- (4) The process used to generate the pressurization sequence was reviewed
- (5) The process to test the pressurization sequence in the VTL was reviewed
- (6) REDMAN and portions of the SCP flight software used to execute the pressurization sequence were reviewed
- (7) The list of recovery commands used was reviewed
- (8) The Contingency Mode response was reviewed in some detail
- (9) Performance specifications for the SCPs, CIU, CIX, SCUs, and PRAs were reviewed
- (10) Schematics and materials and parts lists for the CIU, CIX, SCUs, and PRAs were reviewed
- (11) Held discussions and interviews with Astro personnel involved with C&DH, flight software and REDMAN, pyrotechnic electrical system, and system I&T

- (12) Held numerous discussions and interviews with JPL flight team members involved with C&DH, flight software and REDMAN, Power Subsystem, VTL, and sequencing
- (13) Reviewed memos documenting previous analysis and simulations of premature Solar Array deployment failure scenarios performed by the JPL flight team
- (14) The ordnance (pyro) harness interconnection diagram and wire connection list, and core harness wire connection list were reviewed
- (15) Submitted a set of questions to the JPL project and key Astro personnel to clarify remaining issues

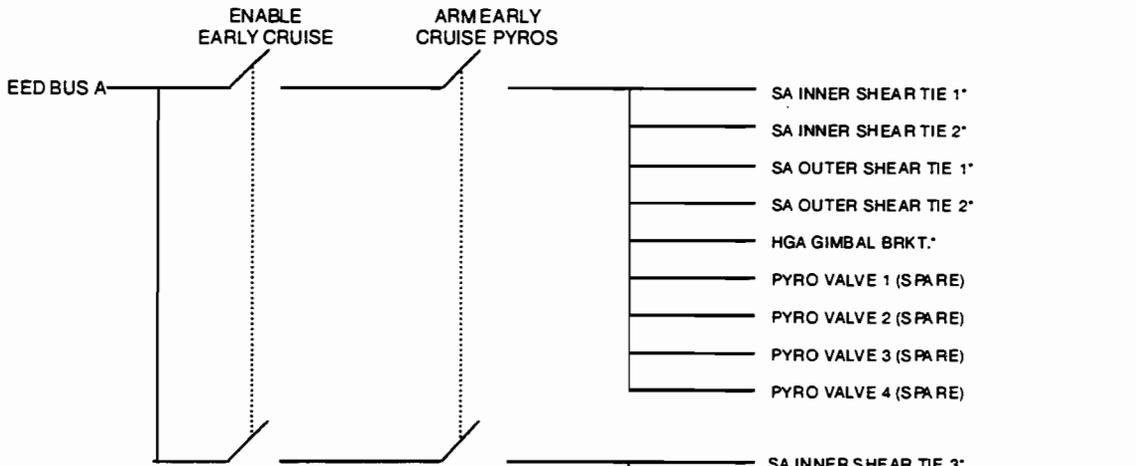
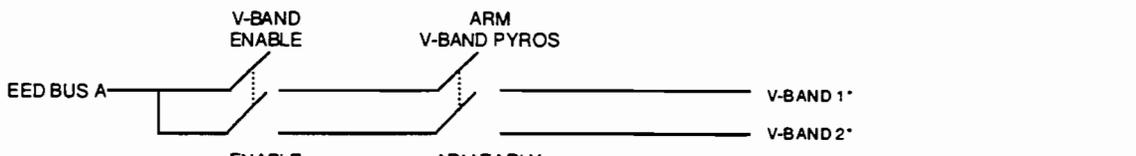
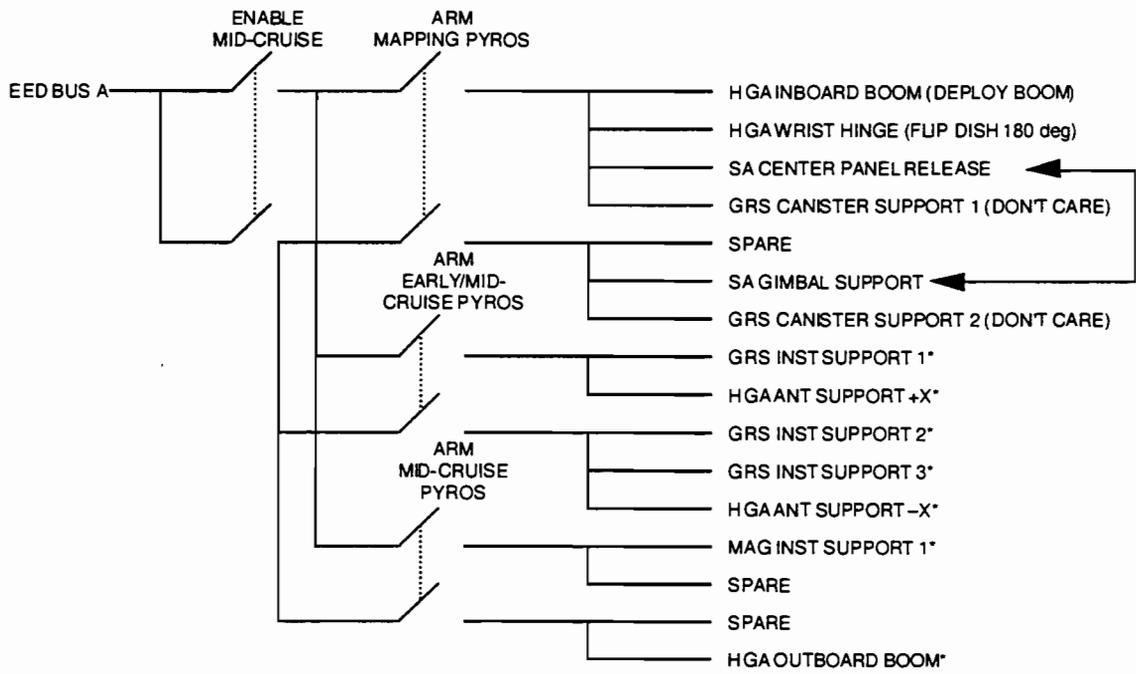
The results of this analysis activity follow.

The pyro bus Enable and Arm System is shown in Figure 7-3. This figure shows which pyros were fired previously in the mission, the pyros planned to be fired, and other pyros that may have been fired instead. Testing included an end-to-end pyro harness, pyro shock, and a number of deployment tests. The end-to-end pyro harness test verified that all the proper pyros fire using a pyro simulator connected to all electroexplosive device (EED) inputs simultaneously (Figure 7-4). Each individual pyro output was verified to be enabled, armed, and fired, and no other EED was inadvertently fired. In addition to verifying the pyro harness, this test verified the EED functions of other spacecraft components, including the SCP, CIU, CIX, SCUs, and PRAs. To prevent damage to the PRA relays, the pyro simulator limits the current through the harness to 2 A. The spacecraft configuration was not changed in any area that might have affected the pyro events after the last time the full end-to-end pyro simulator verification test was performed in May 1992.

The pyro shock test fired test PV-5 (prime) and PV-8 (the backup to PV-7). This test, as with the deployment tests, verified the functions of spacecraft components associated with their respective pyro events.

Although some questions remain (How many pyro shock test firings were performed? Which pyro valve is 5 and which is 6?), it is almost impossible that the planned pyro firing order was reversed (PV-7 then PV-5). However, if the firing order were reversed, this scenario would then couple to Hypothesis C1B and be consistent with the observables only if Hypothesis C1B results in the loss of the spacecraft.

Pyros to further deploy the HGA require different enable and arm commands and circuits to fire than do PV-5 and -7. At least three separate failures would be required for this scenario: a miswire of a pyro and a miswire or an error of both the enable and arm functions in the SCU. Additionally, if the HGA had deployed, recovery commands sent from the ground should have enabled communications on the +Y LGA. This scenario is not consistent with the observables.



NOTE: THERE IS AN IDENTICAL GROUPING OF RELAYS FOR EED BUS B.

* PYROS FIRED PRIOR TO 8/93

← SECOND
 ← FIRST
 } PLANNED SEQUENCE

Figure 7-3. Pyro bus Enable and Arm System (primary side shown).

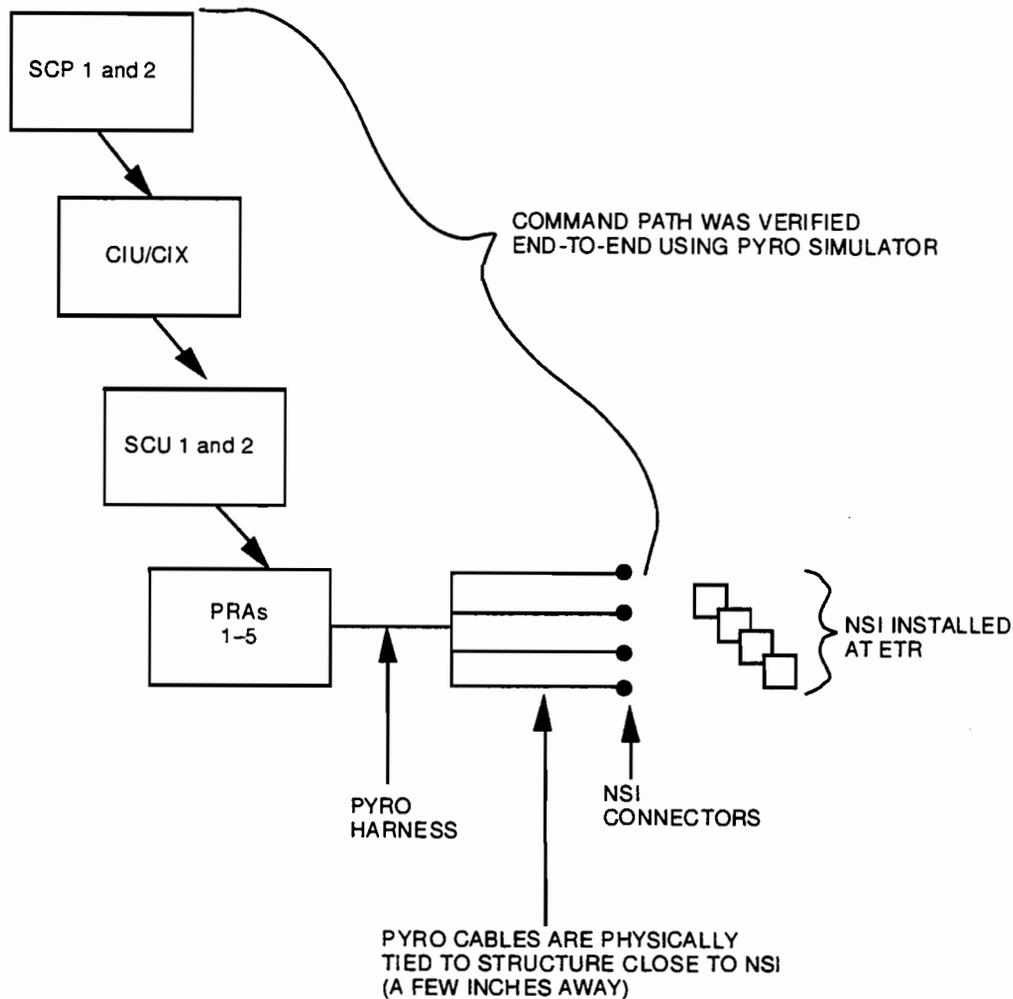


Figure 7-4. Flight pyro harness testing.

The Solar Array is further deployed only if both the center-panel-release and gimbal-support pyros fire. These pyros require different enable and arm commands and circuits to fire than do PV-5 and -7. At least three separate failures would be required for this scenario: a miswire of both the center panel release and gimbal support pyros and a miswire or error of both the enable and arm functions in the SCU. However, if these pyros fire instead of the two expected pyros, the Solar Array will partially deploy into a mapping position such that the Solar Array does not point at the Sun, but rather in a position along the $-Z$ -axis (Figures 7-5 and 7-6). With the Solar Array in this position, the array is not illuminated by the Sun and the batteries begin to discharge. Attitude control will exit Deploy Mode, enter Sun-Star-Init, and then enter an Array-Normal-Spin control state resulting from the commands issued by the pressurization sequence. Noting that Sun sensor head 4 is located on the Solar Array, there are four possible results with respect to Sun visibility and attitude control response.

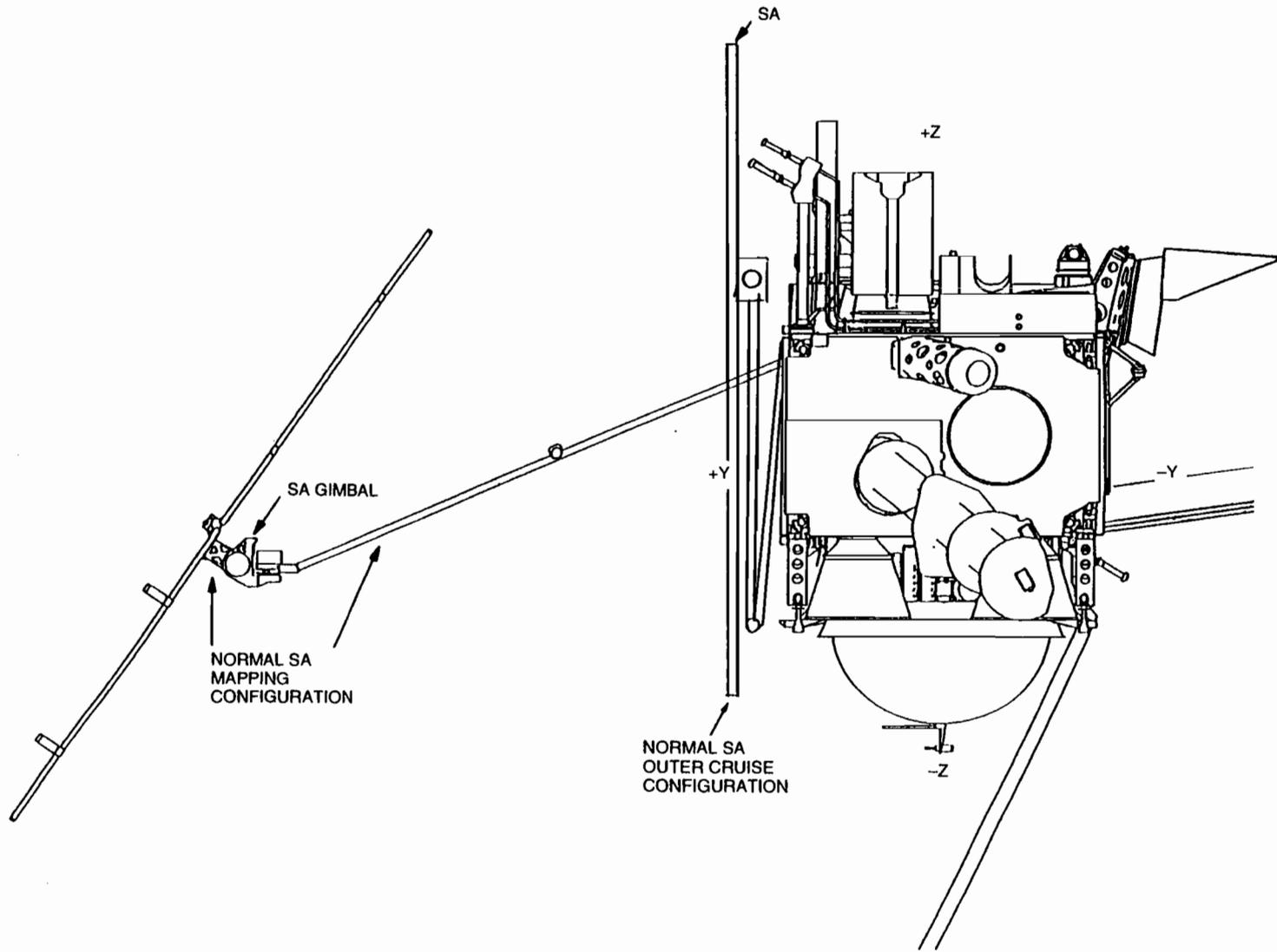


Figure 7-5. Solar Array outer cruise position and mapping positions.

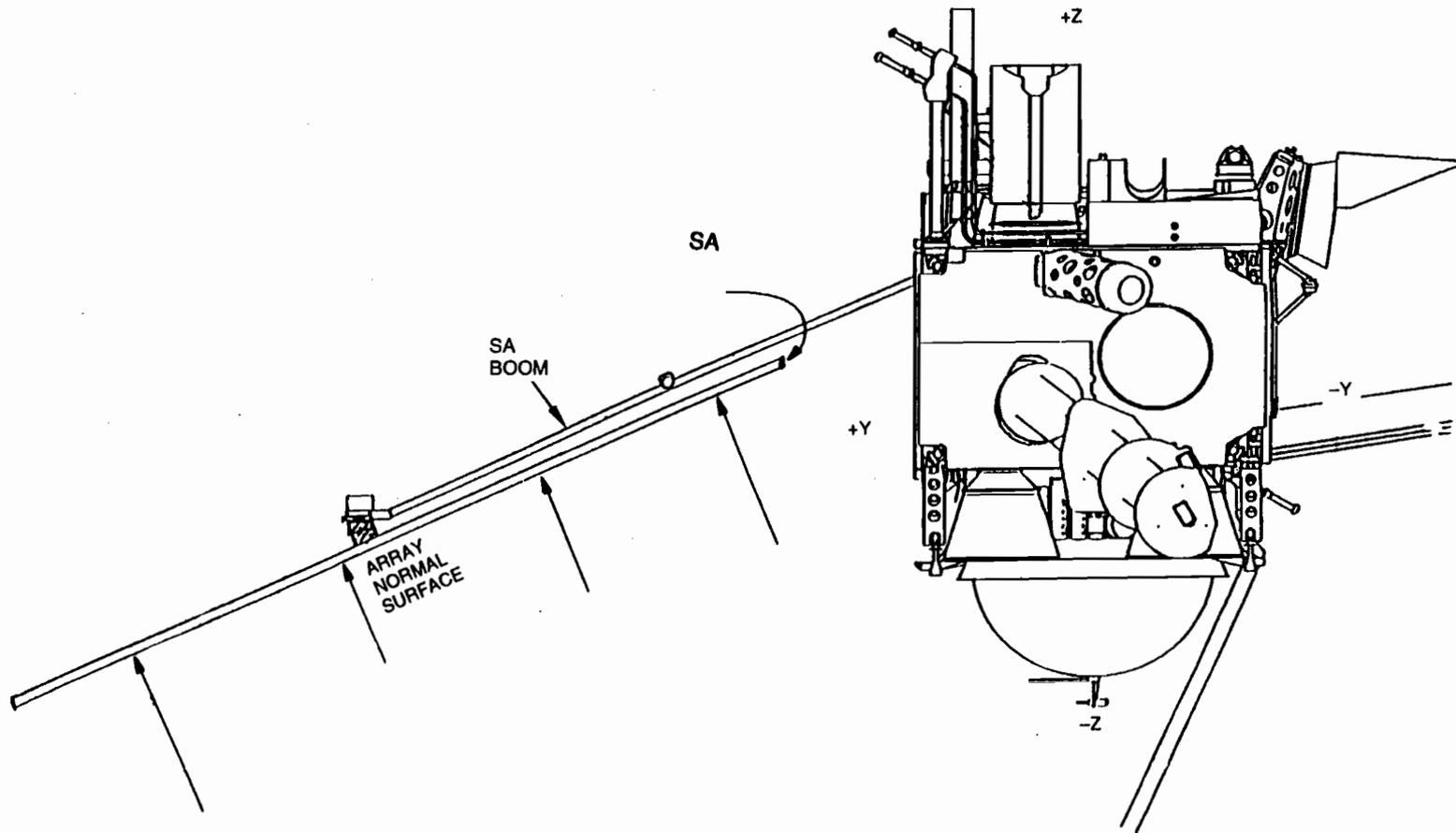


Figure 7-6. Solar Array deployed in partial mapping position.

First, sensor head 4 does not detect a Sun signal, but other spacecraft-body-mounted Sun sensors do. AACS will maintain the ANS state. The pressurization sequence would put communications on the HGA as planned. This state would continue for approximately 2 hours, until the battery SOC fell to 66 percent, at which time Contingency Mode would be entered. The Contingency Mode response would configure the uplink and downlink over the LGAs, but not turn on the RPA beam because of the low SOC condition. This scenario appears inconsistent with the observables, since HGA downlink would be maintained for about 2 hours until the batteries discharge and cause entry to Contingency Mode.

Second, no sensor detects a Sun signal. AACS will maintain the ANS state. The pressurization sequence would put communications on the HGA as planned. This state would continue for about 1 hour until REDMAN begins to swap Sun sensor heads and then CIU/CIX I/O buses. Swapping heads and I/O buses does not help, so a Sun search followed by Contingency Mode entry occurs. This scenario appears inconsistent with the observables since HGA downlink would be maintained for at least 1 hour and some minutes after the initial transient.

Third, sensor head 4 detects a Sun signal stronger than any other Sun sensor. This possibility is highly unlikely given the orientation of the Solar Array. However, AACS will maintain the ANS state, and start a 15-min timer at the time the SA normal deviates by more than a few degrees from the Y-axis. This timer could begin after PV-5 was fired in the nominal sequence. The pressurization sequence would put communications on the HGA as planned. This state would continue for a short time and would maintain HGA downlink communications for about 11 min after the RPA beam comes on. Then the AACS will accept the new Sun location indicated by Sun sensor head 4, assuming that the Solar Array is still pointing in the +Y direction, and slew the spacecraft to point the +Y-axis to the new Sun position. Further complex AACS responses result, but are not key to this scenario. This scenario appears inconsistent with the observables since HGA downlink would be maintained for an adequate time after the RPA beam comes on to observe a signal.

Fourth, no sensor sees the Sun in the +Y-axis, but Mars is accepted as the Sun. This scenario is similar to Probable Cause S6, Sun Sensor Head 4 Failure and is inconsistent with the observables since HGA downlink would be maintained for an adequate time to observe a signal after the initial transient.

Conclusion

This is an obvious concern even though few (if any) possibilities would be a credible cause of the actual anomaly. All information shows that the pyro circuits were carefully checked in assembly and test. Because of differences between mechanical and electrical drawings, some question exists as to whether PV-5 (prime) or PV-6 (PV-5 backup) was fired. However, if PV-6 fired, potential danger would exist only if oxidizer were present in the Pressurization System. Analysis of the hypothetical cases where the HGA and the SA are deployed shows them to be inconsistent with the observables. The possibility of this hypothesis occurring is vanishingly small. Hypothesis C7 is Category C: not credible.

J. Sequence Error (C9)

Hypothesis

In this hypothesis, a sequence error is defined as either a mistake in specifying an intended command, a mistake in specifying the intended time of execution of an intended command, or an unanticipated consequence of the intended sequence of commands. An error caused by faulty memory management of the stored sequence can be considered a sequence error or a (ground) software error. For all intents and purposes, the result of a sequence memory management error can look like almost anything conceivable. Practically speaking, however, this can be dispensed with after having closely investigated the actual memory locations used.

In the broadest sense, a sequence error could be considered to do almost anything, including, for example, switching between high- and low-gain antennas with a period less than the time required for ground receiver signal detection (10 s). Rather than pursue every possible malicious sequence, it seems better to prove that the sequence loaded into the spacecraft was the intended one, and consider single deviations to it. For example, the RPA Beam On command may have been mistakenly specified to be Beam Off or was omitted altogether. Another example is a command in the sequence that caused a 180° turn. A final example is that the delta time word prior to any of the commands after the first one in the pressurization block could have been mistakenly specified to be very large (by several weeks or months).

An example of the third type of sequence error, i.e., the intended sequence having an unanticipated consequence, would be the execution of two pyro valve openings within 5 min of each other, causing physical damage in the Propulsion Subsystem. However, ground testing never tested valve opening with a loaded Propulsion System or tested two valve openings as close as 5 min. Note that actual examples of this type of hypothesis would result in a unique entry in the list of hypotheses.

Consistency With Observables

All of these scenarios have been developed to produce the symptom of an initial lack of a downlink signal. However, none will continue to maintain the lack of downlink. Downlink would have eventually been restored either through an onboard fault detection and response or via the recovery commanding pursued by the ground.

In addition to not being able to produce a sequence error that would fit the observables, the sequence was run completely in VTL, both before and after the anomaly. While it is not guaranteed that VTL or the analysis of VTL output provides a foolproof verification, it is almost impossible that a sequence error of the first or second type would not be detected.

Conclusion

The results of VTL simulations and consideration of the recovery commands sent show that this hypothesis scenario is almost impossible, but the complexities and uncertainties associated with the modeling and analysis require caution. This hypothesis is not a credible potential cause of the actual Mars Observer anomaly unless there is an error or oversight in the modeling or analysis. Hypothesis C9 is Category B: credible, but very unlikely.

K. Skew RWA Stall (C10)

Hypothesis

A skew RWA motor stalls when used in Deploy Control Mode.

Causal Connection to Sequence

A skew RWA had been off and was turned on by sequence.

Anomaly Scenario

A motor stalls due to debris or excessive friction, which causes the motor to burn out, draw excessive current, or dissipate excessive heat.

Conclusion

The sequence was analyzed to determine how long a wheel could be stalled before corrective action was taken. The passive wheel test is effectively disabled in Deploy Mode, so a wheel could be stalled during the entire 6 min of Deploy Control Mode. After Deploy Mode is terminated, no more control torque commands are sent to the skew wheel, and it is powered off 10 min later by the sequence. For the X, Y, and Z wheels, once Deploy Mode is exited, the passive wheel test will detect a stalled wheel in seconds and swap to the backup (skew) wheel. Conclusion: no more than 6 min of wheel stall would be possible.

The manufacturer was consulted on what the effect of a stall would be on an RWA. An RWA draws 2.5 A in stall, which will cause a 0.4 C °/min temperature rise. This gives less than a 2.5 C ° rise in the 6 min available and leaves the wheels well within their flight allowable temperature limits and even below 20 °C.

The spacecraft Power Subsystem Team was asked if this unanticipated power load would have been a problem and concluded that it could be easily handled.

Conclusion

Analysis shows that this hypothesis is not credible and the complexities and uncertainties associated with the modeling are not a concern. This hypothesis is not a credible potential cause of the actual Mars Observer anomaly. Hypothesis C10 is in Category C: not credible.

L. Loss of Exciter Frequency Reference (C11)

Hypothesis

Both MOT exciters are unable to generate drive to the RPAs because of a loss of frequency excitation from all available sources.

Causal Connection to Sequence

Exciter 2 was active at the start of the pressurization sequence and was commanded off during the sequence. Near the end of the sequence, exciter 2 was commanded back on to initiate the downlink.

Anomaly Scenario

A single failure point or control circuit/strategy failure is postulated to exist such that all available frequency references are removed from the exciters. The resulting state would preclude any drive to the RPAs and cause complete loss of the downlink.

Relevant Information From Recovery Activity

The recovery strategy repeatedly ground-commanded the exciters on as part of the RPA Beam On SCP software macro. Individual SCP discrete commands were subsequently sent to turn on the exciters. Tracking periods existed with and without an uplink that would have automatically selected between receiver VCO and the USO or auxiliary oscillator for downlink excitation.

Summary of Analysis

Each MOT exciter can generate a downlink from any of three frequency references: the VCO in the associated MOT receiver, the auxiliary oscillator in its own exciter, and the USO. The VCO can only be selected when the receiver is phase-locked to an uplink signal. That selection normally occurs automatically unless overridden by a two-way noncoherent (TWNC) command.

Analysis has shown⁵ that no single failure point exists within the telecom subsystem that can prevent *all* three frequency sources from being available for downlink generation. In addition, if control lines, which are separate to each of the MOTs, should fail, the fault routines in REDMAN would have corrected the problem by swapping exciters.

⁵ J. Webster, *Response to JPL Review Board Question C11*, JPL Interoffice Memorandum SCT-93-0630, Jet Propulsion Laboratory, Pasadena, California, October 15, 1993.

Conclusion

Analysis shows that this hypothesis scenario is not credible and the complexities and uncertainties associated with the modeling are not a concern. Hypothesis C11 is Category C: not credible.

M. Hardware/Software Conflict Preventing RPA Turn-On (C12)

Hypothesis

A conflict existing between hardware fault protection and software commandability is preventing use of either RPA, resulting in no downlink.

Causal Connection to Sequence

RPA-2 was active at the start of the pressurization sequence. Both RPA-1 and RPA-2 filaments were on at the start of the sequence. During the sequence, the RPA-2 beam was commanded off by SCP macro and both RPA filaments were commanded off by SCP-discrete commands. The RPA-2 filament and beam should have been commanded back on by the SCP software after the scheduled pyro firings.

Anomaly Scenario

Use of the filament off commands in addition to the SCP macros is postulated to have established an incompatibility in the spacecraft onboard state tables. The use of a SCP software macro to turn back on the RPAs might not work as a result of a conflict between the selected state and the current state.

Relevant Information From Recovery Activity

Ground commands have been repeatedly sent using the SCP macro procedures in the telecom task of the SCP software. Individual SCP-discrete commands have also been sent to turn on the filaments and beam voltages to the RPAs.

Summary of Analysis

An analysis of the onboard sequence and ground commanding performed during recovery attempts has revealed no mechanism that could cause this hypothesized conflict. SCP software commands were issued as well as SCP-discrete commands during the recovery attempts.

Conclusion

Analysis shows that this hypothesis scenario is not credible and the complexities and uncertainties associated with the modeling are not a concern. Hypothesis C12 is Category C: not credible.

N. RPA Coil Single-Point Failure (RPA Coil Short; C13)

Hypothesis

Events associated with the MOI pressurization sequence (such as described in Table 6-1) may dislodge debris (conductive contamination) and locate it next to coil L2-B, causing a short circuit, or some manufacturing defect at the coil causes a short. This short puts the RPA-B relay on-coil in a permanent short condition, and RPA-A is placed via interlock circuitry in a permanently off state. The RPA internal circuitry may prevent the RPA beam from coming on if the filament was not previously on.

Consistency With Observables

Both RPA-A and -B were powered off during the pressurization sequence. Thus, the initial condition of the two relays of RPA-A and -B is off. This was done by pulsing Q1-A and Q1-B on to energize the L1-A coil of Relay A and the L1-B coil of Relay B (Figure 7-7).

This hypothesis assumes that there was some debris or conductive contamination present in Relay B at the time the pressurization sequence was initiated. The coil has 1- to 2-mm leads 1 to 2 mm apart and, therefore, conductive contamination of at least that

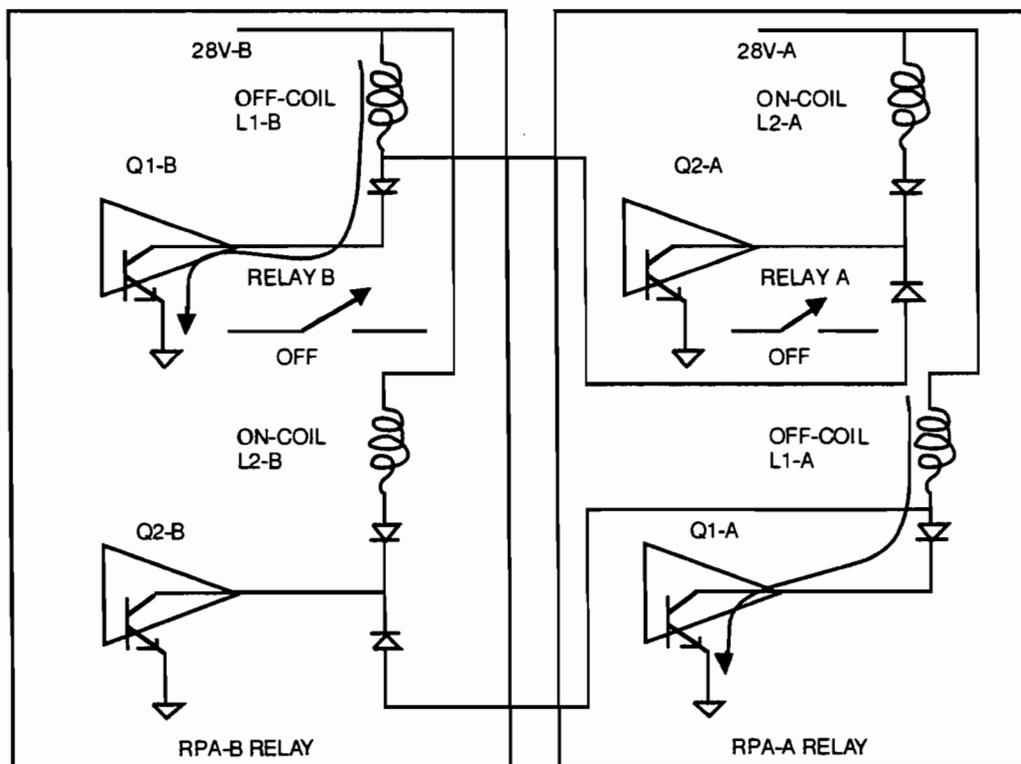


Figure 7-7. Initial condition, both relays are off.

dimension would have to be present. Events described in Table 6-1 (e.g., pyro mechanical shock) could have moved this debris to coil L2-B, thus causing a short circuit of coil L2-B (Figure 7-8).

As part of the pressurization sequence, RPA-B is powered on to get beam-B on. The transistor Q2-B is now turned on. The normal resistance of the L2-B coil is 1.5 k Ω ; therefore, the normal current is 18 mA. Since the debris has now shorted the L2-B coil, there will be no more current limiting to the Q2-B transistor. The current flowing to Q2-B can be 2.8 to 28 A. This current would overstress the Q2-B transistor, with a high probability that Q2-B would now be shorted. This would turn on the L1-A coil. (This is the intentional design of the interlock circuit: whenever RPA-B is turned on, RPA-A has to be turned off—i.e., both RPAs cannot be turned on at the same time.) Since L1-A was previously energized, the RPA-A relay would now be in the permanently off position (Figure 7-9).

In addition to the short caused by debris, one can also speculate that there could be a manufacturing defect at the L2-B coil that could cause the coil to become shorted. This defect could also be aggravated by a mechanical shock like the pyro event.

The transistor has not been studied in detail. Tests could be performed on the device to see if a shorted transistor, caused by high current, can be blown open (or healed with

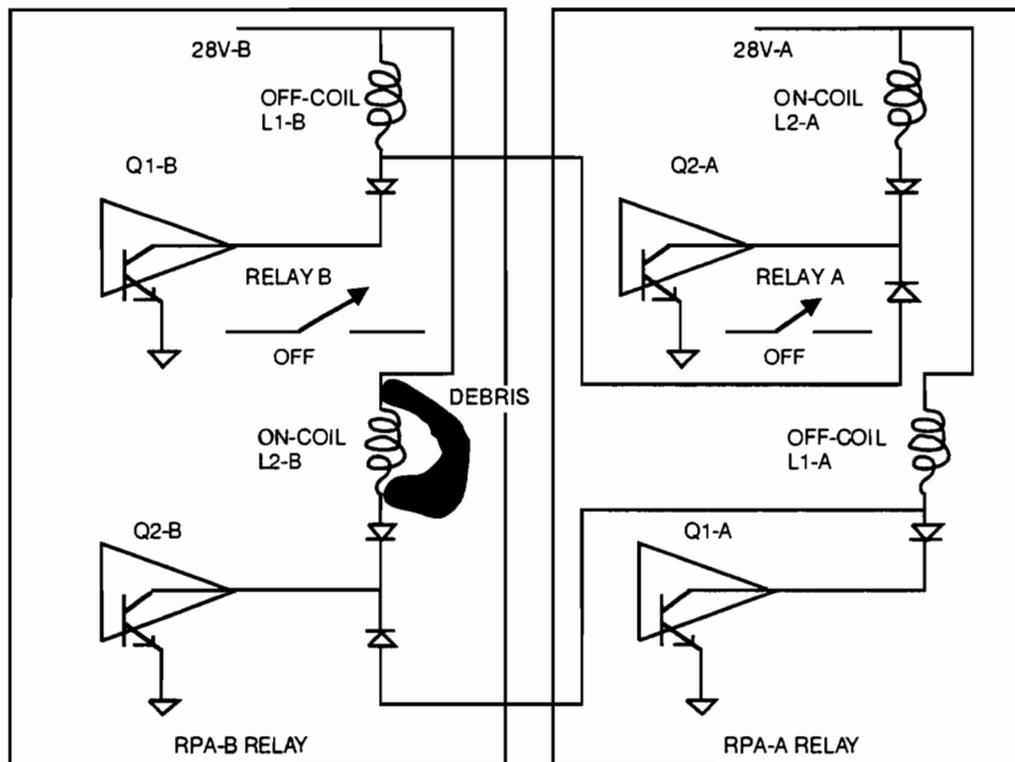


Figure 7-8. Pyro shock leads to internal debris, which leads to short across coil L2-B.

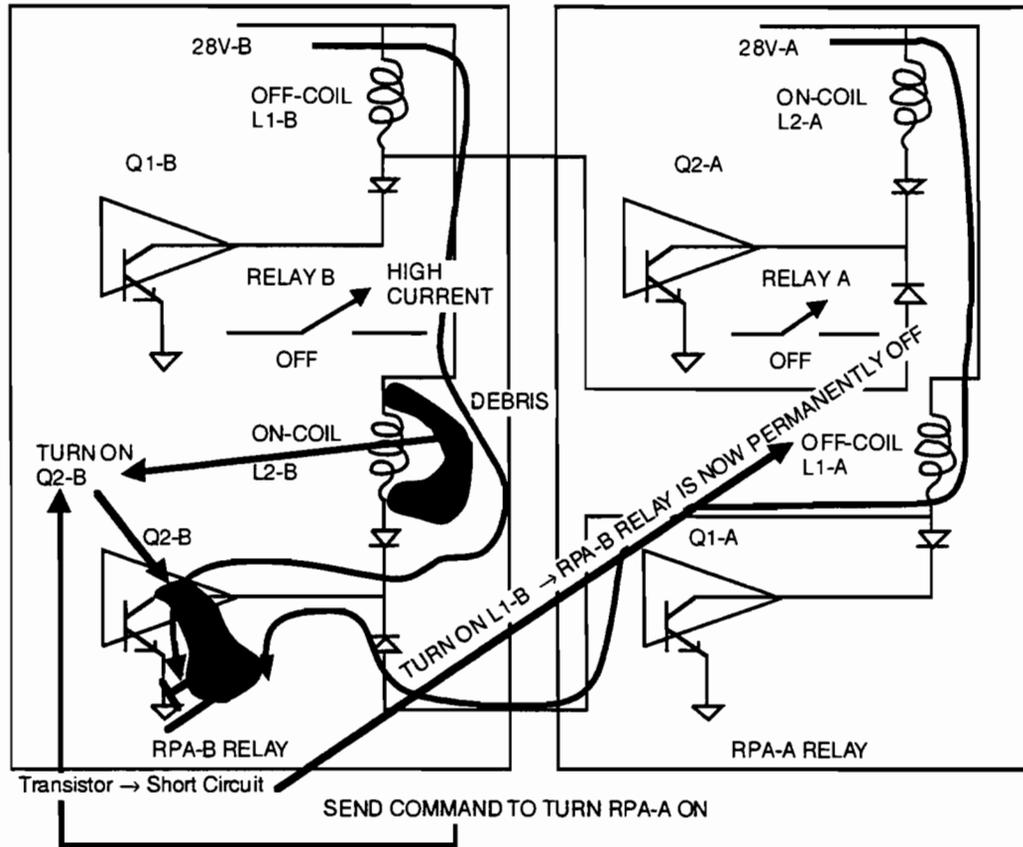


Figure 7-9. Send command to turn RPA-B on.

time). Based on the possibility that the transistor could become open, it has been recommended that the Project send Beam-B Off, then Beam-A On commands, but with a duty cycle less than 10 percent to preserve the health of Relay A, since both the on- and off-coils of Relay A are now energized.

Conclusion

This hypothesis depends on some latent manufacturing defect that manifests itself during the pressurization sequence, or on the presence of some conductive contamination near the location of the L2-B relay coil LGAs that dislodges and shorts the relay coil at the time of the pyro event. The likelihood of a manufacturing defect that manifests itself during the MOI pressurization sequence would clearly be in the class of a straw that broke the camel's back—i.e., extremely unlikely. The presence of conductive contamination that occurs during this period is more conceivable, but is considered very unlikely. Hypothesis C13 is in Category B: credible, but very unlikely.

The categorization of this hypothesis is subject to change once the Mars Balloon Relay (MBR) experiment is concluded. That proposed experiment is discussed in Appendix U of this report. The results of that experiment may provide sufficient information to allow adjustment of the category ranking for this hypothesis.

O. RPA Overcurrent Detector Prevents Turn-On (RPA Overcurrent Protection; C14)

Hypothesis

The RPAs have autonomous hardware failure protection to automatically turn off the RPA when an overcurrent condition exists. If the power bus voltage is abnormal, this overcurrent condition may be triggered during a commanded RPA Beam On event, which would prevent a downlink from occurring.

Causal Connection to Sequence

The RPA was intentionally turned off during the pressurization sequence. Later in the sequence, it was commanded back on. Had a spacecraft power condition prevailed such that the power bus had an abnormal voltage, the RPA could possibly be affected.

Anomaly Scenario

The overcurrent sensing circuit design appears to be marginal in that the in-rush current normally induced comes close to violating the trip condition for the circuit. The nominal design for the sensing circuit is to tolerate 140 W with a detection time constant of 10 ms. If the spacecraft power bus were abnormally low in voltage due to a power fault elsewhere in the spacecraft, then the current consumed might exceed the overcurrent detection threshold and neither RPA would come on.

If the overcurrent trip turns the RPA off, then a Beam Off command followed by a Beam On command must be received before it will attempt to turn on again.

Relevant Information From Recovery Activity

The RPA was commanded on multiple times in the recovery activity. Both SCP software and discrete commands were used. The SCP software command script contains the required Beam Off/Beam On command sequence to accomplish the desired reset of the overcurrent trip condition. Also, SCP discrete commands to turn off and on the beam were used.

Summary of Analysis

An in-depth analysis was performed using schematics provided by the RPA supplier.⁶ That analysis shows that there is at least a 50-percent margin from the hypothesized failure during normal bus voltage conditions. Even when the bus voltage is assumed to drop to where a separate RPA undervoltage protective circuit will function, there is still a slight margin to prevent this hypothecated condition.

⁶ J. White, *Analysis of Overcurrent Trip in MO TWT Power Supply*, JPL Interoffice Memorandum 342-D-93-204, Jet Propulsion Laboratory, Pasadena, California, October 20, 1993.

Conclusion

Analysis shows that this hypothesis scenario is not credible and the complexities and uncertainties associated with the modeling are not a concern. Hypothesis C14 is Category C: not credible.

P. Erratic Activity on Critical CIU Hardware Interfaces (Erratic CIU Interface; C15)

Hypothesis

Three different critical interfaces are included here: erratic activity on the gyro channel select line can corrupt data on one gyro axis; the RXO backup select line can generate an erratic clock into the CIU, disrupting C&DH timing; and the IMU interface select line can corrupt gyro data for all axes.

Causal Connection to Sequence

Possible mechanical hairline break of traces, cold solder joint or erratic digital integrated circuit behavior could be related to an internal chip fault. These effects (described above) might result from thermal stress, pyro-firing-induced mechanical shock, or an electromagnetic spike, as in Hypothesis C5.

Anomaly Scenario

Erratic activity on the gyro channel select line can corrupt data on one gyro axis and result in loss of attitude control. Erratic activity on the RXO backup select line can generate an erratic clock into the CIU, disrupting C&DH timing and resulting in total loss of effective spacecraft control functions. Erratic activity on the IMU interface select line can corrupt gyro data for all axes and result in loss of attitude control.

Relevant Information From Recovery Activity

Ground commands have been repeatedly sent to switch to the backup RXO, with no success. No ground commands have been sent to switch any of the gyro or IMU functions.

Summary of Analysis

These potential single point failures with supporting analysis were documented in Project waivers B19628, B19627, and B19629 by Astro in 1990. Analysis and flight data provided by Astro indicated that such failures are very rare. These waivers were approved by the Mars Observer Project.

The analysis that accompanied these waivers includes a part-failure rate analysis which determined that the probability of any one of these failures occurring is on the order of 10^{-8} , or 1 in 17,000 Mars Observer missions may exhibit an erratic line fault of this kind. Flight data totaling over one million hours on 15 other spacecraft that use equipment that may exhibit the same failures were examined; the data revealed no such failure, indicating that such failures are very rare.

Independent analysis by members of the Mars Observer Special Review Board indicates that erratic activity on the gyro channel and RXO backup select lines are not single-failure points and will not affect the system as described by Astro.

Conclusion

Analysis of erratic activity on the gyro channel and RXO backup select lines as determined by the Mars Observer Special Review Board will not seriously affect the system. However, if the IMU select line is erratic, the spacecraft would not function. This would match the observables. This failure is extremely unlikely and analysis indicates near impossibility.

Hypothesis C15 is Category B: credible, but very unlikely; uncertainties associated with the analysis require caution.

Q. Hardware Failure Preventing RPA Turn-On (RPA Control Failure; C16)

Hypothesis

A hardware failure is postulated to exist such that an RPA Beam On control relay coil in the SCU is permanently energized. At the same time, the filament of the associated RPA is off or was not powered long enough for its 208-s timer to have expired before the Beam On control relay coil became permanently energized. This failure could be situated anywhere from the relay coil driver back to the CIU where the commanded control pulse originates.

Causal Connection to Sequence

The pressurization sequence turned off the RPA-2 beam and both RPA filaments. After the pyro firing events, both the RPA-1 and RPA-2 beams were commanded off as part of the STRPAN software command macro used in the sequence. RPA-2 was then commanded on as part of STRPAN. This was expected to turn on the RPA-2 filament, wait 240 s, then turn on the RPA-2 beam.

Anomaly Scenario

The pressurization sequence commanded both RPA filaments off at 234/00:40:04 UTC ERT. The sequence should have commanded the RPA-2 filament back on with the STRPAN macro at 234/00:50:17 + 4 s. The RPA then requires a 208-s delay before it will respond to a Beam On command. Hence, the earliest the RPA would respond to a Beam On command is 234/00:50:17 + 4 s + 208 s, which is 234/00:53:49 UTC ERT. These times result in a window of 13 min 45 s when the RPA would not respond to a Beam On command if it occurred.

If the RPA received a spurious Beam On command as the result of a hardware failure in the SCU (or upstream), then it would not respond if that command occurred during the 13-min 45-s window described. Indeed, neither RPA would ever respond to a Beam On command again since the RPA requires a Beam Off to Beam On transition to respond and that transition can never occur again. The redundant-side RPA is similarly disabled since it is permanently latched in a Beam Off mode because of the SCU beam control interlock.

Relevant Information From Recovery Activity

Ground commands have been repeatedly sent using the SCP macro procedures in the telecom task of the SCP software. Individual SCP discrete commands have also been sent to turn on the filaments and beam voltages to the RPAs, bypassing the SCP macros.

Summary of Analysis

The RPA requires a commanded transition from the Beam Off to Beam On mode to respond with a true Beam On condition. This is the result of internal hardware logic built into the RPA. Additionally, that off-to-on transition must occur after the filament has been allowed to warm up for at least 208 s or else the commanded transition will be ignored and must be sent again.

This hypothesis seemingly depends on a failure occurring during the 13-min 45-s window described above, such that either of the two SCU Beam On relay coils is left permanently energized. During that window, neither RPA will respond to a Beam On command. More importantly, with either Beam On relay coil permanently energized *neither* RPA can ever receive an off-to-on transition again because of the interlock circuit design.

However, the real window when a failure could have occurred is actually much wider. RPA-2 had been on continuously since August 2 and both RPA filaments had been on continuously since April 9. A failure could have occurred to energize the RPA-2 Beam On relay coil any time since August 2 and would have been transparent to the Flight Team.

During the pressurization sequence, the downlink was observed to be out-of-lock at the expected time. However, the downlink would have gone out-of-lock in any case because the MOT exciter was commanded off as a result of the STRPAF command. Hence, a permanently energized relay coil holding the RPA-2 beam on would not be obvious in executing the sequence.

For a failure resulting in the RPA-1 relay being permanently energized, the window shortens to the 13-min 45-s duration described earlier plus 5 s. The earliest time this failure could have occurred is at the Beam Off command in the sequence. In this case, RPA-1 would have attempted to come on using the LGA. As before, the downlink would have disappeared on time because the exciter was turned off at the same time.

Five seconds after the exciter drive was removed, the sequence commanded both RPA filaments off. With the filament commanded off, an RPA will automatically revert to a Beam Off mode even if the Beam On command level is still set by the SCU. Turning on the filament later will not result in a downlink since an off-to-on transition is required from the SCU to initiate an RPA internal beam-on state. In this failure scenario, that transition can never occur for either RPA because of the interlock circuit. See Figure 7-10 for details of circuit configuration.

Conclusion

Analysis shows that the effect fundamental to this hypothesis is credible. This hypothesis is a possible potential cause of the actual Mars Observer anomaly. Hypothesis C16 is Category A: credible.

The categorization of this hypothesis is subject to change once the Mars Balloon Relay (MBR) experiment is concluded. That proposed experiment is discussed in Appendix U of this report. If that experiment results in detection of the MBR signal, then it is expected that this hypothesis will become the probable cause of the anomaly. If this experiment does not result in detection, the hypothesis becomes Category B: credible, but very unlikely.

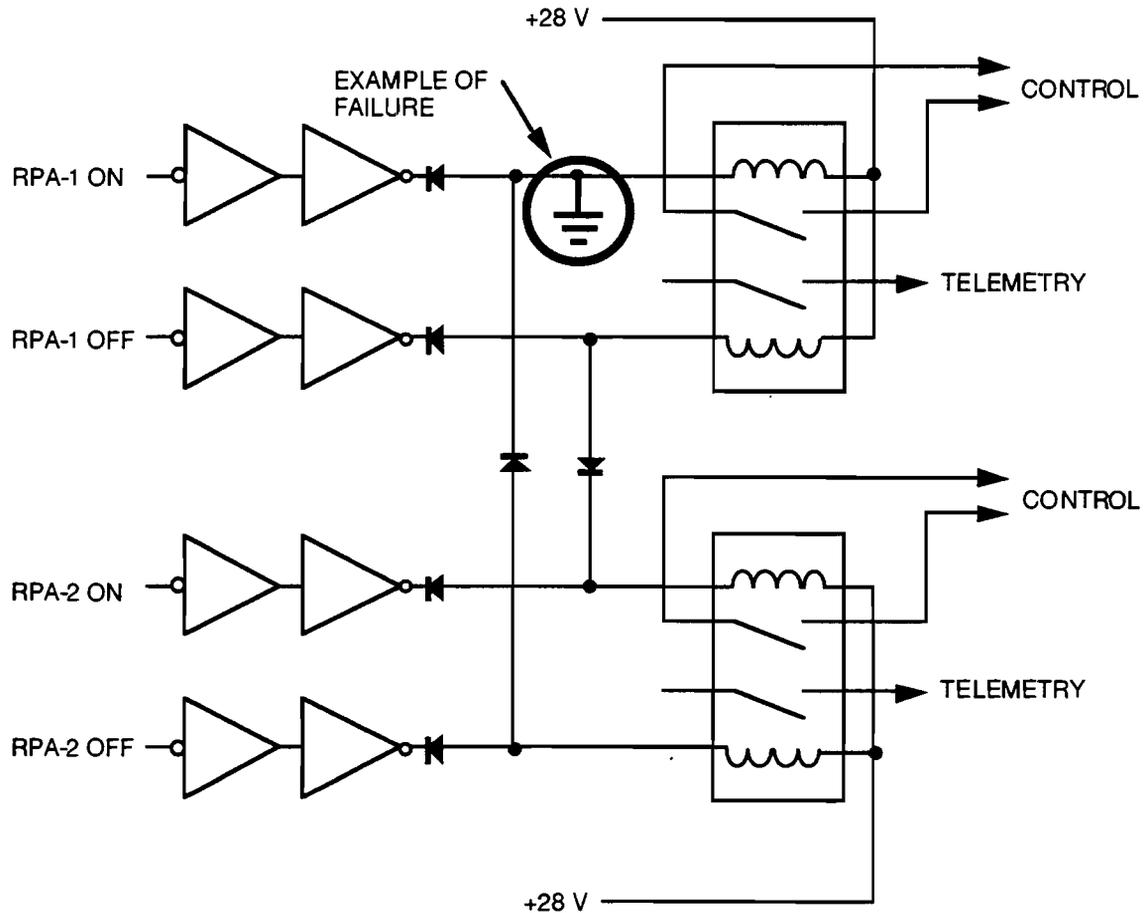


Figure 7-10. An example of a single-failure point in SCU that inhibits RPA Beam On.

R. System Response to Primary-Side Timing Loss (RXO Transistor Failure; S1)

Hypothesis

Side one RXO output (J1) is absent due to failure of a JANTXV2N3421 transistor or there is a failure further downstream in the primary-side timing chain.

Causal Connection to Sequence

Thermal stress or force resulting from pyro-valve firing, check-valve chatter, or reaction wheel vibration causes failure (via final "straw").

Anomaly Scenario

Total loss of SCP-1 function; no switch to backup clock divider, so SCP-2 does not have control of most functions; and effective attitude control is lost.

Relevant Information From Recovery Activity

CIU hardware Clock Divider 2 Select command was tried unsuccessfully.

Summary of Analysis

This anomaly scenario was verified by analysis and VTL testing performed by the JPL Flight Team. The results of these efforts were presented to the NASA and JPL Mars Observer Special Review Boards.⁷ Independent of and concurrent with the JPL Flight Team analysis activity, members of the Special Review Board performed an analysis of the RXO and determined that an SPF of the JANTXV2N3421 transistor contained in the RXO could lead to unanticipated and undesirable system effects, and possibly the loss of the Mars Observer spacecraft.

The origin of the cause for concern over potential failure of the JANTXV2N3421 transistor is given in Appendix S, along with a discussion of the transistor's likely failure mechanisms. It is shown by structural analysis that the most direct way to induce failure in a defective wire bond is by introducing forces through either thermal cycling the transistor or by self-heating, which will occur through power on/off cycles. It is pointed out, however, that degradation will occur as a function of time due to void formation. A bond that is initially weak from manufacturing can degrade with time to such an extent that it potentially can fail from the forces produced by the pyro shock or, in the worst case, can fail spontaneously. For additional information, refer to Appendix S.

⁷ R. Murphy, *Final Report of Spacecraft System Response Analysis for (Possible) Primary RXO +12 Volt Regulator Circuit Failure*, JPL Interoffice Memorandum SCT-93-639, Jet Propulsion Laboratory, Pasadena, California, October 19, 1993.

The postulated transistor failure causes loss of side 1 of the RXO and loss of CIU Clock Divider-1 (CD-1). CD-1 output is dedicated to SCP-1 and IMU-1. Likewise, CD-2 is dedicated to SCP-2 and IMU-2. Most other devices peripheral to the CIU can operate from either CD-1 or CD-2, whichever is selected. The system response to the loss of CD-1 is to switch from SCP-1 to SCP-2, but many peripherals, including the RWAs, would not be switched from the failed CD-1 to the working CD-2. SCP-1 cannot switch the peripherals to CD-2 because its ability to do so is impaired by not receiving necessary CD-1 timing inputs. SCP-2 does not switch the peripherals to CD-2 because its REDMAN CD fault-protection program receives all necessary CD-2 timing inputs, and thus does not detect the failure of CD-1. The failed CD-1 remains selected, resulting in corresponding loss of function to those spacecraft elements using CD-1 frequency inputs. These elements include EDF, XSU, SA GDE, HGA GDE, CIU ACE, PSE, CIX, DTRs, PDS, and MHSA. Note that CIU ACE includes the interface to the RWAs. The RPA would be turned on by SCP-2 as planned in the sequence, which continues to execute.

Because of CD-1 failure, and the inability to switch to CD-2, one of the four RWAs (randomly selected) is read by SCP-2 as having a zero speed. The other wheel speeds are never reread, and so the flight software retains these old values thereafter.

Four attitude time histories are possible; one for each possible RWA selection. These were simulated using the VTL, and are summarized below. The VTL simulations for the cases where the X, Z, or skew wheels are selected show that only one momentum-unloading maneuver occurs (at least within the first 24 hours), and then the spacecraft motion is bounded with the +Y-axis pointing in the neighborhood of the Sun. The downlink LGA-to-Earth angle remains less than 50°, so one could expect an LGA downlink as soon as the spacecraft enters Contingency Mode within 3 to 10 hours after the failure. The resulting attitude has a favorable solar aspect angle and will retain full spacecraft power.

If the Y RWA is selected, the situation is a bit more complicated. There will be no momentum unloading, and the attitude time history is such that the batteries would be completely depleted at 15 ± 1 hr after the failure. With this attitude-time history, a Power Alert would be expected to trip at 225 ± 15 min after the failure, but this alert depends on the EDF, which is disabled by the RXO failure. The Power Alert would therefore never take place. Contingency Mode entry occurs at about 200 min after the failure, due to gyro-scale factor errors leading to a Sun-Monitor-Ephemeris violation. At this time, the RPA beam is already on, having been turned back on by the pressurization sequence. The attitude-time history after Contingency Mode entry is favorable for LGA downlink and the carrier would be expected to be detected almost continuously thereafter. Since the LGA-to-Earth angle varies between 0° and 100°, there would be some brief gaps in continuity (Figure 7-11).

Several other facts are not required to arrive at this conclusion but serve to make the conclusion robust to changes in understanding the system response:

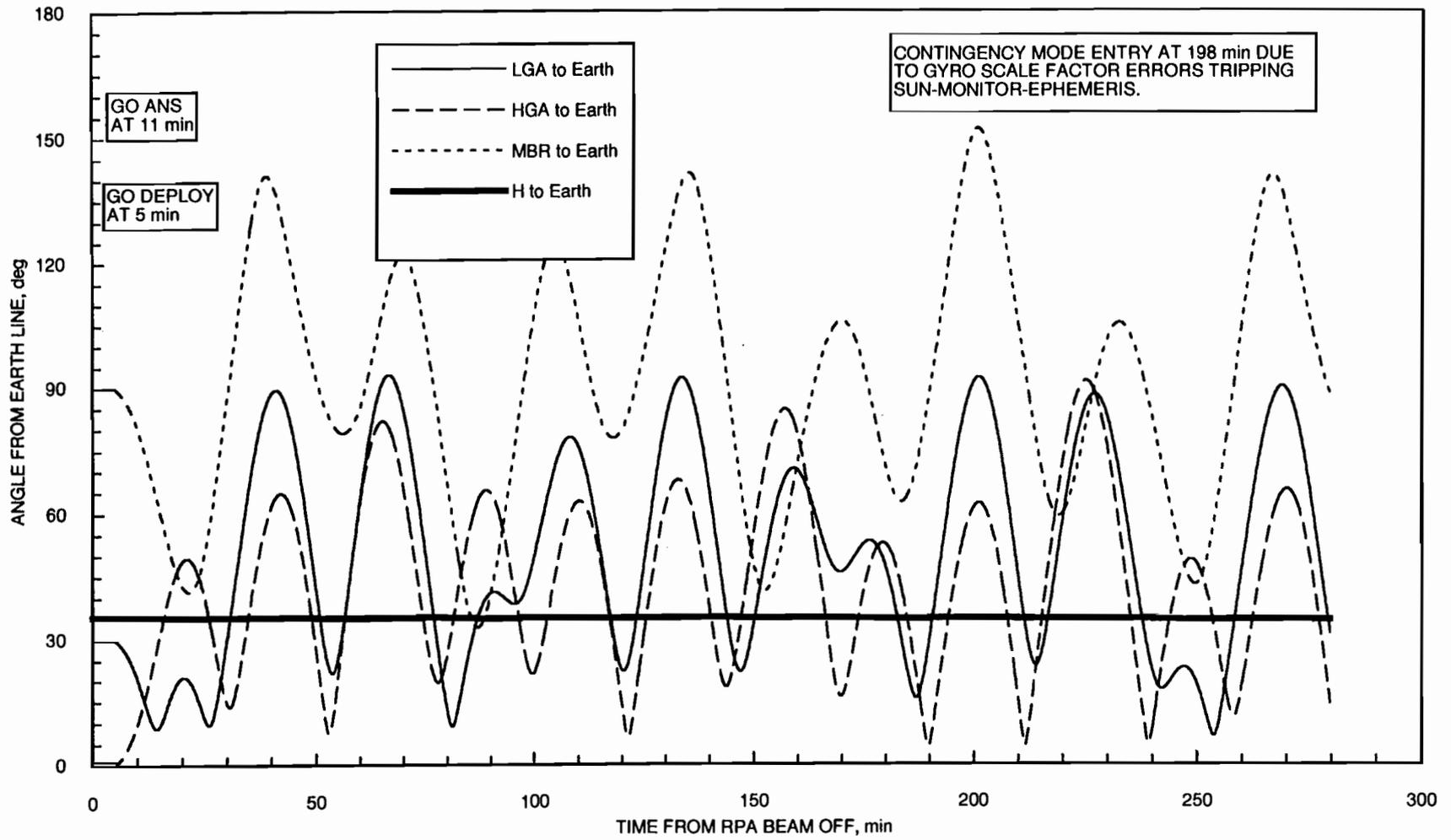


Figure 7-11. LGA boresight deviation from the Earth direction.

- (1) The backup pressurization block was 10.0 hr after the nominal pressurization block. This block included an RPA Beam-On sequence command which would have turned the RPA on.
- (2) The first six RPA Beam-On recovery commands would have arrived at the spacecraft between 5 and 6 hr after the failure. The attitude time history is such that almost all of these commands would have been received.
- (3) Even if Contingency Mode is entered due to a power alert, the spacecraft will accept an RPA Beam-On sequence command after 117 min have elapsed.

It should be noted that the RXO failure was by far the most complex case for VTL to simulate. This simulation required engineers to learn just how the system would respond to the failure and attempt to mimic that response by modifying the hardware or software simulation. Achieving results that were not inconsistent with known behavior took many iterations, including a number of false starts. Due to the complexity of this failure case and the fact that there is no way to validate that VTL simulation is totally accurate, it is not possible to claim that the VTL simulations disprove this possible cause. What one can say is that analysis and simulation both indicate that due to the spacecraft dynamic state at the beginning of the Deploy Mode sequence, if the RXO had failed such that side one of the timing chain was lost, one would expect to detect the LGA carrier at Earth within hours of the start of Deploy Mode.

The inability to command the spacecraft to Contingency Mode and obtain the expected downlink response appears to be inconsistent with the analytically predicted spacecraft state. Failure to respond to ground commanding may only be correlated with the expected spacecraft state if the attitude were sufficiently anomalous to preclude any HGA or LGA coverage. However, VTL simulations show that LGA pointing angles and spin rates will be favorable enough to detect a signal or transmit a command to the spacecraft.

Conclusion

The JANTXV2N3421 transistor is a single-failure point in the RXO. Reliability and structural analysis of the transistor cannot eliminate a wire bond failure that produces failure of the RXO voltage regulator.

The loss of the primary-side RXO power supply (due to the transistor failure or otherwise) has system consequences that are severe; these were not widely known prior to the anomaly investigation by the Project.

Attitude control analysis and simulation indicate that the LGA carrier would be expected to be observed at Earth within hours of the loss-of-signal anomaly. That it was not indicates that this probable cause is very unlikely.

Hypothesis S1 is Category B: credible, but very unlikely; uncertainties associated with the analysis require caution.

S. Primary Power Failure (Power Loss; S2)

Hypothesis

Primary bus high-side short to chassis resulting in loss of all spacecraft power.

Causal Connection to Sequence

Thermal cycling due to current surges during prelaunch testing and flight mission and less probably shock occurring during pyro valve activation during the pressurization sequence.

Anomaly Description

Primary power high-side short to chassis occurs in the Power Supply Electronics (PSE) at the cathode of one or more of the main bus power diodes during turn-off and subsequent turn-on of the RPA following the pressurization sequence. The power bus is pulled down out of regulation below the required minimum input to the RPA of 24.5 Vdc. The load change was about 120 W (4.3 A), which corresponds to a diode mount ΔT of about 4 °C. This fault shorts the available 30 A from the Solar Array and more than 30 A from the battery source through the BVR until the battery energy is exhausted.

Relevant Information From Recovery Activity

This hypothetical failure fits the observables exactly—no evidence of RF carrier, fault protection recovery, or receipt and execution of corrective commands from the ground.

Summary of Analysis

The primary system power return point for this spacecraft is tied directly to chassis with no isolation. This design is vulnerable to a catastrophic high-side short to chassis within the power control electronics (PCE). NOAA-I failed on August 21, 1993, because the Solar Array output was shorted to chassis in the Battery Charger Assembly (BCA) when isolation between the electronics heat-sink (at Solar Array potential) and the radiator failed. This isolation consists of about 10 mils of polyester mesh impregnated with Stycast. An over-long mounting screw, connecting a relay, eventually pierced the mesh (under the influence of thermal cycling) and connected the heat-sink to the radiator, which is chassis and therefore also a 28-V return.

This resulted in total loss of Solar Array power, but not battery power, because it is isolated from this overload by the Solar Array isolation diodes in the PSE. The three batteries provided about 4 hours of additional spacecraft operation and telemetry clearly provided the basis for identifying the fault.

This fault, had it occurred on Mars Observer, would not have provided the Mars Observer observables. The spacecraft would have operated correctly and telemetry would have been received as long as the battery energy sufficed (~3–4 hours).

The fault on Mars Observer could have been due to a similar (but not identical) high-side short circuit in the PSE instead of the BCA.

To satisfy the Mars Observer observables, both Solar Array and battery power sources would have to be eliminated. These sources are joined within the PSE; the Solar Array diode coupled, directly to the 28-V bus, and the batteries, diode coupled, through the BVR to the bus (Figure 7-12).

There are more than 11 locations within the PSE that are potential sites for this fault. More than seven have experienced 15 thermal cycles since launch. Total thermal cycles for this unit are estimated to be 420 ± 75 cycles.

Isolation to chassis for these diode components is by an insulating Sil-Pad under the stud-end (cathode) and a fiberglass shoulder bushing inserted into the through-hole of the heat-sink and retained by the washer and nut combination. The Sil-Pad is a "sandwich," 6 to 7 mils thick, consisting of 1 mil of Kapton and the remaining two elements of silicone rubber.

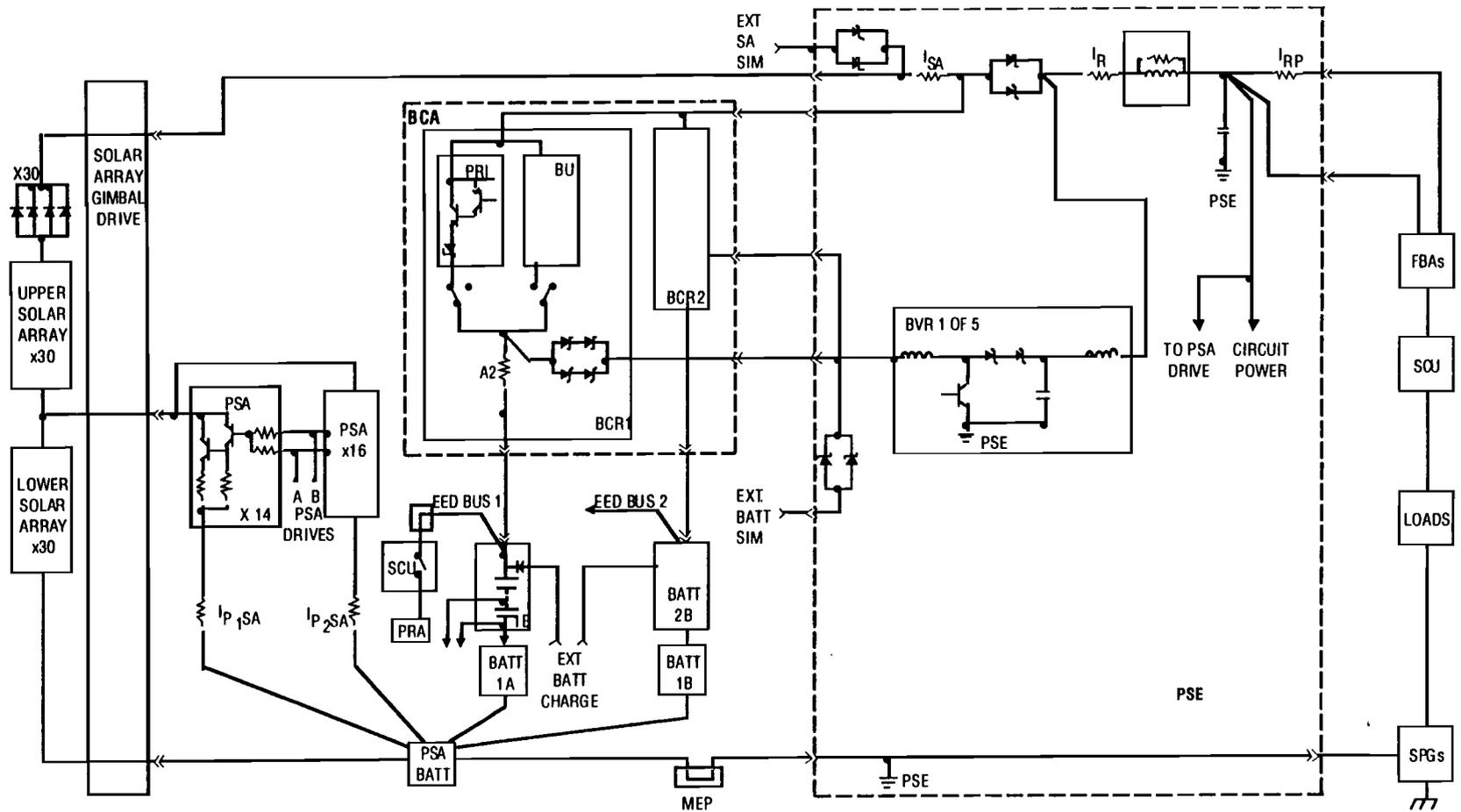
Historically, all insulating pads have been susceptible to damage by over-torquing. Also, the dimensions of the bushing are critical; too long and the diode base is not correctly seated for proper thermal conductivity, too short and the junction of the stud and diode base is unprotected from burrs or debris in the heat-sink through the hole.

In conducting this assessment, the following fault candidates have been eliminated as being not credible:

- (1) Line-to-line shorts
- (2) Fused load shorts
- (3) Filters connected line-to-line and line-to-chassis
- (4) Open lines
- (5) Shorts within the PSE that would eliminate redundant functions, but are functionally isolated from the primary power bus
- (6) All component shorts that the batteries would fuse open
- (7) Multiple failures

Anomaly Scenario

During this investigation, at least seven credible candidates were found that could have caused the Mars Observer anomaly. In this anomaly, the spacecraft would not only be lost, but lost very rapidly. This requires a short to chassis and the subsequent overload of both the Solar Array and battery sources so that the spacecraft primary power regulated bus is held below 24.5 V. The possible fault sites in the PSE can explain all the observables.



* ONE PSA AND ONE SET OF DIODES FOR EACH OF 30 SOLAR ARRAY STRINGS.

Figure 7-12. Unfused power schematic.

Conclusion

This potential cause does not depend on complex modeling and represents a design weakness, but this practice has been universally accepted as sound and cost-effective by the commercial aerospace industry. Even considering the recent NOAA-I failure, the industry experience with the primary power return tied directly to chassis has historically been good, indicating that the probability of failure from this design approach is low. Hypothesis S2 is Category A: credible.

T. Erratic RXO Output (S3)

Hypothesis

The timing signals at both RXO output ports are erratic, preventing the proper functioning of some or all spacecraft equipment that depends on the signals.

Causal Connection to Sequence

The RXO normally produces two identical outputs that are highly stable 5.12-MHz square waves used extensively in the spacecraft as a time base. The RXO is internally redundant and can autonomously switch between primary and backup oscillators to generate the two outputs.

In this scenario, the RXO erratically switches between the primary and backup oscillators such that the resulting two outputs no longer have the spectral purity needed by dependent spacecraft equipment. An erratic RXO-CIU interface can disrupt C&DH timing and result in a total loss of effective spacecraft control functions.

The cause of the RXO degradation is postulated as an intermittent part failure or part-induced noise into the control circuitry of the RXO. The noise causes the RXO to first select the primary side and then select the backup side. Such switching could occur at a rapid (many times per second) rate.

This type of failure was stipulated as the cause behind the loss of NOAA-E in 1984. The erratic RXO outputs caused the inertial reference unit to operate abnormally and the spacecraft tumbled. However, the underlying mechanism for that failure was postulated as noise on the spacecraft power bus or noise in the failure detection circuitry of the RXO. Susceptibility to such causes has been reduced in the Mars Observer RXO because of design changes subsequent to the NOAA-E loss.

Relevant Information From Recovery Activity

Ground commands to select the backup side of the RXO were sent during the recovery activities. However, these commands might not have had any effect under the conditions of this hypothesis.

Summary of Analysis

This potential single-point failure with supporting analysis was documented in waiver B19627 by Astro in 1990. Analysis and flight data indicated that this failure is very rare. The waiver was approved by the Mars Observer Project Office.

The RXO additionally incorporates hysteresis for the primary–backup side selection circuit. The RXO Select line drives a normally off Darlington switch with an output driving CD4019 logic input that has additional hysteresis.

Conclusion

The RXO susceptibility to this type of failure has been substantially reduced since the NOAA-E failure. This hypothesis scenario is almost impossible, but the complexities and uncertainties associated with the modeling and analysis require caution. Hypothesis S3 is Category B: credible, but very unlikely.

U. RPA (TWTA) Cathode Heater Support Failure (RPA Cathode Support Failure; S4)

Hypothesis

During the firing of PV-5 and PV-7 for MOI pressurization, shock waves propagate from the pyro valves located on the nadir panel, through the space-side bulkhead, and reach the two traveling wave tube amplifiers (TWTAs) located on the space equipment panel. Both cathode support tubes in the TWTAs fail structurally under shock loading.

Consistency With Observables

A severe structural failure of the cathode support tube (such as a total separation of the tube from its support base) can cause the dispenser cathode to be nonfunctional. This can, in turn, prevent the TWTAs from properly functioning and can lead to a total loss of downlink capability of the spacecraft.

Summary of Analysis

The TWTA dispenser cathode support tube is formed by rolling a 0.0127-mm (0.0005-in.)-thick molyrhenium sheet into a circular tube with a seam in the longitudinal direction. The tube supports the cathode at one end and is cantilevered from the Kovar support at the other. The base of the tube is confined in a cylindrical socket and attached to the support with 12 spot welds located on the circumference. The kernel of the welds is about 0.0064 mm (0.00025 in.) in diameter. A structural analysis was performed, based on available design data, to determine the load-carrying capability of the tube (Appendix Q). Analysis results indicate that the inertial force produced by the acceleration of the dispenser cathode results in exceedingly high stresses at the base of the cathode support tube. Several modes of structural failure are possible, including breakage of the support tube at the seam, buckling of the tube and subsequent breakage, and tear-out of the 12 spot welds. If the direction of acceleration is along the axis of the TWTAs, tear-out of the spot welds will occur at about 670 g's. If the direction of acceleration is perpendicular to the tube axis, acceleration in the range of 70 to 140 g's could cause tube failure, depending on the orientation of the seam with respect to the direction of acceleration. In addition, it is possible that prior pyro-shock events could have damaged both of the tubes, resulting in lower failure loads during MOI pressurization.

Conclusion

Hypothesis S4 is Category B: credible, but very unlikely.

The probability of occurrence of this hypothesis is also determined by the shock levels that the TWTAs are subjected to during MOI pressurization. A direct shock path along a bulkhead of the Mars Observer bus exists between the pyro valves and the equipment panel on which the TWTAs are located. At present, a pyro firing test with the Mars Observer spare bus is planned (see Appendix G for details of the planned test). The categorization of this hypothesis may change when the test results are available.

The categorization of this hypothesis is also subject to change once the Mars Balloon Relay (MBR) experiment is concluded. That proposed experiment is discussed in Appendix U of this report. The results of that experiment may provide sufficient information to allow adjustment of the category ranking for this hypothesis.

V. Gyro Spin Motor Short (S5)

Hypothesis

A gyro spin motor shorts in the IMU. This known failure mode was to have been covered by a fault protection algorithm. However, gyro noise modeling problems caused difficulty in ground testing and the fault protection was disabled before launch. This absence of fault protection was not discovered until a few days before the anomaly; at that time, the risk of enabling the untried algorithm was deemed more risky to the critical MOI and pre-MOI sequences than leaving it disabled.

Causal Connection to Sequence

Pyro shock or current provides some final "straw" to cause the short; no particularly good candidates have been found.

Anomaly Scenario

When the gyro spin motor shorts, all rotors start to spin down, and scale factor errors grow. Pulse rebalance becomes more frequent as the torquers attempt to keep the rotors centered. Eventually, all rotor spin stops and each output axis is saturated. Both positive and negative saturation are possible. Both axes from all three gyros are saturated. The multiaxis saturation will disable future momentum unloading. AACS is still in Deploy Control Mode.

IMU redundancy management for this fault is not enabled and the remaining fault protection will be ineffective. The result is that the frozen gyro output is meaningless, but still accepted by AACS control algorithms as correct.

The Go ANS command was issued in the sequence. Sun-Monitor-Ephemeris violation should occur within 1 to 2 s of entry into ANS Mode, and Contingency Mode is entered. The STRPAN RPA Beam-On macro started by the sequence is canceled by Contingency Mode entry. The RPA beam will stay off until commanded on via a recovery command or by the backup pressurization sequence.

Upon entry to Contingency Mode (Sun-Comm-Power attitude control state), RWA control is enabled and applies full torque to the RWAs to attempt to remove the measured errors (full torque is requested for any attitude error of 2° or any rate error of 1 mrad/s).

The wheels reach maximum speed less than 7 min after RWA control is enabled, but the passive wheel test is disabled for high-speed wheels. The final state is that all three active wheels are spinning at maximum speed and no wheel unloading can occur. The spacecraft will be (counter)rotating at this time. Analysis shows that the batteries would lose some charge on each rotation of the spacecraft, finally losing spacecraft power between 05:02 and 07:17 SCET of DOY 93-234. Note that the first RPA Beam On commands arrive at the spacecraft starting at 05:29 SCET.

Relevant Information From Recovery Activity

The STRPAN (RPA Beam On) commands in Table 7-1 were the first commands sent in the first few hours after the loss of signal.

Summary of Analysis

The postulated failure, though theoretically possible, has never been seen on such motors. Four variants of this scenario were simulated on VTL. For each case, the LGA–Earth angle varies widely with time, but the duration of a typical uplink pass for either LGA is the important point. This duration is about 2 min, so about 30 percent of the time, the LGA–Earth line will cross 90° while a 40-s duration RPA Beam On command is arriving at the spacecraft. In this case, the command will not get in. In the other 70 percent of the cases, the command will get in. Playing the analysis of this 70-percent chance of getting each of the six commands in against the probability of power loss before a given time shows that there would be over a 95-percent chance of briefly (from several minutes to just under two hours) receiving a downlink in response to the sequence of RPA Beam On commands. Since no downlink was detected, this scenario is unlikely to be the cause of the Mars Observer loss of signal. (Detailed simulation results are shown in Appendix R.)

Conclusion

Analysis shows that this hypothesis scenario is almost impossible. This hypothesis is not a credible potential cause of the actual Mars Observer anomaly, unless there is an error or oversight in the modeling or analysis. Hypothesis S5 is Category B: credible, but very unlikely.

Table 7-1. First radiated recovery commands.

Date and time radiated	Time of arrival at spacecraft	Command
DOY 93-234/05:10	05:29	RPA Beam On (at 7.8)
DOY 93-234/05:23	05:42	RPA Beam On (at 7.8)
DOY 93-234/05:35	05:54	RPA Beam On (at 7.8)
DOY 93-234/05:45	06:04	RPA Beam On (at 7.8)
DOY 93-234/05:53	06:12	RPA Beam On (at 7.8)
DOY 93-234/06:05	06:24	RPA Beam On (at 7.8)

W. Sun Sensor Head #4 Failure (S6)

Hypothesis

Assume that Sun sensor head #4 fails in such a way that the Sun can no longer be detected. Furthermore, assume that another Sun sensor has its thresholds set wrong such that Mars is accepted as the Sun if the real Sun is not within any of the remaining 4π SS FOVs.

Causal Connection to Sequence

Pyro shock or current provides the final “straw” to produce an unspecified Sun sensor failure.

Anomaly Scenario

Sun sensor head #4, which sees the Sun during Earth- or Sun-pointed array normal spin fails, so the true Sun is not seen. The 4π SS thresholds are set so that Mars cannot be mistaken for the Sun. If the thresholds are correct, the spacecraft will continue gyro/star-scanner-based pointing until the Sun has been missing an hour. It will then swap to the backup Sun sensor, which would allow normal operations to resume.

If the 4π SS thresholds are incorrect (in addition to a 4π SS head #4 failure), Mars might be mistaken for the Sun. Since Mars is approximately 90° from the last known Sun location, Sun sensor fault protection (enabled in Deploy Control Mode) will wait for the new direction to be consistent for 15 min before Mars will be declared the Sun and Contingency Mode entered. It will take less than 7 min to turn 90° to Mars. During that turn, one of the other Sun sensors will see the true Sun, which will be brighter than Mars, and start a new 15-min clock. The +Y-axis will be pointing at Mars for more than 8 min before the clock runs out and a turn to the Sun is begun. The spacecraft will then continue to oscillate back and forth between the Sun and Mars.

HGA communications would have been available for 5 min after Beam On before the first Sun sensor 15-min time-out. LGA communications would have been available at least twice per hour for periods of at least 8 min each thereafter.

Conclusion

Analysis shows that this hypothesis scenario is not credible, and the complexities and uncertainties associated with the modeling are not a concern. This hypothesis is not a credible potential cause of the actual Mars Observer anomaly. Hypothesis S6 is therefore in Category C: not credible.

X. RWA Overspeed (S7)

Hypothesis

Unspecified RWA electronics or CIU RWA interface failure leading to full torque commands to one of the wheels.

Causal Connection to Sequence

For the skew wheel, the skew RWA had been off, and then was turned on by sequence. For other wheels, the pyro shock or current provide the final “straw” to produce an unspecified reaction wheel failure.

Anomaly Scenario

There are four scenarios, one for each of the four wheels. The skew wheel case is unique in that the sequence will turn that wheel off automatically after 6 min. For the other wheels, wheels X, Y or Z spin up in Deploy Control Mode, causing about a $1^\circ/\text{s}$ spacecraft angular velocity (see Table 5-8). RWA REDMAN is disabled in Deploy Control Mode and is also disabled for wheel speeds in excess of 6000 rpm. The switch out of Deploy Control Mode does not turn off this wheel, and REDMAN will not do anything about it. This results in only two-axis RWA control.

The four cases are discussed in Appendix R. In each case, simulation on VTL shows that LGA communication should have been established within 10 hours.

Conclusion

Analysis shows that this hypothesis scenario is not credible, and the complexities and uncertainties associated with the modeling are not a concern. This hypothesis is not a credible potential cause of the actual Mars Observer anomaly. Hypothesis S7 is Category C: not credible.

Y. Meteoroid Impact (N1)

Hypothesis

A meteoroid impacts any of the pressurized tanks on the Propulsion System during the unobserved 14-min window; this meteoroid is large enough to cause the tank to burst, which in turn destroys the spacecraft functionality. This is not related to spacecraft sequence activity.

Conclusion

This hypothesis requires a minimum meteoroid size (as a function of velocity), which in turn can be compared with the mission meteoroid fluence to calculate a probability of impact in the exposed area. This procedure has been implemented (Appendix I) for an assumed exposed tank area of 2.45 m² to calculate an impact probability of about 3×10^{-7} over the 14-min window. This analysis has conservative assumptions and so is an upper bound on the probability. Hypothesis N1 is Category B: credible, but very unlikely.

Z. DSN Inability To Detect Existing Downlink (DSN Detection Problems; N3)

Hypothesis

Improper DSN configuration or procedures may prevent the detection of an existing downlink signal from the Mars Observer spacecraft.

Causal Connection to Sequence

None.

Anomaly Scenario

The spacecraft may have successfully initiated a downlink when the sequence executed the RPA Beam On command. However, the DSN is postulated to have been unable to detect the presence of the downlink because of misconfiguration or improper operation of equipment.

Relevant Information From Recovery Activity

The initial anomaly occurred during tracking by DSS 15 at Goldstone. Within the first hour, the 70-m antenna at Canberra was brought into the search. Subsequently, all 34-m high-efficiency front-end (HEF) and 70-m antennas have been utilized with updated predicts for pointing and tuning. There has been no hint of a signal received since the anomaly.

Summary of Analysis

DSS 15 had been routinely tracking Mars Observer for many months before the anomaly. During the pressurization sequence, DSS 15 correctly executed the sequence of ground events specified by the Project. Predict sets successfully used during the early part of the sequence were employed at the time of expected downlink reinitiation.

When the anomaly was noted, DSS 15 initiated tuning on both channels 16 and 20 and began a broad spectrum search with the SSI within 7 min. Within an hour, DSS 43 (70-m, Australia) was brought up and also tuned for channels 16 and 20 using the SSI for the entire pass. After 1 h 11 min, DSS 15 went off point and checked receiving capability using a test signal. After ascertaining that all was okay, DSS 15 returned to point and searched one way on channel 16. The 70-m subnet and 34-m HEF subnet searched continuously through August 23.

In the following week, additional detection capability was provided using the High-Resolution Microwave Survey (HRMS) spectrum analyzer employing joint operations of DSS 15 and DSS 13 during Goldstone view periods. At the same time the Experimental Tone Tracker was employed at both Goldstone and Canberra.

Throughout the entire period, the DSN continued to routinely track other spacecraft during scheduled periods. That such tracking was successful without significant anomalies attributable to the DSN confirms the basic operability of the DSN and integrity of equipment and procedures at the three complexes.

In view of the intensive use of six different DSN stations, the updating of predicts since the anomaly, and the successful demonstration of DSN operability by tracking other spacecraft, this scenario is not considered credible. Either the Mars Observer downlink was not present or was sufficiently weak or of short enough duration to escape detection even with the use of the most sensitive equipment of the DSN.

Conclusion

Analysis shows that this hypothesis scenario is not credible, and the complexities and uncertainties associated with the modeling are not a concern. Hypothesis N3 is Category C: not credible.

AA. Multiple Failures (N4)

Hypothesis

Loss of mission by failure of two units was recognized as a failure mode that cannot be practically avoided (on all other projects as well as Mars Observer); the dual failures of this type that result in loss of a scenario-critical function are given in Table 7-2.

Table 7-2. Dual-unit failures creating observed anomaly.

Failed units	Last redundant unit observation	Exceptions
CIU/CIX-1 + CIU/CIX-2	$T_0 - 11$ months	None
IMU-1 + IMU-2	$T_0 - 11$ months	None
SCU-1 + SCU-2	$T_0 - 20$ days	None
RPA-2 + RPA-1	$T_0 - 20$ days	None
MOT-2 + MOT-1	$T_0 - 20$ days	None
SCP-1 + SCP-2	$T_0 - 0$ days	In-control function
SCP-2 + RXO-1 power supply	$T_0 - 0$ days	None
SCP-1 + RXO-2 power supply	$T_0 - 0$ days	RXO-2 amplitude
RXO-1 + RXO-2	$T_0 - 0$ days	RXO-2 amplitude

T_0 is the time of the anomaly.
 Functions last verified in prelaunch tests include CIU/CIX2 I/O buses, SCP-2 in-control functionality, and RXO-2 amplitude.
 Only the downlink elements in the MOT are scenario critical in this potential cause.
 SCU-2/MOT-2/RPA-2 was used at Contingency Mode entry at $T_0 - 20$ days.
 Loss of hardware switching capability is modeled as a second unit failure; loss of software switching capability is modeled in Potential Cause C6.
 Failures in the JANTXV2N3421 transistor in the RXO are modeled in Potential Cause S1.

It was recognized that complex, multiple, simultaneous failures that cannot be managed by onboard fault protection are possible, and there is no project requirement to provide this protection (a situation typical of most projects, and not unsound because these scenarios are extremely unlikely and very difficult to deal with). These scenarios were not studied during development and not investigated by this Special Review Board, but are known to be considerably more unlikely than multiple failures of the type given in Table 7-3, and so are ignored in the probability estimation.

Consistency With Observables

This hypothesis scenario must match the observed anomaly scenario: no known failure of any unit, followed by loss of scenario-critical function in 14 min. The calculations given here encompass this multiple failures scenario when it occurs at any time after launch.

Conclusion

An estimate of unit failure rates is required for the analysis; these values can be analyzed (albeit with uncertainty and some controversy), but this analysis has not been done on this Project and is not worth the effort for this purpose because approximations will serve here. The failure rates are conventionally quoted in failures in 10^9 hours or FITS (100 FITS is 100 failures in 10^9 hours). The FIT values at the unit level in Table 7-3 are rough estimates based on experience that provide the correct order of magnitude for the probability estimate.

Table 7-3. Unit FIT estimates.

Unit	FITS (operating)	FITS (dormant)
SCP	3000	300
CIX/CIU	1000	100
SCU	1000	100
MOT	1000	100
RPA	1000	100
RXO	100	10
IMU	100	10

The units whose redundant elements are unmonitored (the CIU/CIX and IMU) have the highest probability of matching the observed failure scenario. The failure probability is easily calculated for these units; it is merely the failure of both primary and redundant units when the redundant unit fails first. This is approximately $(0.01)(0.001)/2 = 5 \times 10^{-6}$ for the CIU/CIX and approximately 5×10^{-6} for the IMU.

The calculation of the failure probability for the SCU units with the redundant unit intermittently monitored is very complex; the complexity arises from the variability of monitoring the redundant unit (the values at the time of the actual anomaly were happenstance). Fortunately, a simplistic calculation is adequate here; the simplified model will assume that the duration from launch is 1 year and that the redundant units are powered continuously and monitored every 0.2 year; then the model for failure within any 0.2-year time frame that matches the observed failure scenario is similar to the model used above. The probability of the failure of both the primary and redundant units when the redundant unit fails first is approximately $(0.01)(0.2)(0.001)(0.2)/2 = 2 \times 10^{-7}$. Since there are five of the 0.2-year time periods in the year, the total failure probability that matches the scenario over the one year period is about 10^{-6} .

A similar analysis for the two RF unit pairs (the MOT and RPA) gives similar failure probability (10^{-6} for each pair).

The SCPs are continuously powered and are monitored whenever a downlink is established (nominally one pass a day); a similar analysis for the SCP dual failure gives a failure probability of about 10^{-6} , with the other multiple failure scenarios involving the lower FIT RXO having substantially lower probabilities.

Combination of the above probabilities leads to the assessment that the overall failure probability is 10^{-5} over the 11-month flight time, and in the 14-min window is about 10^{-9} . Note that this quantification does not consider the possibility of an unresolved generic part weakness, which could raise the failure probability dramatically. Hypothesis N4 is Category B: credible, but very unlikely.

The SCPs are continuously powered and are monitored whenever a downlink is established (nominally one pass a day); a similar analysis for the SCP dual failure gives a failure probability of about 10^{-6} , with the other multiple failure scenarios involving the lower FIT RXO having substantially lower probabilities.

Combination of the above probabilities leads to the assessment that the overall failure probability is 10^{-5} over the 11-month flight time, and in the 14-min window is about 10^{-9} . Note that this quantification does not consider the possibility of an unresolved generic part weakness, which could raise the failure probability dramatically. Hypothesis N4 is Category B: credible, but very unlikely.

BB. SEE-Created Problem (N6)

Hypothesis

This hypothesis deals with the effect of one or more upsets in spacecraft logic, data registers, or processor RAM caused by one or more energetic particles. Chapter V.J and Appendix J contain information on the susceptibility of the spacecraft parts to SEEs. The conclusions from that information are that upsets in RAM are highly likely (they were observed many times in flight) and that catastrophic failure of power transistors in the Power Subsystem is not considered possible at the actual operating voltages. For this reason, the scenarios described below deal with effects on RAM contents. Although not identified as susceptible, SEUs in data registers used by the SCP are included for completeness. (It may be noted that an SEE-induced latch-up of critical control logic results in the same effects as noted in the discussion of Hypothesis C5.)

As stated above, upsets can occur directly in the RAM memory, to data, or to instructions in external registers. It should be noted that each word in RAM memory is protected by an error detection and correction (EDAC) code, which corrects single bits in error and detects double-bit errors. (More than two bits in error may result in an erroneous correction.) Therefore, the effect of the hypothesized upset(s) would be a word in memory that is corrupted such that it is not corrected or corrected erroneously, or a word about to be stored in memory (data from an uplink load or a spacecraft sensor) is corrupted before the EDAC code bits are added. The result is the same: an erroneous instruction or data in the SCP-1 memory.

Consistency With Observables

One possible scenario is that if two errors are detected in one word that is about to be processed, SCP-1 detects a machine fault, and control is transferred to SCP-2. This does not result in a failure of the downlink to reappear, because the planned sequence is executed by SCP-2.

In another scenario, there are more than two errors in a word and the corrupted word is not detected. This causes a runaway program execution (RPE). This RPE may or may not include spurious external commands. The case where external commands are involved is described as example D for Hypothesis C6, SCP Software Problem, and can match the observables. If it does not include spurious external commands, it would usually result in a lack of a MEOK signal and control would be transferred to SCP-2 with the same result as above. If MEOK is not withheld, or the program goes into a loop that contains generation of MEOK, then more serious problems arise that would match the initial lack of a downlink signal, but would not be consistent with the failure of ground recovery actions to regain the downlink, unless ground commandability is precluded due to attitude and/or rate problems. This is described also within the discussion of Hypothesis C6, which deals with a design-error-induced SCP software problem.

Yet another scenario would result in SCP-1 issuing an erroneous command (in place of an expected sequence command). This would match the initial symptoms if the missing command was the RPA Beam On command. However, subsequent ground commanding would have immediately regained the downlink. An exception to this would be if the erroneous command caused gross external actions leading to a bad spacecraft attitude, high rates, or physical destruction. However, no single command can be identified that would do this.

Conclusion

The probability that these scenarios could be caused by SEU(s) is vanishingly small for the following reasons. There is a software memory scrub operation that cycles through all of memory every 6 s, whereas the observed SEU rate has been only one per memory per 60 hours. For a word in memory to be corrupted and not corrected or detected, at least 3 bits must be upset. One upset would be corrected, and two upsets in a given word would cause a machine fault when the word is processed, which would cause MEOK to be withheld, with a resultant swap to the backup SCP and continuation of the sequence. If the backup SCP also had two or more errors, the sequence would not necessarily be continued, but multiple errors in one word of each SCP is nearly impossible.

A data word corruption taking place in an input register would have only a minor transient effect if that data were coming from a spacecraft sensor, because the next word would be good and would almost immediately remove the effect of the erroneous data. If the data were coming in from an uplink commanding session, then the error would have been caught in a subsequent memory readout. Program patches have been read out after loading. Also, the pressurization block sequence was read out after loading. Hypothesis N6 is Category B: credible, but very unlikely.

CC. +10-Volt Interface Power Failure (N7)

Hypothesis

Total loss of computational control capability.

Causal Connection to Sequence

Possible noncausally connected circuit short behavior related to an internal part failure or an electromagnetic spike, as in Hypothesis C5.

Anomaly Scenario

Two anomaly scenarios are discussed herein. First, a failure which totally disables the +10-V spacecraft interface power bus and, second, a failure which disables the +10-V spacecraft interface power to critical control circuits in the CIU. Both failures have the same effect, which is to cause total loss of computational control.

Relevant Information From Recovery Activity

There is no command available to recover from either of the postulated failures.

Summary of Analysis

The +10-V spacecraft interface power bus is generated by diode “or”ing the outputs of two redundant electric power converters (EPCs) within the CIU. This power bus is distributed spacecraft-wide to power the control and logic interface signals between the CIU and user subsystems. The interface circuits to 22 components (boxes) are powered in this manner, including the RXO, RWAs, SCUs, IMU, SSEs, and circuits internal to the CIU and CIX.

A standard interface design is used by power bus users which limits the amount of current that each user can draw to about 50 mA. This is a protective feature to help mitigate against a single failure from disabling the entire power bus, since this failure would be mission catastrophic. Analysis shows that possible failures that could totally disable the 10-V power bus include: (1) a gross harness failure, (2) failure of both CIU EPCs, (3) an unidentified design, fabrication, or materials flaw, (4) unidentified conductive contamination (such as a solder ball or wire) which shorts a key power bus distribution circuit within the CIU (e.g., backplane), or (5) multiple part failures (i.e., resistor and filter capacitor shorts) in user interface circuits which excessively loads the power bus and takes it down. The CIU EPC will not supply enough current to clear shorts. Although these potential failures are possible and would meet the observables, they are considered to be very unlikely.

The +10-V spacecraft power bus is also extensively used to power functions within the CIU and CIX. One of those functions powered within the CIU is the A-11 board which contains the nonredundant and critical circuits for SCP in control, I/O bus

crossed/not crossed, I/O bus select A/B, clock divider select, and more. The A-11 board design is such that circuits on the board are organized into eight circuit groups and each group is powered by the +10-V spacecraft power bus. Some groups are separately isolated and limited on the bus by use of the standard interface circuit mentioned above. The circuit groupings are such that circuits for SCP in control, I/O crossed/not crossed, and I/O bus select A/B are powered by the same input, and do not use the standard capacitive filter circuit mentioned above. This design (the lack of filter capacitor in the circuit) makes these functions more susceptible to the electromagnetic spike effect discussed in Hypothesis C5. A single part short in this circuit or a resistor short (very rare) local to the grouped +10-V power input can cause a mission catastrophic loss of control failure identical to that described in Hypothesis C5. Analysis shows that noncausally connected circuit shorts related to an internal part failure or an electromagnetic spike as in Hypothesis C5 can also initiate this type of failure.⁸ This potential failure is possible and would meet the observables. It is considered to be very unlikely, but more likely than a failure that would disable the entire +10-V spacecraft interface power bus.

Conclusion

These failures are very unlikely, and analysis indicates near impossibility. However, in any of these cases, the spacecraft would not function. This would match the observables.

Hypothesis N7 is Category B: credible, but very unlikely; uncertainty associated with the analysis requires caution.

⁸ T. Nguyen, *Assessment of CIU Power Line Short Model*, JPL Interoffice Memorandum 5211-93-494, Jet Propulsion Laboratory, Pasadena, California, October 26, 1993.

CHAPTER VIII

ASSESSMENT OF THE HYPOTHESES

A. Hypotheses Summary

Table 8-1 summarizes certain relevant information about each hypothesis.

The attitude dynamics categories from Chapter IV.C.3 may be applied to all the hypotheses generated in Chapter VII. The first six columns in Table 8-1, Hypotheses Summary, document these categories. The next few columns classify the hypotheses in terms of the observables.

In some cases, the scenario and resulting attitude-time history should have produced an autonomous downlink. Hypotheses receiving a "yes" in this column do not meet the observables.

Some hypotheses result in undesirable spacecraft states which the correct sequence of ground commands can fix. These are indicated in the next column.

If there exist commands which could fix the hypothesized problem, the next column indicates if those commands were sent, and indicates, by the designation "H," if the transmitted commands were CIU-hardware-decoded commands.

The next column indicates if the scenario and resulting attitude-time history would allow uplink commands to be received and acted upon. If commanding could fix the problem, the right commands were sent (and often enough), and the scenario allows uplink, then the scenario does not match the observables. (Hypothesis S1 is an example of this type.)

The next column combines the data in the preceding columns to determine if the hypothesis meets all of the observables.

The final column indicates the Board's assignment of the hypothesis category designation, which is defined in Chapter VI.B and in Table 6-3.

The fact that the spacecraft did not recover, either autonomously or by ground commands, leads to the conclusion that the failure is unrecoverable. (The spacecraft is either physically damaged or in an unrecoverable electronic state that occurred during the 14-minute transmitter-off period.)

In summary, the four most credible hypotheses (all Category A) for the cause of the loss-of-signal anomaly are:

- (1) Destruction of the spacecraft due to a breach of the Propulsion System caused by one of the following three mechanisms:
 - (a) Ejection of a NSI squib/initiator from the pyro valve (Hypothesis C4),
 - (b) Pressure regulator failure due to contamination (Hypothesis C2), or
 - (c) Propellant reaction in the pressurant lines (Hypothesis C1A)
- (2) Electrical power loss due to a massive short in the Power Subsystem (Hypothesis S2)
- (3) Loss of the spacecraft computational function (both spacecraft computers prevented from controlling the spacecraft) in a way that could not be corrected by ground commands (Hypothesis C5)
- (4) Loss of both transmitters due to failure of an electronic part (Hypothesis C16)

B. Assessment

The analysis of the Mars Observer loss-of-signal anomaly is difficult due to the lack of available diagnostic information. The only available information is that which can be inferred by the lack of success in detecting a downlink carrier either autonomously or through ground command activity. The analysis and investigations of the Board did not result in a "smoking gun" that would have made one hypothesis the obvious cause of the failure. The result of this situation is the impossibility of establishing either a *primary cause* or a *contributing cause* for this anomaly; all the Category A and B hypotheses have thus been identified as credible *potential causes*. (These italicized terms are defined by NASA.¹)

The discussion of the hypotheses in Chapter VII shows that a priori, none seems particularly likely based on all available information. It is naturally tempting to conclude that one of the least improbable potential causes is the cause of the anomaly, but there is no assurance that this is correct. The actual ex post facto probability of anomaly occurrence is unity (it happened), so the inescapable conclusion is that one of the following applies:

- (1) The hardware flown makes one of the identified potential causes unusually probable, or
- (2) An important single-point failure or unanticipated system response remains undiscovered, or
- (3) There is an undiscovered generic flaw in the hardware or software, or
- (4) The anomaly was an unfortunate happenstance.

¹*Mishap Reporting and Investigating*, NASA NMI 8621.1F, Washington, DC, December 31, 1991.

Table 8-1. Hypotheses summary.

Hypothesis	Attitude Dynamics				Attitude and scenario give autonomous downlink	Commanding can fix?	Commands to fix were sent? ^b	Attitude and Scenario allow uplink?	Meets Observables?	Hypothesis Category A/B/C
	Nominal Control	No High spin rate	Attitude does not matter	Complex attitude dynamics						
C1A Reaction in lines		✓			Possible	No		Unlikely a	Likely	A
C1B Reaction in tank			✓		No	No		No	Yes	B
C1C "Liquid bullet"		✓			Possible	No		Unlikely a	Likely	B
C2 Regulator fails open			✓		No	No		No	Yes	A
C3A Flaw bursts tank			✓		No	No		No	Yes	B
C3B Meteoroid damages tank			✓		No	No		No	Yes	B
C3C Flaw ruptures line		✓			Possible	No		Unlikely a	Likely	C
C4 NSI impacts tank			✓		No	No		No	Yes	A
C5 CIU indeterminacies					No	1 yes, 1 no	Yes, H	Yes	No ^d	A
C6 Software problem				✓	Assume no	Many yes	Yes, H	Many yes	Some yes	B
C7 Miswired pyros ^c	✓ HGA			✓ SA	Yes	Yes	No	Yes	No	C
C9 Sequence error					Assume no	Many yes	Some	Many yes	No ^d	B
C10 Skew RWA stall	✓				Yes	No		Yes	No	C
C11 Exciter freq. reference loss	✓				No	No		Yes	Yes	C
C12 RPA H/W S/W conflict	✓				No	Yes	Yes	Yes	No	C
C13 RPA coil short	✓				No	No		Yes	Yes	B
C14 RPA overcurrent protection	✓				No	No		Yes	Yes	C
C15 Erratic CIU interface				✓	Some yes	No		Yes	Yes	B
C16 RPA control failure	✓				No	No		Yes	Yes	A
S1 RXO transistor failure		✓ (1 of 4)		✓ (3 of 4)	Yes	Yes	Yes, H	Yes	No ^d	B
S2 Power loss			✓		No	No		No	Yes	A
S3 Erratic RXO output				✓	No	Some yes	Yes, H	Likely	Some Yes	B
S4 RPA cathode support failure	✓				No	No		Yes	Yes	B
S5 Gyro spin motor short				✓	Possible	Yes on DOY 234	No	Yes on DOY 234	Possible	B
S6 Sun sensor head #4 fails				✓	Yes	Yes	No	Yes	No	C
S7 RWA overspeed				✓	Yes	Yes	No	Yes	No	C
N1 Meteoroid (14 min) impact			✓		No	No		No	Yes	B
N3 DSN detection problems	✓				Yes	N/A		Yes	Yes	C
N4 Multiple failures				✓	Assume no	No		Some yes	Yes	B
N6 SEE problems				✓	Assume no	Some yes		Some yes	Some yes	B
N7 +10-V I/F power failure		✓			No	No		No	Yes	B

a Possible but less likely than autonomous downlink.

b H indicates hardware commands were used.

c Miswired pyro valve to HGA or Solar Array (SA) deployment pyro.

d Analysis is so complex that there is some room for error in this conclusion.

C. Tests Performed or in Process

In several cases, the physics, modeling, or analysis of the hypothesis was quite complex. This led to suggestions for laboratory tests or inspection of the spare Mars Observer hardware. Table 8-2 lists the subjects of the tests. In most cases, these tests were suggested by and/or defined jointly with the NASA Review Board and its subsystem teams. In some cases, because the hardware had been impounded, approval for tests was required from the NASA Board and NASA Headquarters.

Table 8-2. Tests performed or in process.

Subject of test	Test description
Propulsion System	<ul style="list-style-type: none"> • Check valves—He gas leakage • Check valves—NTO (liquid and vapor) leakage • “Liquid bullet” • Chemical reaction (in lines and in MMH tank) • Inspection/sectioning of pyro valves after firing <ul style="list-style-type: none"> • Two from pre-launch pyro shock test • Ten from lot acceptance tests • Six from upcoming pyro shock test
Pyro shock	<ul style="list-style-type: none"> • g-level spectrum • EMI pulse (electronic part latch-up) • RPA cathode support structure mock-ups • Survival of key equipment (RPA, RXO, and IMU) • Impact impulse if NSI is ejected
Power System Electronics	<ul style="list-style-type: none"> • Visual inspection and partial disassembly • Diode isolation failure • Capacitor short tests
Verification Test Laboratory	<ul style="list-style-type: none"> • Many simulation runs
Mars Balloon Relay	<ul style="list-style-type: none"> • Send commands to activate MBR transmitter • Positive detection will elevate Hypothesis C16 to a single probable cause • Lack of detection will move Hypothesis C16 to Category B^a

^a Due to adverse Sun–Earth geometry, the Board believes that a negative result will not be definitive until February 1994.

In several cases, the tests are complete, but most will not be completed until after publication of this report. The results of those tests may well influence the categorization of some of the Category A and B hypotheses; some may move up to Category A and others may move down to Category B.

CHAPTER IX

FINDINGS

The Mars Observer Special Review Board could not identify a single most probable cause for the Mars Observer loss of signal. However, deficiencies in spacecraft design, qualification, integration and test, or operations were identified and related to the potential causes of the failure. The most significant of these are described in this chapter. Observations *incidental* to the potential causes of the failure are discussed in Chapter X.

The Board was directed to “recommend steps that *could have* or *should have* been taken to prevent this event.” With each finding, the Board indicates which hypothetical failure(s) *could have* been prevented if the recommendation had been followed. These recommendations are also relevant to possible reflight of the spare Mars Observer hardware or a similar planetary spacecraft design. The findings address all the Category A hypotheses for the failure, and some of the similar Category B hypotheses.

The Board elected not to address what “should have” been done in each case. Such a value judgment must be made by the Project, taking into account such constraints as budget, schedule, and mass margins. The statement that the Project “*should have* done everything it *could have* done” is an oversimplification of the complexity and magnitude of the management task.

A. System Engineering

1. Finding

The level and quality of system engineering implemented on the Project did not prevent numerous errors in design, design verification, integration, and test.

2. Discussion

This finding is a global assessment, as many of the other Findings and some of the Observations are specific examples that sprang from this root cause.

The original Observer concept was to use an inherited spacecraft design with minimal changes; in this plan much of the required system engineering had already been accomplished, and the level of systems engineering activity would be much lower than on a more typical project. It is possible that the planned system engineering activity was originally underestimated, but it seems more likely that the abandonment of the original Observer concept (with the addition of significant changes) was not accompanied by an appropriate increase in system engineering activity.

The primary consequences of the low level of system engineering activity was that most problems were found empirically from *anomalies* that occurred, rather than by

deliberate search; this shortcoming was exacerbated by the limited exploration of anomalous conditions during Integration and Test (see Chapter X.C, Observation C). The result of this was that many responses to anomalous hardware conditions were both less understood and less satisfactory than on most spacecraft designs (see Findings D, E, F, G, and H).

This finding is validated by the anomaly and ensuing investigation; much of what is known about the unsatisfactory response of the spacecraft to various faults and failures (including those not related to the anomaly) appears to have been discovered during this investigation activities (largely by the Project and contractor). This suggests that the augmentation of system engineering activity required to discover these flaws during development would not necessarily have caused a significant increase in Project cost.

3. Recommendation

Implement a level of system engineering that provides adequate design, design verification, integration, and test.

B. Propulsion System Pressurization Design

1. Finding

Propellant condensation in the Pressurization System was not prevented by the design of the Mars Observer Pressurization System. Concerns include the lack of isolation of the regulator and the use of a series-redundant regulator. The titanium-thread (for NSI port) pyro valve design is marginal.

2. Relevant Hypotheses

C1, C2, and C4

3. Discussion

a. Hypotheses C1A and C1B—Effects of Liquid Oxidizer Condensed in the Pressurization System

These failure modes could have been precluded by providing heaters and thermostats to maintain higher temperatures in the Pressurization System than those of the propellant tanks at all times. This would prevent condensation of liquid oxidizer.

Alternately, the risk of such a failure could have been reduced by providing pyro valve isolation of both propellants from the Pressurization System during cruise. This risk mitigation would still allow condensation to occur following pressurization of the propellant tanks, but (barring an off-nominal trajectory injection) would have reduced

the time available for such transport to occur by approximately 80 percent. Redesign of the Mars Observer Pressurization System to preclude such faults is a deviation from accepted industry practice for commercial Earth orbital spacecraft.

b. Hypothesis C2—Regulator Failure

This failure mode could have been precluded by providing onboard fault protection software and hardware to allow isolation of a failed open regulator. A separate parallel regulator would have to be provided to allow the mission to continue after such a failure.

Alternatively, the risk of such a failure could be reduced by isolating the regulator from both types of propellant vapors during cruise, since this hypothesis requires long-term interaction between propellant vapors and pre-existing contaminants. Barring an off-nominal trajectory injection, this action would have reduced the time available for such interaction by approximately 80 percent. Further risk mitigation could have been accomplished by more carefully monitoring cleaning and contamination control procedures during subsystem build-up, integration, test, and servicing.

Redesign of the Mars Observer Pressurization System to preclude such faults is an expensive deviation from accepted industry practice and is hence considered to be outside the scope of the Observer concept.

c. Hypotheses C4—NSI Expelled/Pyro-Valve Failure

This failure mode could have been precluded by relying less on heritage and conducting a more thorough pyro valve qualification test. This testing should include sympathetic firing of the second NSI and destructive examination of the test units. Review of the pyro valve stress analysis would have revealed that the threads holding the NSI in place had little structural margin and would have focused attention on their condition after firing.

4. Recommendations

Maintain Pressurization System temperatures which preclude condensation of propellants; isolate the propellant tanks with pyro valves; replace the titanium pyro valves with ones less likely to eject a NSI; add pressurization isolation and/or reactivation capability; and review heritage of all components (and requalify if necessary).

C. Primary Power Subsystem Ground

1. Finding

The Primary Power Subsystem grounding scheme is susceptible to high-side power shorts to chassis that disable the spacecraft power. Also, chassis current surges can cause integrated circuit failures.

2. *Relevant Hypotheses*

C5 and S2

3. *Discussion*

The design of the Mars Observer Power System ties the primary power return directly to chassis with no isolation. This design is vulnerable to a catastrophic high-side short to chassis within the power control electronics, which results in total mission failure.

This is a design weakness that has widely been accepted by the commercial aerospace industry.

The difficulty in the direct connected return-to-chassis design is the total dependence on design, fabrication methods, and quality control during the manufacturing process— which is difficult to monitor at the level of detail required. The loss of the NOAA-I spacecraft due to a chassis short in the Battery Charger Assembly on August 21, 1993, supports the existence of these types of problems.

It is recognized that the approach described in Chapter III, of using an existing commercial spacecraft design with minimum modifications, and the use of contractor's processes, with no new quality control or manufacturing requirements, places the implementation of an improved primary system grounding scheme outside the scope of the Observer concept.

However, improved design, manufacturing, and inspection of the isolation components and techniques of the Power Subsystem could have prevented the failure of NOAA-I and this credible potential failure of Mars Observer.

4. *Recommendations*

The preferred solution is to implement isolation between the Primary Power Return and chassis.¹ If this is impractical, improve the isolation of power components to the chassis to preclude failure modes similar to the most recent NOAA-I incident. Provide additional manufacturing improvements and inspection steps in critical areas.

D. **Fault Protection**

1. *Finding*

The Mars Observer Fault Protection design and test program did not provide protection against several serious failure modes.

¹ *Long Life/High Reliability Design and Test Rules Study Report; Topic 230—Primary Power Isolation*, JPL Document-9899, Jet Propulsion Laboratory, Pasadena, California, July 1992.

2. *Relevant Hypotheses*

C13, C16, S1, and S5

3. *Discussion*

A major issue related to spacecraft viability is fault protection. There was a lack of a top-down, system-engineering design approach to fault protection.² This lack has resulted in a set of low-level hardware-specific detections with accompanying logic for switching redundant elements, which does not consider necessary implications of, or the autonomy required by, a planetary mission. The fault protection test requirements for the VTL were not derived from a consistent set of top-level requirements and were inadequate validations for flight.

Software algorithms are only one concern; inattention to FMECAs and hardware responses to failures are some others; Hypotheses C16 and S1 represent problems of this type that were discovered during the Board's investigation.

Fault Protection omissions included: (1) no use of the Reaction Control System (RCS) attitude control when fault protection indicates that the RWAs cannot control the spacecraft; (2) large attitude control errors do not initiate fault responses; (3) the interaction of the RXO and Clock Divider with the spacecraft was inadequately addressed and is a concern for both the spacecraft design and the simulation in the VTL; and (4) Contingency Mode does not ensure a downlink signal.

4. *Recommendations*

Develop system-level requirements for the Fault Protection System that address the unique aspects of a planetary mission. Review the required changes to the hardware and software; implement these changes, and develop a test plan that adequately verifies system performance at the spacecraft level. Specifically address the RXO and Clock Divider system response and the Contingency Mode problems. Test on the spacecraft; use the VTL only to augment testing done on the flight spacecraft, or to perform tests that cannot practically be done on the spacecraft.

E. *Command and Data Handling Subsystem*

1. *Finding*

The Command and Data Handling Subsystem has circuits which can result in an indeterminate state, a dangerous SCP-ULP command hang-up problem, and an RXO that contains suspect parts.

² C. Jones, *Mars Observer Flight Software Fault Protection and Operability Review Board Report*, JPL Interoffice Memorandum CC-CPJ-08-91, Jet Propulsion Laboratory, Pasadena, California, June 3, 1991.

2. Relevant Hypotheses

C5, C16, and S1

3. Discussion

There are single failure points in the CIU whereby a part failure or logic upset can disable critical control functions. They are:

- (1) SCP In Control (C5A)
- (2) I/O Crossed/Not Crossed (C5B)
- (3) I/O Bus Select (C5C)
- (4) RPA lock-up (C16)

Logic upset due to pyro-firing-induced chassis current can alter the state of control logic to the extent that neither redundant function is operational. Connecting the primary system power return to chassis provides a path for the EMI.

The RPA lock-up hypothesis (C16) is referred to here since the generic C5 part latch-up can cause this problem also. This, however, is a separate hypothesis since it can be caused in other ways, and is discussed below in Section H, Unidentified Single Failure Points, below.

As described in the discussion of Hypothesis S2, redesigning the grounding scheme or providing an isolated pyro firing source is considered to be outside the scope of the Observer concept.

However, it is possible to separate the control circuits for redundant elements in the CIU so that one inverter would not be depended on to provide complementary control. This would have prevented a single part failure or upset resulting in both redundant elements being inoperative. The circuit design, including the 51-ohm resistor, should be re-examined.

The SCP-Restart command was tested in the VTL during the recovery operations. This command hung up the uplink processor (ULP) because it waited for the SCP to perform a read of the uplink buffer in the CIU. The SCP does not read the buffer after restart and prevents the CIU from ever commanding the SCP again.

The Redundant Crystal Oscillator contains suspect 2N3421 transistors that can fail and consequently remove one redundant side.

4. Recommendations

Separate the control circuits for redundant elements. Review and modify the CIU, SCP, and flight software as necessary to eliminate the identified uplink command hang-up problem. Adequately test all fault protection logic and critical commands on the spacecraft via the radio link (i.e., a plugs-out test) to validate their usage. Replace the suspect 2N3421 transistors in the RXO.

F. Telecommunications Subsystem

1. Finding

The downlink was turned off during a critical sequence. This complicated the recovery operations and hampered investigations. This also could have initiated the Hypotheses C16 (Category A) failure scenario.

2. Relevant Hypotheses

C13, C16, and S4

3. Discussion

The RPA beam and cathode heater were turned off during this pressurization sequence since it was recommended as safer by Astro. Astro and the RPA manufacturer had confidence that the RPA would survive pyro shock when off (cold), but the manufacturer and JPL technical staff believed that a test should be done to qualify the part for shock when on (hot). Budget constraints precluded that test from being performed.

There apparently was little concern about turning off the RPA because this subsystem had been qualified for 10,000 on/off cycles, and the Project had planned to turn the beam off each orbit during occultation to save power. There was a consensus that an additional off cycle during the pressurization sequence would be insignificant. However, even though the RPA was tested for 10,000 Beam On/Off cycles, there were no qualification requirements or qualification for cathode heater (filament) on/off cycles.

4. Recommendations

The downlink should not be turned off except when spacecraft power cannot support it. This will require qualification of the RPA to withstand pyro shock when the filament and beam are on, and will also require careful design and verification of the new sequences (e.g., one should transmit on the LGA whenever attitude changes are planned or probable). In addition, the function and interactions of the Interlock circuits should be carefully reviewed with respect to any new sequences.

G. Flight Hardware Heritage

1. Finding

Qualification of flight hardware by heritage failed to account for significant differences in hardware design, operating environment, or application for some mission-critical hardware.

2. *Relevant Hypotheses*

C1, C2, C4, and S4

3. *Discussion*

Qualification of some mission-critical flight hardware by heritage was marginal. In some cases, heritage assumptions could not be traced to specific qualification testing of the design flown (e.g., the RPA had been qualified for some environments by extrapolation from tests of similar, but not identical, hardware).

Although similar hardware assemblies may be traced to successful flight spacecraft, such as DMSP, Landsat, and TIROS, the potential exists for major shortcomings in design qualification by heritage. Earth orbiter requirements differ significantly from planetary requirements, so the qualification of the hardware could be compromised, and the hardware would then require re-qualification. This is especially true for the Propulsion Subsystem, where both the design and testing requirements are significantly altered by the need for long-term compatibility of materials with the propellants, and with the need for major propulsion burns a year after launch.

4. *Recommendations*

Re-evaluate flight hardware designs through a series of heritage reviews that thoroughly evaluate the design and qualification status of hardware proposed as heritage. Re-qualify whenever critical hardware elements are not directly traceable to identical hardware used in the same application.

H. Unidentified Single Failure Points (SFPs)

1. *Finding*

During the course of the Mars Observer mission and the Board's investigation, numerous potential SFPs were discovered that had not been previously recognized.

2. *Relevant Hypotheses*

C4, C5, C13, C16, S1, S2, S3, and S5

3. *Discussion*

Several unidentified single failure points were discovered which involved single-part latch-up, shorting, or fault protection response. Examples include:

- (1) SCP control indeterminacy due to latch-up of a single component (Hypothesis C5)
- (2) Inability to turn on either RPA after cathode heater (filament) turn-off if there is a latch-up or failure of any of several parts (Hypothesis C16)

4. Recommendation

Re-evaluate single failure points through a thorough review of circuit diagrams, fault trees, and FMECAs. Evaluate the risk of identified SFPs, and disposition appropriately.

CHAPTER X

OBSERVATIONS

During this investigation, the Board made various observations that were significant, but which were *incidental* to the cause of the loss-of-signal anomaly. Some observations relate to Category B or C hypotheses, which are almost certainly not the cause of the failure. Others relate to deviations from generally accepted design practice, or to improvements that could increase reliability. Some had been recognized by the Project but were not effected for programmatic or other reasons. It is recommended that the Project review and disposition these recommendations prior to reflight of the existing spare, or flight of a new, Mars Observer spacecraft.

I. TECHNICAL OBSERVATIONS

A. *Redundant Crystal Oscillator (RXO)*

1. *Observation*

There is a set of RXO failures whereby one of the two outputs will be lost.

2. *Discussion*

The RXO is internally redundant and for some failure modes provides an output on both of its outputs (J1 and J2). There is ample indication that some Project members did not expect either output to disappear. Block diagrams erroneously showed complete cross strapping of the oscillators with the buffer amplifiers. Other documents that exist indicate that some members of the Project Team were aware that one output disappears in some failure modes.

The system response to the loss of the one RXO output is extraordinarily complex. The clock signals are divided down in the CIU to many frequencies and sent to many subsystems. The Clock Divider switch logic was such that many of these subsystems would end up without a clock reference if such a failure occurred. It is clear that the fault protection logic used had not been designed to handle this case.

3. *Recommendations*

Re-examine the Clock Divider switching logic and fault protection for RXO output failures, and modify as appropriate. Consider possible RXO modifications to ensure two outputs, and to telemeter both output signal levels.

B. Command and Data Handling Subsystem

1. Observation

Critical control circuits in the CIU are potential single failure points.

2. Discussion

The CIU A-11 board contains the critical control circuits for SCP in control, I/O bus crossed/not crossed, and I/O bus select. The complement of these signals is generated by using separate inverters within the same part. This means that the failure of this part, or the +10-V power supplied to it, can disable all of these functions.

3. Recommendation

Separate these control circuits to use different parts which use separate +10-V power inputs. Generate complementary signals (for at least these three functions) without relying on a single inverter. Use a high-reliability capacitive filter on the +10-V power supplied to these circuits.

C. Integration and Test

1. Observation

The spacecraft-level test program was inadequate.

2. Discussion

The spacecraft-level test program did not adequately test the fault protection algorithms, and Safe Mode, nor did it perform high-integrity pyro shock testing. The CIU-hardware-decoded commands (e.g., SCP Restart) were not thoroughly tested before launch.

3. Recommendations

Test as much of the system functionality as possible on the spacecraft, while protecting the safety of the spacecraft.

D. Sequence

1. Observation

Safe Mode was disabled during the pressurization sequence.

2. Discussion

Because pressurization was done so close to MOI, it occurred during the period when Safe Mode was disabled. Safe Mode was disabled at MOI-7 days because the MOI sequence would have been aborted by entry into Safe Mode, and it was thought that the Flight Team could not perform a recovery from Safe Mode in less than 7 days. Safe Mode is usually the final resort if other fault responses cannot correct a problem. Safe Mode includes rebooting the SCPs to operate out of ROM, and if this mode is disabled, certain RAM software-related problems cannot be solved.

3. Recommendations

During the period when Safe Mode must be disabled to protect the MOI sequence, keep the spacecraft as quiescent as possible. Do not perform any activities that may increase the probability of fault protection responses being initiated. Have the Flight Team practice recovery from Safe Mode, so that the period that the spacecraft must be disabled can be minimized to less than 7 days.

E. Recovery Operations

LGA

1. Observation

It took more than 7 hours to command a switch to the LGA.

2. Discussion

Arm and Go to Contingency Mode were the first ground commands sent that would have selected the LGA for downlink. Since the spacecraft was on the HGA during the nominal sequence, any attitude error greater than about 28° would preclude a downlink.

3. Recommendation

The first ground action after a loss-of-signal anomaly should be to command a switch to the LGA and turn the RPA beam on.

Clock Divider

1. Observation

Recovery commanding did not adequately ensure early reception of the Clock Divider 2 Select command.

2. Discussion

The Clock Divider 2 Select command was sent only twice on day 237; it was not sent again until day 260, when it was sent 70 times. A loss of prime Clock Divider output results in a condition whereby the reaction wheels cannot be commanded to control the spacecraft attitude (see Hypothesis S1). With the resultant time-varying spacecraft attitude, and also possible temperature-related changes to the receiver best-lock frequency, multiple commanding is required to ensure successful reception.

3. Recommendations

When commanding in the blind, commands should be sent on the order of 10 times at irregular intervals, and there should be a special uplink acquisition sweep(s) by the DSN to ensure command lock.

F. Mars Balloon Relay Experiment

1. Observation

The attempt to perform this experiment failed because the wrong commands were sent.

2. Discussion

The Project was requested to turn on the MBR by the NASA Review Board, and a listening campaign by three large antennas was conducted (see the description of this experiment in Appendix U). The importance of this experiment is that if an MBR signal is detected, it would single out one of the RPA-only failures (C16, C13, or S4) as the single probable cause of the anomaly. Conversely, if the signal is not detected (and if one is convinced that a signal should be detected), then Hypothesis C16 would be downgraded to Category B.

This failure occurred because the commands sent cannot be executed with the ROM software that was being executed by the spacecraft. Apparently, the commands were simulated, but with the full flight software, not the ROM code version.

3. Recommendations

Ensure that Flight Team and VTL simulation procedures identify the correct spacecraft state before validating command sequences. Perform the MBR experiment with an alternative set of commands that the ROM code can execute. Listen for the MBR signal for several months until the Earth-spacecraft-Sun geometry improves sufficiently to assure a conclusive result.

II. PROGRAMMATIC OBSERVATIONS

A. Fixed-Price Contracts

1. Observation

Fixed-price contracts do not work well when significant development is required.

2. Discussion

The uncertainty and changes intrinsic to development are incompatible with the objective of fixed-price contracts.

The original Observer Program included the concept of a science payload module that would isolate the “production line” spacecraft from the science instruments. That concept was dropped early in the program (to save mass on the spacecraft) and only the GFE Payload Data System (PDS) survived. Eliminating the payload module resulted in many additional spacecraft system changes.

3. Recommendations

Do not use fixed-price contracts when development is required, or when changes are anticipated, or when control over detailed technical implementation is required.

B. Operations

1. Observation

The knowledge base of the spacecraft design was not adequately transferred from the spacecraft developer to the Mission Operations Team.

2. Discussion

There was inadequate understanding of the spacecraft by the Flight Team. Examples include the RXO, Sun sensor fields of view, the MBR commands sent in Safe Mode, and the antenna patterns. Some of the information (e.g., regarding the RXO) was incorrect or misleading.

3. Recommendations

Ensure improved information and knowledge transfer from development to operations. Improve documentation and training provided for operations. Begin operations development and training earlier. Train operations personnel by involving them in development. Transition key developers into the operations phase. Provide easy and quick access to developers by operations personnel after launch and especially for, or in advance of, key mission events. Prepare the development organization in advance of key mission events by involving them in project reviews and discussions, or by establishing a special contingency working team within their organization.

C. Reliability

1. Observation

Reliability risk assessment was not complete.

2. Discussion

Reliability assurance was neither thoroughly conducted nor concluded on the Mars Observer Project. The documentation does not reflect that the risk assessments on FMECAs, waivers, and circuit analyses were adequately considered and mitigated. The review processes failed to uncover the design shortcomings covered in this report.

3. Recommendations

Implement a more thorough and complete reliability assurance program.

D. Documentation and Configuration Control

1. Observation

It was difficult to obtain accurate and consistent information on the as-built configuration of the spacecraft.

2. Discussion

The Board found many examples where the documentation received was inconsistent or in error. It was difficult to know the latest design and what was actually flown. Documents were not updated (many came from other programs) and had Engineering Change Notices (ECNs) on top of other ECNs. It was impossible to get electronic part lists for selected subsystems. Photographic documentation of the flight spacecraft and its assembly panels was informal and incomplete.

Poor documentation not only caused problems in the investigation, but could have contributed to misunderstandings among Development and Flight Team members.

3. Recommendations

Require quality documentation of the system as flown.

CHAPTER XI

GLOSSARY

AACS	Attitude and Articulation Control Subsystem
ACE	attitude control electronics
ANS	array normal spin
AO	Announcement of Opportunity
AOS	acquisition of signal
Astro	Martin Marietta Astro Space
AUX	auxiliary
AW	acceptance withheld
BATT	battery
BCA	battery charger assembly
BDB	bus distribution board
BIT	bench integration test
BPROP	bipropellant
bps	bits per second
BU	backup (also B/U)
BVR	boost voltage regulator
C&DH	Command and Data Handling Subsystem
CD	clock divider
CDU	Command Detector Unit
CEA	central electronics assembly
Chg	charge
CIU	controls interface unit
CIUG	CIU ground
CIX	controls interface extender
CLT	Command Loss Timer
CM	contingency mode
CMD	command
CMDLOS	command loss fault protection program
CMOS	complementary metallic-oxide semiconductor
CNTLS	controls
CONFIG	configuration
CSA	Celestial Sensor Assembly
Curr	current
CV	command verification
CYCEXEC	cyclic executive
Δ	delta
DL	downlink (also D/L)

DMSP	Defense Meteorological Satellite Program
DOR	differenced one-way ranging
Δ DOR	delta differenced one-way ranging
DOY	day of year
DPA	destructive physical analysis
DRV	drive
DSN	Deep Space Network
DSS	Deep Space Station
DTR	digital tape recorder
Δ V	change in velocity
EDAC	error detection and correction
EDF	engineering data formatter
EED	electroexplosive device
EEE	electronic, electrical, and electromechanical
EIRP	effective isotropic radiated power
EM	engineering model
EMC	electromagnetic compatibility
EMI	electromagnetic interference
ENG	engine or engineering
EPC	electric power converter
EPET	electrical performance evaluation test
ER	Electron Reflectometer
ERT	Earth-received time
ESA	European Space Agency
ESD	electrostatic discharge
ESTEC	European Space Research and Technology Centre
ETR	Eastern Test Range
EXT	external
FBA	fuse board assembly
FEI	Frequency Electronics, Inc.
FET	field effect transistor
FET	functional electrical test
FITS	failures per billion hours
FLT	flight
FOV	field of view
4π SS	4π Steradian Sun Sensor
FP	fault protection
FPR	functional performance review
FSW	flight software
GDA	gimbal drive assembly
GDE	gimbal drive electronics
GEN	generator
GFE	government-furnished equipment

GHe	gaseous helium
GMBL	gimbal
GRS	Gamma Ray Spectrometer
GSE	ground support equipment
HEF	high-efficiency front end
HGA	high-gain antenna
HRMS	High-Resolution Microwave Survey
H/W	hardware
IABS	integral apogee boost stage
I/F	interface
IMU	inertial measurement unit
INST	instrument
I/O	input/output
IPTO	initial power turn-on test
IPTO	integration power test operations
ISA	Incident/Surprise/Anomaly form or report
ISH	inertial slew hold
IU	interface unit
JPL	Jet Propulsion Laboratory
LET	linear energy transfer
LGA	low-gain antenna
LMC	link monitor control
MAG	Magnetometer
MANUVR	maneuver
MBR	Mars Balloon Relay
MEMCHK	memory check
MEOK	SCP software state indicating good health
MGA	Medium Gain Antenna
MGCO	Mars Geoscience Climatology Orbiter
MHSA	Mars Horizon Sensor Assembly
MMH	monomethylhydrazine
MMSA	multimission support area
MO	Mars Observer
MOC	Mars Observer Camera
MOI	Mars orbit insertion
MOLA	Mars Observer Laser Altimeter
MON	monitor data
MOR	Mars Observer Relay Antenna
MOS	Mission Operations System
MOT	Mars Observer Transponder
MSS	mission simulation software

NASA	National Aeronautics and Space Administration
NFSC	nonflight spacecraft components
NOAA	National Oceanic and Atmospheric Administration
NRL	Naval Research Laboratory
NSI	NASA standard initiator
NTO	nitrogen tetroxide
ODE	one-dimensional equilibrium (computer code)
OWLT	one-way light time
PCE	power control electronics
PDS	Payload Data Subsystem
PDT	Pacific Daylight Time
PEF	predicted events file
P/L	payload
PMIRR	Pressure Modulator Infrared Radiometer
PMPCP	Parts, Materials, and Processes Control Plan
POB	parallel output buffer
POR	Power On Reset
PRA	pyrotechnic relay assembly
PRI	primary (or prime)
PROP	propulsion
PSA	partial shunt assembly
PSE	power supply electronics
PSU	partial shunt regulator
PV	pyro valve
RAD	radiation
RAID	real-time application interactive debugger
RAM	random access memory
RCS	Reaction Control System
RCV	receiver
REA	rocket engine assembly
REDMAN	redundancy-management program
RF	radio frequency
RFI	radio-frequency interference
RFP	request for proposal
ROM	read-only memory
RPA	RF power amplifier
RPE	runaway program execution
RTL	round-trip light time
RWA	reaction wheel assembly
RXO	redundant crystal oscillator
SA	solar array (also S/A)
SATCOM	Committee on Scientific and Technical Communication

SATCOM	Committee on Scientific and Technical Communication
S/C	spacecraft
SCET	spacecraft event time
SCMF	Spacecraft Command Message File
SCP	Standard Control Processor
SCT	Spacecraft Team
SCU	signal conditioning unit
S&E	science and engineering telemetry
SEB	single-event burnout
SEE	single-event effect
SEGR	single-event gate rupture
SENDPDS	send commands to PDS program
SEPET	system electrical performance evaluation test
SEQTRAN	sequence translator program
SEU	single-event upset
SFOC	space flight operations complex
SFOF	Space Flight Operations Facility
SFP	single failure point (same as SPF)
SIM	simulation
SMOEXEC	special mode executive program
SN	serial number (also S/N)
SOB	serial output buffer
SOC	state of charge
SOE	Sequence of Events
SPF	single-point failure (same as SFP)
SPG	single-point ground
SSA	Sun sensor assembly
SSE	Sun sensor electronics
SSI	Spectral Signal Indicator
STAREX	star processing executive program
STE	system test equipment
STRPAN	spacecraft expanded block to turn an RPA on
SUPT	support
S/W	software
TCE	temperature control electronics
TCM	trajectory correction maneuver
Telecom	Telecommunications Subsystem
TES	Thermal Emission Spectrometer
TLM	telemetry
TOS	transfer orbit stage
TVC	thrust vector control
TWNC	two-way noncoherent
TWT	Traveling Wave Tube
TWTA	traveling wave tube amplifier
UL	uplink (also U/L)

USO	Ultra Stable Oscillator
UTC	Coordinated Universal Time
VIB	vibration
VPEF	Verification Test Laboratory Predicted Events File
VTL	Verification Test Laboratory
XMTR	transmitter
XPNDR	transponder
XSU	cross-strap unit

APPENDIX A
BOARD CHARTER AND MEMBERSHIP

102-93/LND:drh

August 30, 1993

TO: Board Members

FROM: Larry N. Dumas 

SUBJECT: Formation of a Special Review Board Regarding Mars Observer
Loss of Signal

A Review Board for the Mars Observer loss of signal is hereby appointed. the members are:

R. Rhoads Stephenson, Chairman
Robert E. Anderson
Douglas C. Bernard
Larry W. Wright
Thomas E. Gindorf
Carl S. Guernsey
Michael C. Lou
Duncan MacPherson
Gordon E. Wood
John P. Slonski, Jr. (Systems Engineering Consultant)

1. The Review Board is directed to:
 - a. Ascertain the most likely cause(s) of the Mars Observer loss of signal considering all relevant design, fabrication, test, and mission operations data.
 - b. Recommend steps that could have or should have been taken to prevent this event.
2. In the event that other review boards are formed to investigate this anomaly, the Board will cooperate with those boards as required to minimize duplication of efforts while still maintaining the independence of each board.
3. Appointments to the Review Board are effective immediately. The Board is directed to initiate planning immediately and to start operations not later than September 1, 1993. The Board Chairman has the prerogative to select a non-voting recording secretary for the Board.

4. A report of Board Findings and Recommendations is due to the Deputy Director not later than October 29, 1993.
5. Administrative support to the Review Board is to be provided by the Mars Observer Project Office.

Distribution:

W. T. Huntress, NASA/S
F. D. Gregory, NASA/Q
G. E. Cunningham

Board Members:

R. Rhoads Stephenson
Robert E. Anderson
Douglas C. Bernard
Larry W. Wright
Thomas E. Gindorf
Carl S. Guernsey
Michael C. Lou
Duncan MacPherson
Gordon E. Wood
John P. Slonski, Jr.

Executive Council

JET PROPULSION LABORATORY

INTEROFFICE MEMO
800 465/RRS/93:ld

September 14, 1993

TO: Board Members

FROM: R. Rhoads Stephenson



SUBJECT: Update of MO Special Review Board Membership

Subsequent to the chartering memo dated August 30, 1993, the following changes and additions to the board have been made:

1. David Eisenman replaced Robert Anderson.
2. Joe Savino is added.
3. Teo Almaguer is added as recording secretary.


Concurred: Larry Dumas, Deputy Director

cc: John Casani
Glenn Cunningham

APPENDIX B
BRIEFINGS LISTING

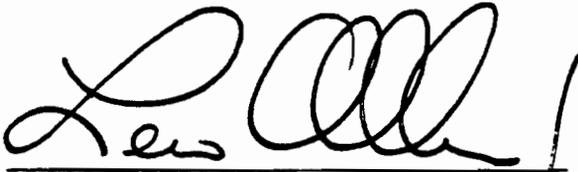
Table B-1. Briefings to the Mars Observer Special Review Board.

Date of briefing	Briefing	Source
September 1, 1993	Mars Observer contract overview	Mars Observer Project Office
September 2, 1993	Mars Observer Project overview and introduction to loss of communications	Mars Observer Project Office
September 3, 1993	Redundant crystal oscillator	Mars Observer Flight Team staff
	MOI sequence recovery commands, spacecraft emergency sequence and rationale	Mars Observer Project Office
September 7, 1993	Commands issued prior to pressurization, recovery command sequence	Mars Observer Project Office
September 8, 1993	Mars Observer Verification Test Laboratory	Mars Observer staff
	Telecom link analysis	Mars Observer and DSN
September 9, 1993	Mars Observer redundant crystal oscillator and the 2N3421 transistor	FEI
	Propulsion assessment related to Mars Observer communications loss	Mars Observer staff
September 10, 1993	Mars Observer Command and Data Handling Subsystem, SCP commanding and telemetry	Mars Observer staff
	Mars Observer system fault protection tutorial	Mars Observer staff and Astro
September 14, 1993	Command and Data Handling and Mars Observer flight software	Astro
	Telecom and data rates versus modulation indices	Astro
	Pyro shock and environmental testing	Astro
September 15, 1993	Integration and testing, system test program summary	Astro
	Flight software	Astro
	Response to Special Review Board data requests	Mars Observer Staff
	NOAA-I anomaly failure hypotheses	JPL Board Representative
	Mars Observer Power Subsystem	Astro
September 16, 1993	Summary of nominal loads by phase and modes (28 V)	Astro
	Mars Observer Telecommunications Subsystem	Mars Observer staff and Astro
September 16, 1993	Mars Observer Attitude and Articulation Control Subsystem	Mars Observer staff
	Mars Observer Power Subsystem	Mars Observer staff
September 17, 1993	Power Subsystem	Mars Observer staff
September 24, 1993	NRL Investigation Board trip report	Mars Observer staff
September 29, 1993	Mars Observer fault protection design review—historical overview	Mars Observer Fault Protection and Software Review Board Chairman
October 11, 1993	RF power amplifier	Hughes Electron Devices Division
October 15, 1993	ESA pyro valve tests	ESA

APPENDIX C
MARS OBSERVER PROJECT INITIATION AGREEMENT

MARS GEOSCIENCE/CLIMATOLOGY ORBITER

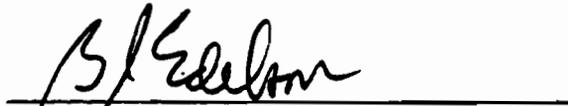
PROJECT INITIATION AGREEMENT



Lew Allen, Jr.
Director, Jet Propulsion Laboratory

9 Nov 83

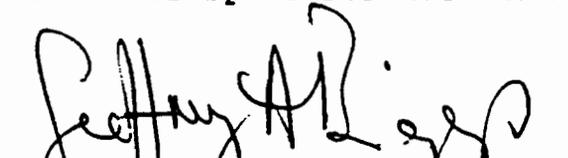
Date



Burton I. Edelson
Associate Administrator
Office Of Space Science and Applications

12/20/83

Date



Geoffrey A. Briggs
Director
Earth and Planetary Exploration Division

25 Nov 83

Date

MARS GEOSCIENCE/CLIMATOLOGY ORBITER (MGCO)
PROJECT INITIATION AGREEMENT

This initiation agreement sets forth the major responsibilities, interfaces, procurement plans, and schedule and resources to be followed in the implementation of the MGCO mission. The Project is planned for an FY 1985 start leading to a launch in August of 1990 and mission completion in August of 1993. The Jet Propulsion Laboratory, as the implementing center, will manage the Project, acquire the science instruments, conduct the flight operations, and contract with industry for the build and test of the spacecraft bus.

I. OBJECTIVES AND REQUIREMENTS

The Mars Geoscience/Climatology Orbiter mission addresses first order scientific questions relating to the atmosphere, the surface, and the interior of Mars. This mission will provide new observations of Mars, not feasible from Earth or Earth-orbit, which extend and complement existing data and provide an improved basis for future intensive exploration. Specifically, the scientific objectives are:

- determine the global elemental and mineralogical character of the surface material;
- define globally the topography and gravitational field;
- establish the nature of the magnetic field;
- determine the time and space distribution, abundance, sources, and sinks of volatile material and dust over a seasonal cycle;
- explore the structure and aspects of the circulation of the atmosphere.

Global mapping of Mars is necessary to meet these objectives. The climatology objectives (last two objectives) require mapping with sufficient frequency and extent that the state of the atmosphere and the volatile inventory can be characterized globally on a seasonal basis over a full Martian year. Candidate instruments and measurements that satisfy the science objectives are:

<u>Candidate Instrument</u>	<u>Principal Measurement</u>
Gamma Ray Spectrometer	Elemental abundance--potassium, uranium, thorium, iron, silicon, oxygen, carbon, hydrogen
Mapping Visual and Infrared Spectrometer	Minerology and condensates
Pressure Modulated Infrared Radiometer	Profiles of temperature, water, and dust
Radar Altimeter	Topography
Radio Science	Gravitational field and refractivity profiles
Ultraviolet Spectrometer	Ozone profiles
Ultraviolet Photometer	Atomic hydrogen column abundance
Magnetometer	Intrinsic magnetic field

These candidate experiments will return on a global basis highly synergistic quantitative measurements of the Martian surface, interior and atmosphere. Overall, the objectives and experiments seek to build on existing knowledge of Mars by returning measurements directed at answering specific questions in a global context.

The candidate instruments satisfy the mission objectives and form the explicit basis for establishing requirements to be met by the flight system. Science instrument selection will follow spacecraft system selection. The Announcement of Opportunity (AO) will be accompanied by documentation describing the spacecraft system to be used. In this way experimenters can tailor their proposals and instrument designs to a fixed spacecraft design. Assistance in refining the detailed science requirements will be provided by the MGC0 Science Working Group. The Science Working Group's activities will terminate with the release of the AO and a Project Science Group will be formed after selection of the MGC0 experiments.

II. TECHNICAL APPROACH

Mission

The MGCO mission will deliver a single spacecraft to Mars during the 1990 opportunity from a Space Shuttle launch utilizing an injection stage. For the acceptable mass performance, the 1990 opportunity requires a type II interplanetary trajectory with a flight time of nearly one year. A twenty-day launch period beginning in August 1990 results in arrival at Mars in August 1991. At Mars, the spacecraft will be initially inserted into a low near-circular polar orbit, the phasing orbit, which will provide coverage of the planet's polar regions while the orbit plane transitions to the desired solar orientation. After about two months, a plane change maneuver will place the spacecraft into the mapping orbit, which is near-circular at low altitude (350 km) and sun-synchronous at the desired solar orientation. Repetitive observations of the planet's surface and atmosphere will be conducted from the phasing and mapping orbits for one Mars year (687 Earth days). The primary mission observations will be completed in July 1993. The spacecraft will maintain a nadir-pointed attitude for the body-fixed surface instruments, and the atmospheric instruments will be self-pointing from the nadir to the limb, as required. After the primary mission, an extended mission for an additional Mars year may be possible. To conform with international agreements against the contamination of Mars with terrestrial organisms, the spacecraft will finally be raised to a higher altitude quarantine orbit.

Flight System

The MGCO Flight System consists of a spacecraft bus and payload module, a Mars orbit insertion capability, and an injection stage. The bus and insertion capability will be procured from an industrial contractor. The payload module will be designed and built by JPL and delivered to the contractor for integration with the bus. The injection stage may be provided to the contractor as GFE by NASA. A single flight system will be assembled, tested, and flown.

The spacecraft will be launched from the Space Shuttle orbit by an upper stage that is currently planned to be derived from the SRM-1 rocket motor. JPL is currently retaining the option to have the contractor provide this injection capability or to GFE the upper stage.

The spacecraft bus is planned to be a fixed-price procurement from a systems contractor. It will be a derivative of an existing, production-line, Earth-orbital spacecraft with the necessary minimal modifications for the interplanetary mission. Studies have shown this approach to be technically feasible and cost effective. The contractor will also be responsible for providing the Mars orbit insertion capability, which could be either a solid rocket motor or part of an integrated liquid system.

JPL will design, build, and deliver to the contractor a payload module which will match the existing spacecraft bus interfaces. The payload module will consist of a mounting shelf to which the science instruments and an interface data system will be attached. The data system will serve to distribute commands from the spacecraft to the instruments, as well as to collect the science data and send it to the spacecraft's command and data handling subsystem in one data stream. JPL will also provide the X-band transponder and command detection and telemetry modulation units. The contractor will be responsible for mating the payload module to the spacecraft bus, integrating the telecommunications, and integrating and testing the entire flight system.

Five of the candidate science instruments will be body-fixed on the spacecraft with fields-of-view toward the planet and its limb. The gamma-ray spectrometer and the magnetometer will be mounted on booms for isolation from the spacecraft. In Mars orbit, the spacecraft will be maintained in a nadir-pointing attitude. It may be either 3-axis or dual-spin stabilized. The propulsion system will provide for Mars orbit insertion (MOI, about 2.24 km/s), plus navigation and orbit maneuvers which total about 450 m/s. Power for the spacecraft will be provided by solar arrays, with batteries being used during occultation and maneuvers. Data storage will be on tape recorders with a minimum capacity of 33 hours of science data on each. Telecommunications will use an X-band system for both the uplink and downlink. The system will support a data rate of 8 kb/s at maximum range to a 34-meter DSS.

Mission Operations

The overall flight operations will reflect simplicity in operations through the use of highly repetitive sequences and automation in both planning and data handling. The operating simplicity is aided by the spacecraft body-fixed instrumentation and the repetitive nature of the mapping mission. The development and subsequent operating costs will be minimized through the use of the latest advances in ground-based hardware and software.

Standardization of instrument, spacecraft, and ground handling interfaces will play an important role in this process; additionally, it will allow incorporation, as appropriate, of new developments in technology.

Mission operations will be conducted utilizing a small staff of personnel. The majority of the staff will reside at a central Mission Support Area; the remainder of the staff, principally the scientists, will be located remotely at their home institutions. Highly automated workstations employing the latest techniques in data basing, communications, and display will be used to link all of the scientists, planning, engineering analysis, and management personnel together. Periodic face-to-face planning and coordination meetings will be held which include the remotely located personnel. These same workstations will be used to disseminate all data to the various users and to receive inputs for planning and conducting the mission. Routine operations will be the theme for the duration of the mission.

The planning of sequence activities will be performed 30 days in advance. Resulting sequences will then be transmitted to the spacecraft approximately 3 times per week. The actual update frequency will be a function of spacecraft sequencing capability and mission phase activity. The workstations, which will provide scheduling information, data accountability, sequence planning tools, and command constraint checking will enable the scientists to directly interact in the process of updating a basic set of repetitive sequences.

Real time and spacecraft tape recorder playback data will be received during one 8-hour period per day over a Deep Space Network (DSN) 34-meter station which will vary depending on tracking station availability. A 64-meter station may be utilized during the period following Mars orbit insertion while at maximum communications distance. First-order monitoring using various alarm techniques will be performed on the real time data to assess the overall spacecraft health and status. Further analysis will be performed on the data acquired from the daily playback during the normal workshift. Navigational information and spacecraft attitude information will be processed to provide position information relating to the acquired science data. The scientists may directly query the central data base from their remote work stations for their data.

The ground system will be developed early to allow support of instrument tests and will be fully configured at the start of instrument-to-payload module integration. This early development and utilization will enable the users to become accustomed to using the tools with which they will conduct the mission. Additionally this configuration may be used to support the sequence validation tests during spacecraft system testing at the contractor's facility, end-to-end tests at the launch facility, and post launch spacecraft conditioning. The equipment used in the ground system will conform to the standards adopted by the project and will be implemented using commercially available components to allow incorporation, as appropriate, of new developments in technology. Except for normal Tracking and Data Acquisition (TDA) services and navigation functions, the ground system will be developed by the project utilizing the multimission elements of the Space Flight Operations Center (SFOC) where appropriate.

III. SCHEDULE

See Figure I

IV. COST

The JPL MGC0 Development Project cost in real year dollars is \$265.0M including reserve. Headquarters contingency, Allowance for Program Adjustment, and Contract Administration are not included. This estimate is based on the implementation as proposed at the Cost Review of July 1983 and is dependent upon the use of a production line, Earth-orbiting spacecraft bus adapted for this mission.

The development cost spread by Fiscal Year is as follows:

	<u>FY</u>	<u>85</u>	<u>86</u>	<u>87</u>	<u>88</u>	<u>89</u>	<u>90</u>	<u>TOTAL</u>
COST (RY \$M)		6	29	45	63	72	50	265

For reference, the development cost in FY 1985 \$ as presented at the Cost Review is as follows:

	<u>FY</u>	<u>85</u>	<u>86</u>	<u>87</u>	<u>88</u>	<u>89</u>	<u>90</u>	<u>TOTAL</u>
COST (FY'85 \$M))		6	27	39	51	54	35	212

Costs required for pre-project efforts in FY 1983 have been estimated at \$2.5M to cover:

- key staff positions
- preparation of requirements
- preparation of RFP for the spacecraft bus
- proposal evaluation
- preparation of Project Plan
- preparation of Implementation Plan
- generating guidelines for cost estimating
- support new start process

V. IMPLEMENTATION MODE

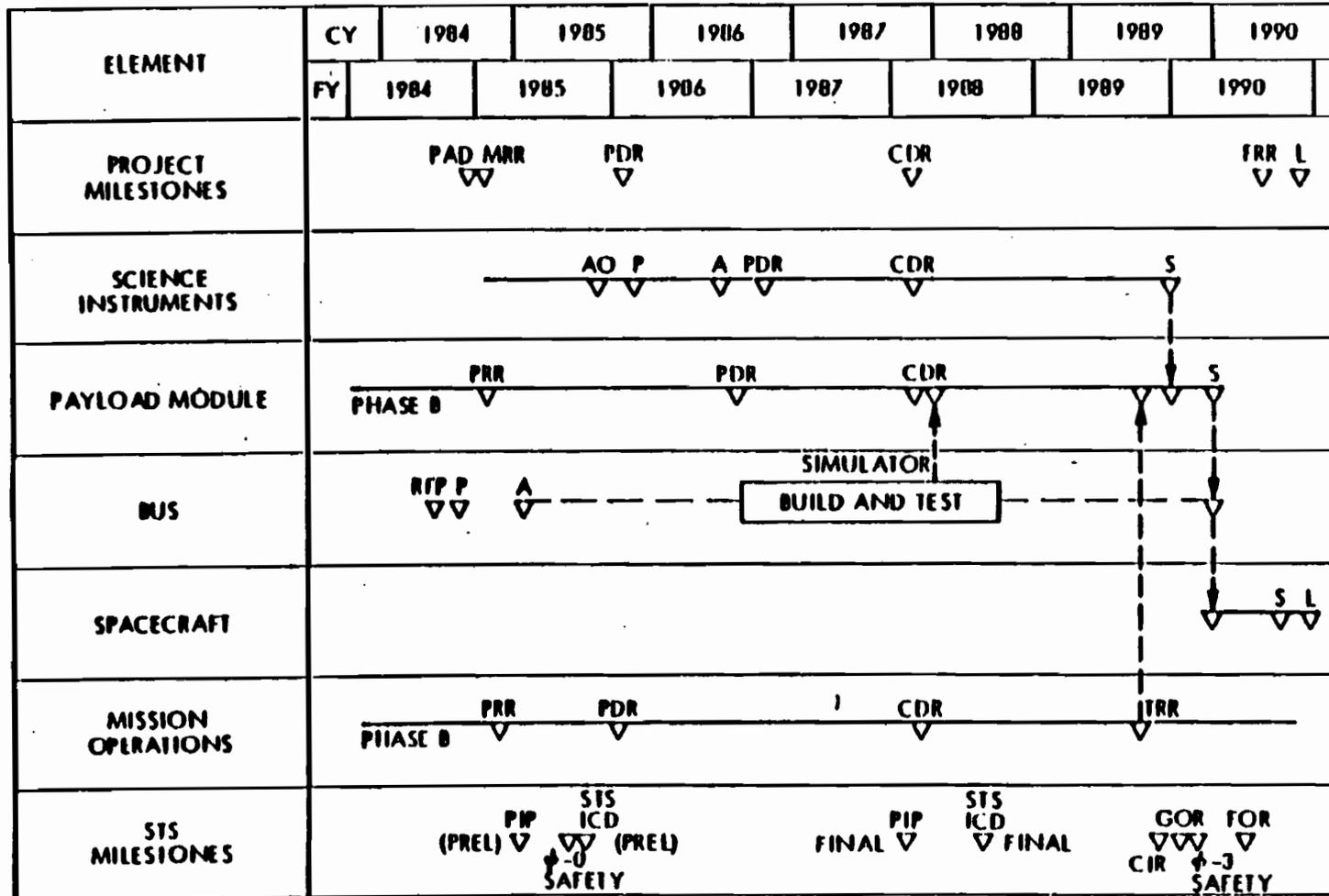
The Jet Propulsion Laboratory is responsible for the management of the Project, the design and implementation of the payload module including the acquisition and integration of the science instruments, the mission design, and the mission operations. A contractor will be selected who will be responsible for the build and test of an Earth-orbiting design spacecraft bus modified for the mission, the integration of the payload module with the spacecraft bus, and its integration into the STS. The science instruments will be supplied by Principle Investigators selected through the Announcement of Opportunity process.

VI. SPECIAL CONSIDERATIONS

The project may include in the RFP a provision for the acquisition of two or more spacecraft buses. If the multiple buy concept proves to be cost effective and practical, then the same bus may be used for subsequent Planetary Observer missions.



Mars Geoscience/Climatology Orbiter Project PROJECT SCHEDULE



LAUNCH
AUGUST 1990

 ARRIVE AT MARS
AUGUST 1991

 END OF MISSION
JULY 1993

 END OF PROJECT
FEBRUARY 1994

A - AWARD
 L - LAUNCH
 S - SHIP
 P - PROPOSALS

PAD - PROJECT APPROVAL DOCUMENT
 PDR - PRELIMINARY DESIGN REVIEW
 CDR - CRITICAL DESIGN REVIEW
 RFP - REQUEST FOR PROPOSAL
 FRR - FLIGHT READINESS REVIEW
 PRR - PRELIMINARY REQUIREMENTS REVIEW

MRR - MISSION REQUIREMENTS REVIEW
 TRR - TEST READINESS REVIEW
 CIR - CARGO INTEGRATION REVIEW
 PIP - PAYLOAD INTEGRATION REVIEW
 FOR - FLIGHT OPERATIONS REVIEW
 GOR - GROUND OPERATIONS REVIEW

Figure 1

C-10

APPENDIX D
JPL CONTRACT TASK ORDER

TRIPPLICATE

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION TASK ORDER (Or Task Order Amendment)		PAGE NO. 1	NO OF PAGES 4
CONTRACT NO. NAS7-918	TASK ORDER NO. RE-223	AMENDMENT NO. BASIC	CHANGE NO.
TO: (Contractor's name and address) CALIFORNIA INSTITUTE OF TECHNOLOGY Jet Propulsion Laboratory 4800 Oak Grove Drive Pasadena, California 91109		ISSUED BY: NATIONAL AERONAUTICS AND SPACE ADMINISTRATION NASA Resident Office - JPL 4800 Oak Grove Drive Pasadena, California 91109	

Research and Development:
 Research and Program Management

PROJECT: **MARS OBSERVER (OSSA)**

Basic Task Order
 The above numbered Task Order is modified as follows:

1. SCOPE OF WORK

a. The Contractor shall perform the work relating to the project designated Mars Observer as more particularly described below.

b. Objectives

The objectives of the Mars Observer Project are to:

- (1) Determine the global, elemental and mineralogical character of the surface material.
- (2) Define globally the topography and gravitational field.
- (3) Establish the nature of the magnetic field.
- (4) Determine the time and space distribution, abundance, sources, and sinks of volatile material and dust over a seasonal cycle.
- (5) Explore the structure and aspects of the circulation of the atmosphere.

This mission will provide new observations of Mars, not feasible from Earth or Earth-orbit, which will extend and complement existing data and provide an improved basis for future intensive exploration. The mission will be accomplished with a single spacecraft to be launched in 1990. Science data will be obtained from a near-circular sun synchronous orbit at Mars.

Except as hereby modified, all terms and conditions of said Task Order as heretofore modified remain unchanged and in full force and effect (if an Amendment).

OCT 16 1984

DATE _____

UNITED STATES OF AMERICA

BY

Peter M. Tackney
 SIGNATURE OF CONTRACTING OFFICER
 PETER M. TACKNEY

035

TYPED NAME OF CONTRACTING OFFICER

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
TASK ORDER, TASK AGREEMENT

(Or Amendment)
(Continuation Sheet)

CONTRACT NO. NAS7- 918

TASK ORDER NO. RE-223
 TASK AGREEMENT NO. _____
 AMENDMENT NO. BASIC
 CHANGE NO. _____

c. Technical Direction and Guidance

The Contractor shall be responsible to the Associate Administrator, Office of Space Science and Applications, NASA Headquarters, for the execution of work under this Task Order. The NASA Mars Observer Program Manager or his designated alternate will furnish the overall technical direction and guidance contemplated by ARTICLE 1(d) of Contract NAS7-918. Technical direction and guidance shall be furnished within the general scope of the applicable approved Project Plan, as it may be amended from time to time, and within the limitations of funds allotted to this Task Order.

d. Technical Plan

The Contractor will be responsible for the management of the Mars Observer Project; acquisition of the science instruments; design of the payload data system, x-band transponder, and command detector unit; mission design and mission operations; and will subcontract with industry, as appropriate, for the design, development, manufacture and test of the spacecraft bus, the Mars orbit insertion capability and the injection stage. These elements plus the Contractor supplied payload data system, the x-band transponder, and the command detector unit comprise the flight system. The subcontractor will support mission design, support mission operations and integrate the flight system with the Space Transportation System under the overall direction of the Contractor. The Contractor may elect to utilize a NASA Center for supplying the injection stage and for integrating the flight system with the Space Transportation System.

This work shall be carried out in accordance with the approved Project Plan, to meet objectives set forth in paragraph 1.b. above.

e. Reliability and Quality Assurance

The Contractor shall exert its best efforts to achieve the maximum level of reliability that is consistent with effective application of available resources. Particular emphasis shall be given to developing a simple, conservative and test verifiable design, the utilization of redundancy where a sufficient increase in reliability can be demonstrated, and a complete and integrated program of component, subsystem, and system testing to ensure mission success. Consistent with the approved Project Plan, the Contractor shall establish and manage reliability and quality assurance programs within its organization and at its subcontractors as necessary to satisfy overall mission requirements by selecting appropriate provisions from NASA Reliability Publications NHB 5300.4(1A) dated April, 1970, entitled "Reliability Program Provisions for Aeronautical and Space System Contractors;" NHB 5300.4 (2B) dated November, 1971, entitled "Quality Assurance Provisions for Government Agencies;" NHB 5300.4 (1B) dated April, 1969, entitled "Quality Program Provisions for Aeronautical and Space System Contractors" NHB 5300.4 (1C) dated July, 1971, entitled "Inspection System Provisions for Aeronautical and Space System

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
TASK ORDER, TASK AGREEMENT

(Or Amendment)
(Continuation Sheet)

CONTRACT NO. NAS7- 918

TASK ORDER NO. RE-223
 TASK AGREEMENT NO. _____
 AMENDMENT NO. Basic
 CHANGE NO. _____

Materials, Parts, Components and Services;" and NHB 5300.4 (3A-1) dated December, 1976, entitled "Requirements for Soldered Electrical Connections." Quality delegations, as required, to other Government Agencies will be formulated and assigned as detailed in NASA Quality Publication NHB 5330.7 dated April, 1966, entitled "Management of Government Quality Assurance Functions for Supplier Operations." Applicable provisions of these publications shall be included contractually in subcontracts and in delegations to Government Agencies as necessary to ensure compliance with Project requirements as indicated by the Project Plan.

f. Reporting

The format and frequency of reporting to NASA will be subject to the approval of the Director, Solar System Exploration, OSSA. Reporting will include the following:

- (1) Reporting categories will be selected in a manner which will permit integrated time-cost management control and reporting and will be based upon the approved Mars Observer Work Breakdown Structure. Contractor workforce shall be included in the monthly OSSA Project Management Reports. Actual and projected workforce shall be reported at an agreed upon level of the approved Work Breakdown Structure.
- (2) Financial reporting by the Contractor shall be against the code number, to the Program/Project and System level, prescribed in the NASA Agency-Wide Coding Structure. The Contractor shall apply the provisions of the NASA Contractor Financial Management Reporting System (including NASA Form 533 reporting) to cost-type subcontracts, price redeterminable subcontracts, and fixed-price incentive subcontracts (where cost considerations are involved) as appropriate, which it places pursuant to this Task Order.
- (3) The Contracting Officer may require, and the Contractor shall provide workforce plans and utilization reports, such as those to be included in Program Operating Plans, Monthly Workforce Reports or other reports in such form and at such frequency as may be specified by the Contracting Officer.
- (4) In the Program Operating Plan submitted by the Contractor for approval, the Contractor's estimate of costs of performing the work hereunder shall be shown against the approved Work Breakdown Structure.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
 TASK ORDER, TASK AGREEMENT
 (Or Amendment)
 (Continuation Sheet)

CONTRACT NO. NAS7- 918

TASK ORDER NO. RE-223
 TASK AGREEMENT NO. _____
 AMENDMENT NO. BASIC
 CHANGE NO. _____

2. RESOURCES

a. Estimated-Cost

The estimated cost of performing the work hereunder will be the estimated cost shown on the current approved Program Operating Plan, (i.e., the sum of the total amounts shown thereon for the fiscal years of the term of the project), less the amounts for periods subsequent to the terminal date of Contract NAS7-918.

b. Amount Allotted

The total sum allotted for the performance of work hereunder is \$2,000,000.00.

c. Accounting and Appropriation Data:

Fiscal Year	NASA Code		Amount	Appropriation Amount
	Program Use	Fiscal Use		
MGCO 1985	838-00-00-00-00 12208/08001	55-5-00-4-251	\$2,000,000.00	805/60108
	TOTAL ALL CODES		\$2,000,000.00	

3. PERIOD OF PERFORMANCE

a. The Contractor shall perform the work specified in this Task Order from the date of this Task Order and exert its best efforts to complete this project in accordance with the requirements of this Task Order.

b. It is estimated that the amount allotted will be exhausted on or about January 31, 1985.

4. PROJECT MANAGEMENT

The Contractor shall perform for this Project the functions of Project Manager as set forth in applicable NASA Management Issuances, and as specifically defined in the Project Plan approved by the Office of Space Science and Applications, NASA Headquarters.

5. APPLICABLE CONTRACT PROVISIONS

This Task Order is issued pursuant to paragraph (a)(1) of Article 1 of Contract NAS7-918. Except as may be otherwise provided herein, all the terms and conditions of Contract NAS7-918, as amended, shall apply to this Task Order.

Ancillary Information - Establishes new Task Order for the Mars Observer project. Initial FY 1985 resources authority and funds made available by NASA form 506A issued by OSSA under Serial No. 85/18 dated October 1, 1984.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION TASK ORDER (Or Task Order Amendment)		PAGE NO.	NO. OF PAGES
		1	2

CONTRACT NO. NAS7-918	TASK ORDER NO. RE-223	AMENDMENT NO. 28
		CHANGE NO.

TO: (Contractor's name and address) CALIFORNIA INSTITUTE OF TECHNOLOGY Jet Propulsion Laboratory 4800 Oak Grove Drive Pasadena, California 91108	ISSUED BY: NATIONAL AERONAUTICS AND SPACE ADMINISTRATION NASA Resident Office - JPL 4800 Oak Grove Drive Pasadena, California 91108
--	---

Research and Development
 Research and Program Management

PROJECT: MARS OBSERVER (OSSA)

Basic Task Order
 The above numbered Task Order is modified as follows:

- Paragraph 1., Scope of Work, subparagraph b., Objectives, the second paragraph is revised to change the launch date from 1990 to 1992.
- The estimated amount, as shown in subparagraph 2.a., is increased by the amount of \$1,082,000.00 from \$101,228,861.00 to \$102,310,861.00.
- The amount allotted, as shown in subparagraph 2.b., is increased by the amount of \$1,082,000.00 from \$101,228,861.00 to \$102,310,861.00.
- Subparagraph 2.c., Accounting and Appropriation Data, is revised to the following extent shown below:

Fiscal Year	NASA Code Program Use	Fiscal Use	Increase Amount	Revised Amount	Appropriation Number
<u>SOLAR SYSTEM EXPLORATION</u>					
<u>Mars Observer</u>					
1988	838-10-00-00-00	55-8-00-4-251	\$ 1,082,000.00	\$ 40,293,400.00	808/90108
TOTAL CODE 838-10				\$ 97,186,861.00	
TOTAL INCREASE			\$ 1,082,000.00		
TOTAL ALL CODES				\$102,310,861.00	

For NASA Use Only: PPC-SE, Station No. 55, Funding Action.

- Paragraph 3., PERIOD OF PERFORMANCE, subparagraph b. is revised as follows:
 - It is estimated that the funds allotted for work will be exhausted on or about September 12, 1988.

Except as hereby modified, all terms and conditions of said Task Order as heretofore modified remain unchanged and in full force and effect (if an Amendment).

DATE _____	UNITED STATES OF AMERICA BY <u>Allen T. Burke</u> SIGNATURE OF CONTRACTING OFFICER <u>Allen T. Burke</u> 859 TYPED NAME OF CONTRACTING OFFICER
AUG 9 1988	

APPENDIX E
ISA FOR LOSS OF SIGNAL

INITIATION	1. INITIATOR RICK MURPHY	ORGANIZATION MO SET	EXTENSION 3-5970	MAIL 264-550	INITIATION DATE MO 8 DAY 21 YEAR 93	2. INCIDENT REPORTED TO: S. DALLAS	PAGE 1 of 1					
	3. PROJECT MO	SC ID. 94	4. TIME OF INCIDENT (MM/TT/CC) AT 234 HOUR 00 MIN 54 SEC ---	5. OBSERVATION LOCATION: <input type="checkbox"/> JPL 230 <input checked="" type="checkbox"/> JPL 264 <input type="checkbox"/> JPL 8AF <input type="checkbox"/> KSC <input type="checkbox"/> OTHER	6. MISSION ACTIVITY: <input type="checkbox"/> MOB TEST <input type="checkbox"/> GDS TEST <input type="checkbox"/> LAUNCH <input type="checkbox"/> CRUISE <input checked="" type="checkbox"/> ENCOUNTER <input type="checkbox"/> OTHER	7. SUSPECT PROBLEM AREA: <input type="checkbox"/> SPOF <input type="checkbox"/> MOCF <input type="checkbox"/> IPC <input type="checkbox"/> NOCC <input type="checkbox"/> S/C <input type="checkbox"/> MPSB <input type="checkbox"/> MPSF <input type="checkbox"/> DIS <input type="checkbox"/> GCF <input type="checkbox"/> OTHER	8. SUSPECT CAUSE CATEGORY: <input type="checkbox"/> S/C HARDWARE <input type="checkbox"/> GND HARDWARE <input type="checkbox"/> PROCEDURES <input checked="" type="checkbox"/> UNKNOWN <input type="checkbox"/> S/C SOFTWARE <input type="checkbox"/> GND SOFTWARE <input type="checkbox"/> DOCUMENTATION <input type="checkbox"/> OTHER					
ACTION STATUS	9. (A) DESCRIPTION OF INCIDENT: (B) REAL TIME CHECKS / ANALYSES: (C) REAL TIME CORRECTIVE ACTIONS: (a) SPACECRAFT DOWNLINK WAS NOT REACQUIRED AFTER BITPROP TANK PRESSURIZATION. (b) NORMAL DSN/MCT/SCT PROCEDURES EFFECTED FOR 'NO DOWNLINK CONDITION' WITH NO SUCCESS. MOS ANALYSIS AND RECOMMENDING IN PROGRESS (c) NONE	9. (A) MISSION OPERATIONS IMPACT ASSESSMENT MOR LEVEL: <input checked="" type="checkbox"/> MAJOR <input type="checkbox"/> SIGNIFICANT <input type="checkbox"/> MINOR	9. (B) CORRECTION REQ'D BY - DATE OR ACTIVITY	10. MOR <input checked="" type="checkbox"/> MAJOR <input type="checkbox"/> SIGNIFICANT <input type="checkbox"/> MINOR	11. MISSION APPLICABILITY <input type="checkbox"/> LAUNCH <input checked="" type="checkbox"/> CRUISE <input checked="" type="checkbox"/> ENCOUNTER	12. CORRECTION REQUIRED DATE	13. ACTION ASSIGNMENT INDIVIDUAL: (1) Durham (2) _____ (3) _____	ORGANIZATION: SCT	DATE: 8/22/93			
	ACTION ANALYSES / CORRECTION / VERIFICATION	14. CAUSE CATEGORY <input type="checkbox"/> S/C HARDWARE <input type="checkbox"/> GND HARDWARE <input type="checkbox"/> PROCEDURES <input type="checkbox"/> UNKNOWN <input type="checkbox"/> S/C SOFTWARE <input type="checkbox"/> GND SOFTWARE <input type="checkbox"/> DOCUMENTATION <input type="checkbox"/> OTHER	15. COMMAND RELATED <input type="checkbox"/> YES <input type="checkbox"/> NO	16. SEP <input type="checkbox"/> YES <input type="checkbox"/> NO	17. (A) ANALYSES, (B) CORRECTIVE ACTIONS, AND (C) CORRECTION VERIFICATION (EACH SEPARATE ENTRY MUST BE IDENTIFIED BY NAME AND DATE)	18. FOLLOW UP ACTIONS/ DOCUMENTS <input type="checkbox"/> SIC PFR NO. _____ <input type="checkbox"/> ISA NO. _____ <input type="checkbox"/> MOCF PFR NO. _____ <input type="checkbox"/> DSN DR NO. _____	19. ACTION RESPONSIBLE ORG ^W _____ DATE _____	20. TEAM CHIEF _____ DATE _____	21. PROJECT ICAC _____ DATE _____	22. OFFICE MGR. _____ DATE _____	23. MOAM _____ DATE _____	24. CAUSE CODE _____
APPROVALS		CONCURRENCES	CLOSE OUT	26. CAUSE CODE	25. FAILURE EFFECT. RSK RATING							

APPENDIX F
MISHAP REPORT

NO. 09219
 MASTER FILE NO.

MISHAP REPORT

(See Instructions on Reverse Side of Yellow Part 2)

NOTE: Fill in unshaded blocks within one working day. Please print or type. Fill out reverse side of this sheet.

GENERAL INFORMATION

1. NAME OF ORGANIZATION JPL		2. MISHAP DATE (MDY) 8/21/93		3. MISHAP TIME (24 Hrs) 17:54		4. ORG FILE NO. 2500-0001-93					
5. MISHAP CATEGORY (Check as appropriate)				6. CLOSE CALL		7. LEVEL OF POTENTIAL					
TYPE A 1 <input type="checkbox"/> DEATH 2 <input type="checkbox"/> LOST TIME 3 <input type="checkbox"/> INJURY 4 <input type="checkbox"/> INJURY 5 <input type="checkbox"/> DAMAGE 6 <input checked="" type="checkbox"/> DAMAGE 7 <input type="checkbox"/> TEST FAILURE 8 <input type="checkbox"/> TEST FAILURE				TYPE B 2 <input type="checkbox"/> LOST TIME 3 <input type="checkbox"/> PERM DISABILITY 4 <input type="checkbox"/> INJURY 5 <input type="checkbox"/> HOSPITALIZATION 6 <input type="checkbox"/> DAMAGE 7 <input type="checkbox"/> TEST FAILURE				TYPE C 2 <input type="checkbox"/> LOST TIME 4 <input type="checkbox"/> INJURY 6 <input type="checkbox"/> DAMAGE 7 <input type="checkbox"/> TEST FAILURE		INCIDENT 4 <input type="checkbox"/> INJURY 6 <input type="checkbox"/> DAMAGE MISSION FAILURE <input checked="" type="checkbox"/>	
				9. SPECIFIC AREA Mars Observer		11. PROGRAM IMPACT Loss of Mission					
12. DESCRIPTION OF MISHAP (Sequence of events, extent of damage and injuries, cause, if known, etc. Use additional sheets, if necessary.) Spacecraft downlink was not reacquired after BIPROP tank pressurization, (ISA 3813 Attached), prior to planned Mars Orbit Insertion.											

PERSONNEL INVOLVED

13. NAME (Last, first, middle initial)		14. AGE		15. SEX <input type="checkbox"/> M <input type="checkbox"/> F		16. SECTION / JOB TITLE	
17. SHIFT WORKED <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3		18. HOURS OF CONTINUOUS DUTY BEFORE MISHAP		19. FIRST AID ONLY <input type="checkbox"/> YES <input type="checkbox"/> NO		20. FATALITY <input type="checkbox"/> YES <input type="checkbox"/> NO	
21. INJURY TYPE (Codes)		22. BODY PART(S) AFFECTED (Codes)		23. DAYS LOST NO. <input type="checkbox"/> TOTAL <input type="checkbox"/> CONTINUING		24. CAUSE (S) OF DAMAGE (Codes) PRIMARY CONTRIB. POTENTIAL	
				25. MISHAP-ENVIRONMENT (Codes) AGENT ACTIVITY			
26. HAS EMPLOYEE RECEIVED TRAINING / CERTIFICATION APPLICABLE TO TASK? <input type="checkbox"/> YES <input type="checkbox"/> NO							

EQUIPMENT / PROPERTY DAMAGED

27. CLASS OF EQUIPMENT / PROPERTY DAMAGED 1 <input checked="" type="checkbox"/> FLIGHT HARDWARE 2 <input type="checkbox"/> GROUND SUPPORT EQUIPMENT (GSE) 3 <input type="checkbox"/> FACILITY				28. SPECIFIC ITEM DAMAGED Mars Observer Spacecraft			
29. SERIAL / NEWS NO.				30. SYSTEM / SUBSYSTEM AFFECTED			
		31. CAUSE (S) OF DAMAGE (Codes) PRIMARY CONTRIB. POTENTIAL		32. COST ESTIMATE \$ 250M FINAL \$			
33. SUBMITTED BY (Name, title, mail code) Glenn E. Cunningham, Project Manager 264-627		SIGNATURE <i>Glenn E. Cunningham</i>		PHONE NO. (818)354-5319		DATE 09/01/93	

CORRECTIVE ACTION

34. ACTION PLAN (Describe Corrective Action to be taken, including completion dates and names of personnel and organizations responsible for correction. Use extra sheets, if necessary.)

35. CONTRACT NUMBER

35. SECTION APPROVAL (Name, title, mail code)	SIGNATURE	PHONE NO.	DATE
---	-----------	-----------	------

36. JPL MANAGEMENT CONCURRENCE WITH CORRECTIVE ACTION PLAN

DIVISION APPROVAL (Name, title, mail code)	SIGNATURE	PHONE NO.	DATE
--	-----------	-----------	------

OCCUPATIONAL SAFETY OFFICE USE ONLY

37. LESSONS LEARNED <input type="checkbox"/> YES <input type="checkbox"/> NO	REF. NO. (if Yes)	APPROVAL FOR CLOSURE
38. TYPE OF INVESTIGATION <input type="checkbox"/> BOARD <input type="checkbox"/> TEAM <input type="checkbox"/> INVESTIGATOR	NAME AND TITLE	
39. STATUS <input type="checkbox"/> OPEN <input type="checkbox"/> CLOSED	SIGNATURE	DATE

OCCUPATIONAL SAFETY OFFICE

JPL 0554-S R 6/90

APPENDIX G

CAUSAL FACTOR: PYRO SHOCK

I. Description of Threat

Environment Description

Mechanically transmitted pyro shock was induced on Mars Observer by firing the spacecraft V-band separator, the Solar Array pyros, the HGA pyros, the GRS pyros, the Magnetometer pyros, and the pyro valves in the Propulsion Subsystem. A summary of the Mars Observer system test pyro firing sequence and flight pyro firing sequence is presented in Tables G-1 and G-2. System test pyro events are listed in Table G-1 by subsystem and approximate date of the test firings. Mars Observer system pyro firings were performed at times in the Integration and Test schedule that Astro deemed most convenient and did not match the order of the flight firings. Pyros were fired in the system test by the flight pyro system using test software and ground power. Test pyro valve 5 was fired followed by pyro valve 8, then they were reinstalled, but it is not clear that a second firing occurred (they were to be fired three times). System test shock responses at equipment panel assemblies as induced by specific test pyro firings are presented in Table G-2 for information only.

Critical Hardware

RXO, RPAs, RF switch S2, MOTs, EDF (Engineering Data Formatter), SCU (Signal Conditioning Unit), PRAs, and SCP are known to be sensitive to shock. None of these assemblies, except the PRAs and the SCU, were shock tested at the assembly level. The other sensitive assemblies were accepted by heritage even though there were, in some cases, design changes which affected sensitivity. Only an analysis was done to qualify TWT design changes. The hardware considered critical for the loss of signal anomaly are the RPAs, RF output switch S2, LGA waveguide, and RXO.

Relationship to Environmental Threat

The assemblies listed above are mounted to Mars Observer bus equipment panels and were subject to shock induced by the spacecraft pyro firing events. The Solar Array pyros and HGA pyros appear to have more direct shock paths to the equipment panels than the GRS pyros, Magnetometer pyros or the pyro valves. However, one of the low-pressure line pyro valves is directly above one of the bus vertical bulkheads and has a direct in-plane path to the RPA and RF switch equipment panel.

Test Fallacies

The Mars Observer test pyro valves were attached to the nadir panel with the same nylon ties and standoffs as the flight valves. However, the propulsion line shock transmission path was not included in the test. This also caused a reduced tie stiffness (factor of 4) which may have reduced the pyro valve shock transmitted to the bus panels. There was a large variability in the Mars Observer pyro shock response data, especially from the test pyro valve firings. Also, a large proportion of the Mars Observer pyro firing data was in or near the data system noise floor at the equipment panels, leaving questions about the data system sensitivity settings. About 5 percent of the pyro valve shock data, in particular, was considered good data. Finally, most Mars Observer system test pyros were fired only once (in a non-flight order), and there was a high possibility that flight shock responses exceeded the test firing environment.

II. Method of Investigation

Mars Observer pyro devices were fired as described in Tables G-1 and G-2 to provide at least one exposure of sensitive equipment to pyro shock environments. The test shock response levels did not necessarily represent the actual flight environment since much of the data was questionable and because the set of Mars Observer test pyros fired is small statistically (only 1 firing for most pyros). Industry experience shows that the shock induced by multiple pyro firings at a single location can vary as much as 6 dB.

A pyro firing test with the Mars Observer spare bus is being planned to eliminate the questions left by the pre-launch pyro valve firing test. The test setup will include the spare primary structure, including the central cylinder, bulkheads, zenith, nadir, and all equipment panels with flight-like interconnections. It will also include a He pressure supply, pyro valves (high and low pressure), regulator, pressure transducers, service valves, and the pressure line up to, but not including, the check valves. High-quality shock data will be taken at sensitive equipment locations, including the RPAs, RF output switch S2, LGA waveguide, and RXO. The recommended test plan configuration also includes having the above sensitive equipment mounted in the flight configuration. The presence of the sensitive equipment is critical to the test objective of determining shock-induced damage to these assemblies. Three firings of the pressure line pyro valves (primary and backup) are recommended to form the minimum acceptable statistical data set.

III. Results of Investigation

Results of the Mars Observer spare bus pyro shock test were unavailable at press time. Results of the investigation will be supplied after the Mars Observer spare bus pyro shock test.

Table G-1. Mars Observer system pyro test firing events, listed by approximate firing order and date.

Spacecraft Separator, V-Band		Anti Vel Sun Panel	Vel Sun Panel	Anti Vel Space Panel	Vel Space Panel	Vel Space Panel	Location As Noted
Date 4/17/92		RXO			RPA's	RF S2 Switch	RWA
Pyro Set # 1	Primary	52 gpk, 1Y	No Data	63 gpk, 1Y	No Data	No Data	183 gpk, Cylinder 1Y
Magnetometer Boom Deployment, Cable Cutter							
Date 4/18/92		RXO	Vel Sun Panel	Anti Vel Space Panel	RPA's	RF S2 Switch	RWA
Boom Deployment Pyro	Primary	117gpk, 3Y Note 1	No Data	Bad Data	No Data	No Data	Bad Data
HGA Deployment, Cable Cutter							
Date 4/18-26/92		RXO	Vel Sun Panel	Anti Vel Space Panel	RPA's	RF S2 Switch	RWA
-X Support Release 4/18	Primary	No Data	No Data	1700gpk,3Y clipped	64gpk,5Y Note 1	64gpk,5Y Note 1	68 gpk, Cylinder 1Y
+X Support Release	Primary	No Data	No Data	Bad Data	No Data	No Data	No Data
Antenna Frame Release 4/23	Primary	No Data	No Data	Bad Data	64 gpk,5Y Note 1	55 gpk, 1Y	366 gpk, Zenith Panel 4Z
Antenna Frame Release 4/26	Primary	No Data	No Data	Bad Data	Bad Data	Bad Data	171 gpk, Zenith Panel 4Z
Gimbal Bracket Release 4/23	Primary	No Data	No Data	Bad Data	30gpk, 1Y Note 1	30 gpk, 1Y	219 gpk, Zenith Panel 4Z
Gimbal Bracket Release 4/26	Primary	No Data	No Data	Bad Data	No Data	Bad Data	107 gpk, Zenith Panel 4Z
Wrist Hinge	Primary	No Data	No Data	No Data	No Data	No Data	No Data
Propulsion Pyro Valve, Pyro Valve							
Date 4/22 & 23/92		RXO	Vel Sun Panel	Anti Vel Space Panel	RPA's	RF S2 Switch	RWA
Test HP Pyro Valve, Firing 1	4/22	Bad Data	Bad Data	Bad Data	No Data	Bad Data	Bad Data
Test LP Pyro Valve, Firing 1	4/22	No Data	Bad Data	Bad Data	No Data	Bad Data	Bad Data
Test HP Pyro Valve, Firing 2	Questionable Firing	4.7 gpk, 1Y *	No Data	No Data	No Data	No Data	No Data
Test LP Pyro Valve, Firing 2	Questionable Firing	Bad Data	Bad Data	5.4 gpk, 1Y *	No Data	Bad Data	Bad Data
GRS Deployment, Cable Cutter							
Date 4/23,27/92		RXO	Vel Sun Panel	Anti Vel Space Panel	RPA's	RF S2 Switch	RWA
GRS # 2 Support 4/23	Primary	5 gpk, 1Y	69 gpk, 2Y	Bad Data	32 gpk,1Y Note 1	32 gpk, 1Y	82 gpk, Zenith Panel 5Z
GRS # 3 Support 4/23	Primary	9 gpk, 1Y	105 gpk, 2Y	4 gpk, 1Y	54 gpk,1Y Note 1	54 gpk, 1Y	107 gpk, Zenith Panel 5Z
GRS # 1 Support 4/23	Primary	13 gpk, 1Y	73 gpk, 2Y	4 gpk, 1Y	13 gpk,1Y Note 1	13 gpk, 1Y	135 gpk, Zenith Panel 5Z
GRS # 4 Support 4/27	Primary	6 gpk, 1Y	65 gpk, 2Y	6 gpk, 1Y	66 gpk,4Y Note 1	10 gpk, 1Y	85 gpk, Zenith Panel 5Z
Solar Array Deployment, Cable Cutter							
Date 4/23,29/92		RXO	Vel Sun Panel	Anti Vel Space Panel	RPA's	RF S2 Switch	RWA, Anti Vel Sun
Solar Array Inner Tie #1,4/28	Primary	No Data	No Data	No Data	No Data	No Data	No Data
Solar Array Inner Tie #3,4/28	Primary	No Data	No Data	No Data	No Data	No Data	No Data
Solar Array Inner Tie #2,4/28	Primary	No Data	No Data	No Data	No Data	No Data	No Data
Solar Array Inner Tie #4,4/28	Primary	No Data	No Data	No Data	No Data	No Data	No Data
Solar Array Outer Tie #1,4/28	Primary	No Data	No Data	No Data	No Data	No Data	No Data
Solar Array Outer Tie #3,4/28	Primary	No Data	No Data	No Data	No Data	No Data	No Data
Solar Array Outer Tie #2,4/28	Primary	No Data	No Data	No Data	No Data	No Data	No Data
Solar Array Outer Tie #4,4/28	Primary	No Data	No Data	No Data	No Data	No Data	No Data
Solar Array Shear Tie #9,4/29	Primary	65 gpk,1Y Note 2	149 gpk, 1Y	No Data	No Data	No Data	231 gpk,4Y Note 1
Solar Array Shear Tie #9,4/29	Primary, fire # 2	58gpk,4Y Note 1	62 gpk, 1X	No Data	No Data	No Data	58 gpk,4Y Note 1
Note 1: Data bad, available data from same equipment panel used							
Note 2: SRS = 231 gpk at 4Y							
* Questionable data; may not represent actual flight environment							

Table G-2. Mars Observer flight pyro firing events, listed in firing order, system pyro shock response for information only.

Spacecraft Separator (Launch Script), V-Band				MO System Pyro Test Shock Response at Assemblies; reference Table 1			
Date UTC	Time UTC	Pyro Firing Order		RXO	PRA's	RF S2 Switch	RWA
9/25/92	17:20	Pyro Set # 1	Primary	52 gpk, 1Y	No Data	No Data	183 gpk, Cylinder 1Y
		Pyro Set # 2	Primary	No Data	No Data	No Data	No Data
		Pyro Set # 1	Backup	No Data	No Data	No Data	No Data
		Pyro Set # 2	Backup	No Data	No Data	No Data	No Data
Solar Array Deployment (Launch Script), Cable Cutter				MO System Pyro Test Data for Shear Tie #9 Only			
Date UTC	Time UTC	Pyro Firing Order		RXO	PRA's	RF S2 Switch	RWA
9/25/92	17:38	Solar Array Shear Tie #1, Outer	Primary	No Data	No Data	No Data	No Data
		Solar Array Shear Tie #1, Outer	Backup				
		Solar Array Shear Tie #3, Outer	Primary				
		Solar Array Shear Tie #3, Outer	Backup				
		Solar Array Shear Tie #2, Outer	Primary				
		Solar Array Shear Tie #2, Outer	Backup				
		Solar Array Shear Tie #4, Outer	Primary				
		Solar Array Shear Tie #4, Outer	Backup				
		Solar Array Shear Tie #1, Inner	Primary				
		Solar Array Shear Tie #1, Inner	Backup				
		Solar Array Shear Tie #3, Inner	Primary				
		Solar Array Shear Tie #3, Inner	Backup				
		Solar Array Shear Tie #2, Inner	Primary				
		Solar Array Shear Tie #2, Inner	Backup				
		Solar Array Shear Tie #4, Inner	Primary				
		Solar Array Shear Tie #4, Inner	Backup				
HGA Deployment (Launch Script), Cable Cutter				MO System Pyro Test Shock Response at Assemblies			
Date UTC	Time UTC	Pyro Firing Order		RXO	PRA's	RF S2 Switch	RWA
9/25/92	17:41	-X Support Release	Primary	No Data	64gpk,5Y Note2	64gpk,5Y Note2	68 gpk, Cylinder 1Y
		-X Support Release	Backup	No Data	No Data	No Data	No Data
		+X Support Release	Primary	No Data	1700 gpk, Note 1	1700 gpk, Note 1	No Data
		+X Support Release	Backup	No Data	No Data	No Data	No Data
		Antenna Frame Release	Primary	No Data	64 gpk, 5Y Note2	55 gpk, 1Y	366 gpk, Zenith Panel 4Z
		Antenna Frame Release	Backup	No Data	Bad Data	Bad Data	171 gpk, Zenith Panel 4Z
		Gimbal Bracket Release	Primary	No Data	30gpk, 1Y Note2	30gpk, 1Y	219 gpk, Zenith Panel 4Z
		Gimbal Bracket Release	Backup	No Data	No Data	Bad Data	107 gpk, Zenith Panel 4Z
GRS Deployment (Launch Script), Cable Cutter				MO System Pyro Test Shock Response at Assemblies			
Date UTC	Time UTC	Pyro Firing Order		RXO	PRA's	RF S2 Switch	RWA
9/25/92	17:43	GRS # 2 Support	Primary	5 gpk, 1Y	32 gpk, 1Y Note2	32 gpk, 1Y	82 gpk, Zenith 5Z
		GRS # 2 Support	Backup	No Data	No Data	No Data	No Data
		GRS # 3 Support	Primary	9 gpk, 1Y	54 gpk, 1Y Note1	54 gpk, 1Y	107 gpk, Zenith 5Z
		GRS # 3 Support	Backup	No Data	No Data	No Data	No Data
		GRS # 1 Support	Primary	13 gpk, 1Y	13 gpk, 1Y Note2	13 gpk, 1Y	135 gpk, Zenith 5Z
		GRS # 1 Support	Backup	No Data	No Data	No Data	No Data

G-4

Table G-2. Mars Observer flight pyro firing events, listed in firing order, system pyro shock response for information only (continued).

Magnetometer Boom Deployment (Launch Script), Cable Cutter				MO System Pyro Test Shock Response at Assemblies			
Date UTC	Time UTC	Pyro Firing Order		RXO	PRA's	RF S2 Switch	RWA
9/25/92	17:46	Boom Deployment Pyro	Primary	117 gpk,3Y Note2	No Data	No Data	Bad Data
		Boom Deployment Pyro	Backup	No Data	No Data	No Data	No Data
Propulsion Pyro Valve (Launch Script), Pyro Valve				No Data in the Flight Configuration			
Date UTC	Time UTC	Pyro Firing Order		RXO	PRA's	RF S2 Switch	RWA
8/22/93 (8/21/93 PST)	approx. 1:00	Propulsion Pyro Valve 7	Primary	No Data	No Data	No Data	No Data
		Propulsion Pyro Valve 5	Primary	No Data	No Data	No Data	No Data
	approx. 11:00	Propulsion Pyro Valve 8	Backup	No Data	No Data	No Data	No Data
		Propulsion Pyro Valve 6	Backup	No Data	No Data	No Data	No Data
UTC - Universal Greenwich Time/ Note 1: Assumes symmetry with Anti Vel Space panel./ Note 2: Bad Data, other data on same equipment panel used.							

APPENDIX H

PYRO-INDUCED FAILURE MECHANISMS IN CIU HARDWARE

I. Introduction

This Appendix discusses potential failure mechanisms in the CIU hardware that could be induced by transient currents that result when a squib is fired. The basic hypothesis is that latch-up occurs in CMOS devices in the CIU control logic that disrupts the normal operation of the subsystem in a manner that locks out potential recovery mechanisms from normal external command signals. More detailed analyses are provided.¹

In order for the proposed failure mechanism to occur, the following sequence of events must occur:

- (1) **The "high" contact of the squib must short to the case during squib firing, resulting in a short, intense pulse of current in the spacecraft ground.** Laboratory tests of a number of squib devices indicate that this occurs in about 4 percent of squib firings.
- (2) **Sufficient energy must be coupled from the transient current of the squib to circuit boards to initiate latch-up in some of the CMOS circuits.** This is the most difficult part of the proposed mechanism to assess. The hypothesized coupling mechanisms depend strongly on the geometry of wiring, ground connections, and circuit boards, and are very difficult to calculate because of the complex geometry. The estimated fraction of the transient electrical energy from the squib that must be transferred to circuit-board wiring to cause latch-up is ≈ 0.05 percent (based on experimental tests of electrically induced latch-up in CD4000-series CMOS circuits). This is a small amount of the total energy, and it is not inconceivable that this could occur. However, the various coupling mechanisms are very inefficient, and calculations of the expected magnitude of voltages and currents for simplified geometries vary over a wide range, depending on the geometrical assumptions that are used. This mechanism needs more extensive laboratory testing, because of the strong dependence on specific layout.
- (3) **Latch-up must occur in a critical circuit that will cause single-point failure in the Mars Observer circuitry.** Analysis of the CMOS logic used in Mars Observer shows that there are many points in the CIU circuitry where latch-up in a CMOS circuit would cause single-point failure. Thus, if the coupling mechanisms proposed in Step 2 can transfer sufficient energy to cause latch-up, they are likely to cause failure in the Mars Observer control circuits.

¹ T. Nguyen, *Cover Memo for Pyro Event Report*, JPL Interoffice Memorandum 5211-93-489, Jet Propulsion Laboratory, Pasadena, California, October 25, 1993.

The remaining sections of the report discuss these three steps in more detail, along with experimental evidence to support them.

II. Step 1: Squib Transient Current

One of differences between Mars Observer and other JPL spacecraft is that the Mars Observer design connects the electrical ground of logic and control subsystems directly to the external chassis. This provides a direct path between currents in the chassis and electronic circuitry. This in turn leads to the possibility that currents from the squib might interact with other circuitry in the event that the squib is inadvertently shorted to the external case. The path from the squib case to the chassis is rather complicated, and involves current flow through structures (such as the fuel tank and associated tubing) as well as through the chassis and wiring. An example is shown in Figure H-1; more detailed discussion will follow in a later section.

A number of experimental tests have been done to investigate currents from the squib after it is fired. In some cases (≈ 4 percent, based on very limited statistics) the squib shorts through the insulating cup, and a high-intensity current will then flow in the chassis ground. Figure H-2 shows a cross-sectional diagram of the squib just after it is fired. An intense plasma is created, which opens the bridge wire. The figure shows the plasma shorting through the side of the cup, which occurs in a small number of firings. Evidence for this is provided by examining squibs after firing, which sometimes show fracture through the cup.

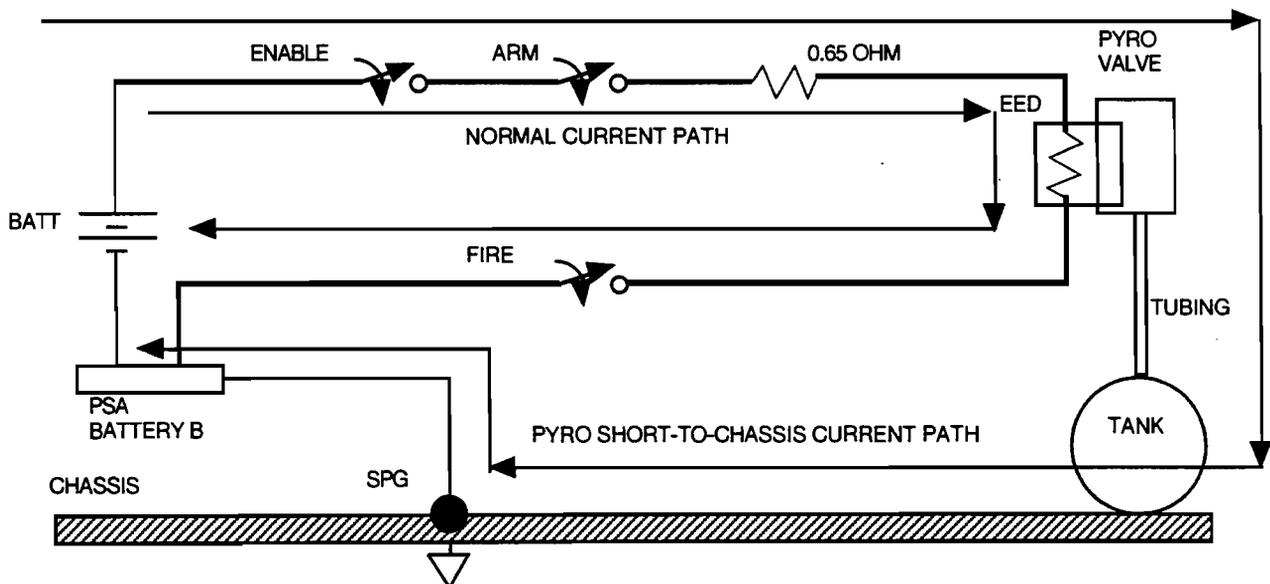


Figure H-1. Chassis current induced by pyro short.

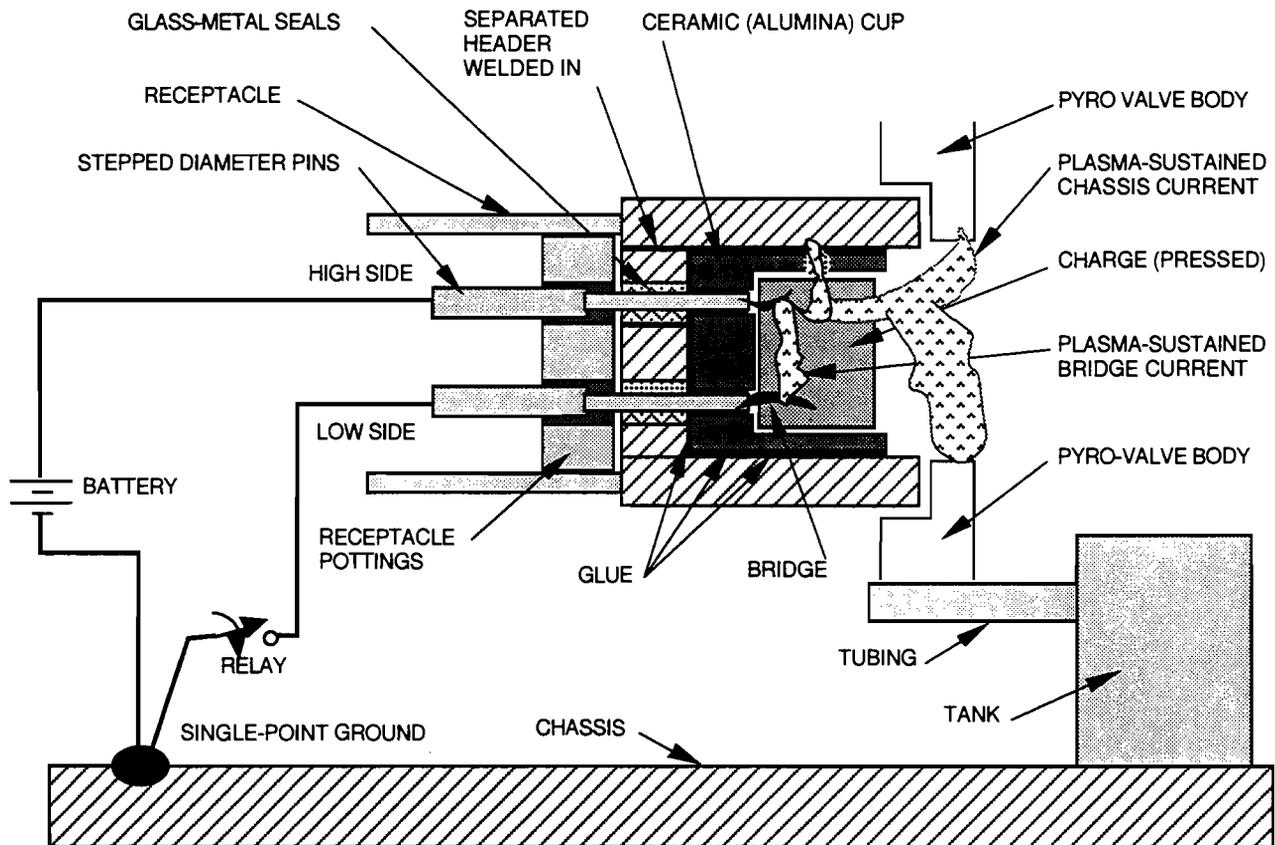


Figure H-2. A model of current flow from short in NSI induced by plasma to chassis.

Figure H-3 shows experimental measurements of chassis current during one of the cases in which the squib shorted. These measurements were obtained by firing squibs in a mockup of the Magellan system, which used the same type of squib as the Mars Observer NSI. In this example, the maximum current could not be measured, because the oscilloscope sensitivity was too high. However, analysis of the circuit shows that it should be in the range of 5–10 amperes. The pulse width of the chassis current signal is 30 μs ; the pulse width of the shield current appears to be much longer. Pulse rise times are 0.05 to 0.2 μs ; however, note that ringing will result in faster rise times in actual circuits. Assuming that the peak value is 10 A, the total charge induced in the chassis by shorting of the squib circuit is 300 μC .

The large surge of current in the chassis will cause voltage drops and ringing in the ground circuitry. Ringing will increase the risetime of the voltage in the secondary (victim) circuits compared to the measured squib currents in the chassis. It will also produce electromagnetic radiation that may be coupled to other regions of the system. If sufficient energy is coupled to circuit boards, it is possible that latch-up could be induced as a result of firing the squib. These mechanisms are discussed below, after the section on latch-up.

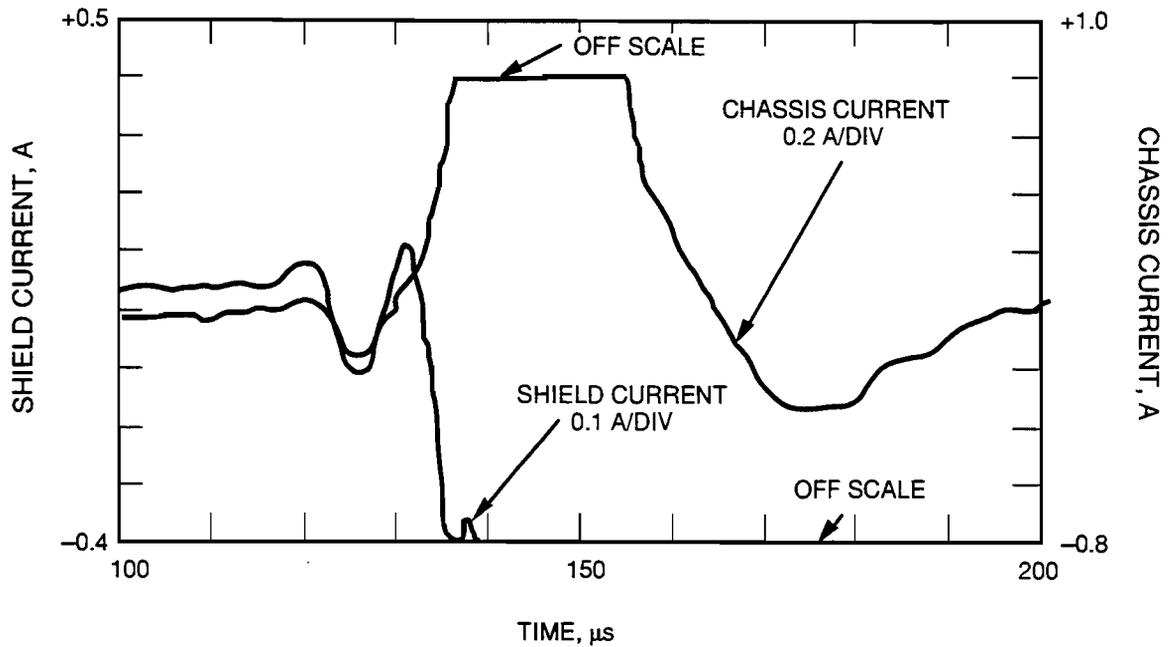


Figure H-3. Chassis and shield currents created by disruption of the squib bridge wire in laboratory simulation of Magellan hardware. Mars Observer used the same type of squib.

III. Latch-up in CD4000 Circuits

A. General Features of Latch-up

Latch-up can be induced by several different mechanisms, including radiation from heavy particles, and electrical transients at inputs, outputs, or power supplies. In this instance one is concerned with electrically induced latch-up, most likely from transients at the device input or at the power supply pin. Figure H-4 shows the current-voltage characteristics of a latchable structure, in this case the CD4049 integrated circuit. The solid symbols in this figure show the device characteristics in its normal (unlatched) state. Once latch-up occurs, the internal four-region structure enters a low-impedance "on" condition, shown by the open symbols in Figure H-4, where it functions as a very efficient switch. The internal impedance from power supply to ground is very low, and current is essentially determined by the resistance of external circuitry. Extremely high currents can occur if there is no external current limiting, which may lead to catastrophic failure from overheating. However, latch-up does not necessarily cause failure if the current is limited to moderate levels ($\approx 100\text{--}200$ mA for typical integrated circuits).

Key latch-up characteristics are as follows: (1) very high currents flow from the power supply to ground during latch-up; (2) the device remains in the latched

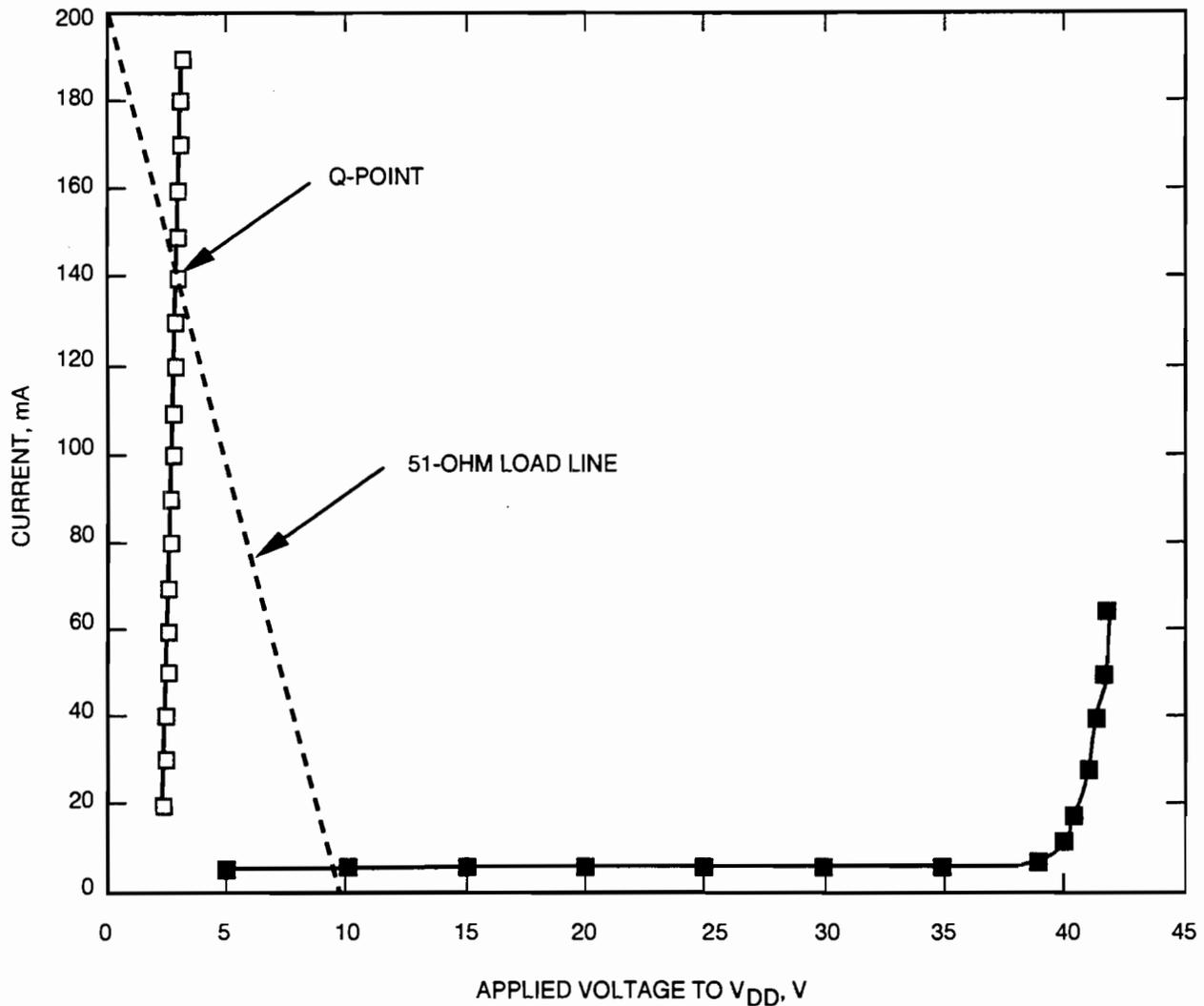


Figure H-4. Latch-up characteristics of a CD4049 inverter triggered by $V_{DD} - V_{SS}$ breakdown mechanism.

condition until it burns out from overheating, or until the power supply voltage is reduced to very low levels (<2 V); (3) the device will no longer respond to input signals after it is latched; and (4) latch-up is usually confined to a localized region, but it will affect the operation of other sections of a circuit. For example, if latch-up occurs in one section of a quad logic circuit, only the section that is latched will be nonfunctional. However, since all sections of the device share a common power supply, the supply voltage on the other three gates will be very low, which will affect their operation as well.

Manufacturers of integrated circuits are very aware of the problem of electrically induced latch-up. All modern devices are designed with special protection circuits at the input and output terminals that will prevent latch-up from occurring as long as the applied transient signals remains below certain limits.

B. Characterization of CD4000 Circuits

Extensive tests have been done to characterize latch-up in the CD4011 and CD4049 circuits. These tests were done using an ESD tester with a 1-k Ω source impedance and 150 pF storage capacitor, and also with a pulse generator. The tests showed that latch-up could be triggered at the inputs with a 50-V pulse through the electrostatic discharge (ESD) tester for all circuits; 50 V was the lowest voltage that could be provided with the test equipment. Tests with the pulse generator showed that some circuits could also be triggered into latch-up with voltages as low as 30 V. The energy required to initiate latch-up was ≈ 0.125 μ J. Rise times of 100 ns or less were required to induce latch-up.

Additional tests were done using a $V_{DD} - V_{SS}$ breakdown simulation technique at the pin to generate the curve shown in Figure H-4 for a CD4049 circuit. The output resistance (slope) in the latched condition is about 8 ohms. However, the CD4049 circuit contains six separate inverters, each of which can latch, and this affects the output resistance. If several circuits latch simultaneously, which was the case in Figure H-4, the slope is very steep. The slope will decrease by approximately a factor of three if latch-up occurs in only a single section of the circuit.

If the external current is not limited by a resistor or current-limited power supply, currents exceeding one ampere will flow after latch-up, causing catastrophic failure within about 10 s in these devices. However, if the current is limited to lower values, burnout will not occur, and the devices will resume normal operation after the power supply is temporarily interrupted. Experimental measurements show that currents ≈ 100 mA will not cause catastrophic failure, even if they remain latched for periods of several hours.

C. Effect on External Circuits

CD4000-series circuits are used in large numbers in the MO CIU, with a 10-V power supply (10-V logic). The transfer characteristics specified by the manufacturer for these devices are shown in Figure H-5. Note that there is a wide variation in inverter switching voltages—from 2 to 7 V—to allow for processing run variations in the threshold voltages of n- and p-channel transistors. Typical devices switch at about 4 V, but the switching point of individual units depends on the threshold voltage of that particular lot. Although it is unlikely that unit-to-unit variations in switching threshold will range over the entire allowed span of 2 to 7 V, there will be differences between different devices. These will likely range from approximately 3 to 5 V. Thus, any logic voltages that fall within this intermediate range will be ambiguous and may be interpreted differently by different circuits.

In all Mars Observer applications of CD4000-series circuits, a 51-ohm resistor was placed in series with the power supply connection to limit the maximum supply

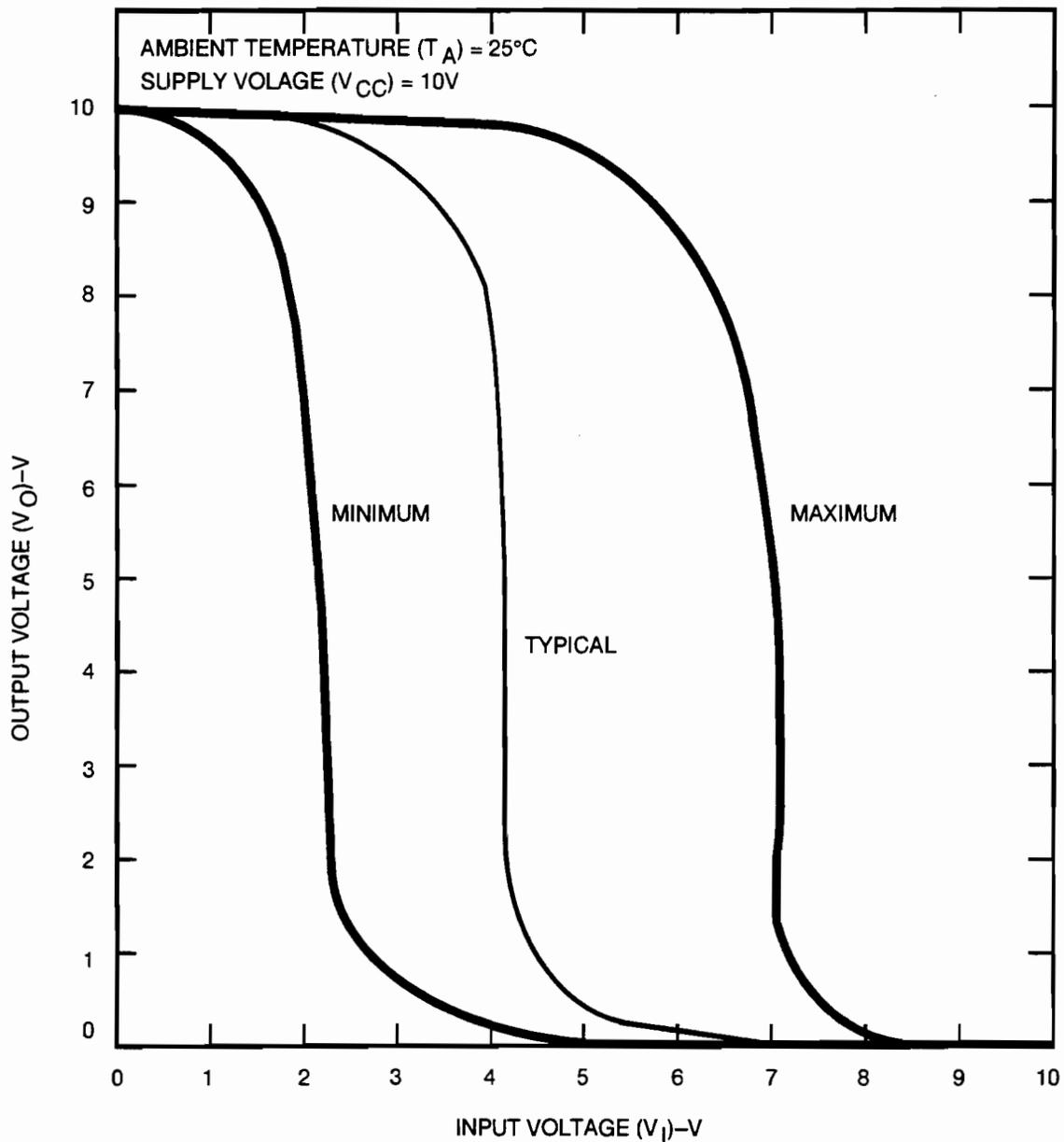


Figure H-5. Transfer characteristics of a CD4049 inverter.

current.² This turns out to be an unfortunate choice if devices are driven into latch-up because the nominal 100-mA quiescent current of the CD4000 with this particular load will reduce the output voltage below 5 V. For example, Figure H-4 shows a 51-ohm load line superimposed on the output characteristics of a latched CD4049 circuit. The quiescent point is above the minimum guaranteed value required for a solid "0," and

² The CD4049 circuit contains six inverters in a single package, with a common power-pin connection. If any of the six circuits latch, the power supply voltage of all the others will be affected, and, if the voltage falls below the guaranteed "1" level, will cause them, as well as the inverter that latched, to be nonfunctional.

hence may result in an indeterminate output voltage. More precisely, some circuits will interpret this voltage as a "1," others as a "0." If the voltage is exactly at the center of the transfer curve of a driven circuit, it may oscillate back and forth between the two states. The I-V characteristics of a latched device are expected to vary somewhat between different parts and different processing runs, and, as noted earlier, also depend on the number of internal latch-up paths triggered by the electrical pulse. Thus, the quiescent point of latched devices with a 51-ohm load might vary from below 3 V to perhaps as much as 6 V, and can result in a hard "0," a hard "1," or intermediate conditions.

IV. Step 2: Energy Coupling Mechanisms

Three methods have been proposed that could couple energy from the squib firing to circuit boards, and hence trigger latch-up in logic circuits: (1) magnetic-field coupling from the primary loop of current in the ground surge to secondary loops in the circuit boards; (2) electric-field coupling from fast-rising signals that are caused by the presence of inductance in the ground and chassis connections; and (3) coupling of the electromagnetic field produced by the ground current surge to resonant sections of conductors and/or cables.

A. Mechanism 1: Magnetic-Field Coupling

Magnetic-field coupling assumes coupling from the magnetic field of a primary loop, through which the ground current flows, with a secondary loop that is connected to the integrated circuit. Elementary formulas for magnetic coupling at large distances show that the magnitude of the coupled field decreases as $1/r^3$, and is also proportional to the area of the two loops. Although this gives a very rough idea of the magnitude and shows that it depends very strongly on distance, it is not adequate for near-field conditions. Calculations are far more difficult for loops in close proximity, even for simplified geometries.

Unfortunately, the geometry of the current loops in the Mars Observer system are very complex. This complexity, along with the strong dependence on distance, makes it extremely difficult to bound the value of the coupled field. The orientation of the loops is also critical, because the field B is a vector quantity. An example of the actual geometry is shown in Figure H-6 for the primary current loop of the squib current. The total area of the loop is estimated to be 4 m^2 , but it makes several twists and turns. There are a number of secondary loops, with similar complexities. The areas of the secondary loops are estimated to be ≈ 1 percent of the area of the primary loop. Initial calculations,³ assuming a secondary loop area of 0.02 m^2 , yielded the results shown in Table H-1. In the table, the primary loop is the "culprit" loop, and the secondary loop is the "victim" loop.

³ Nguyen, 1993.

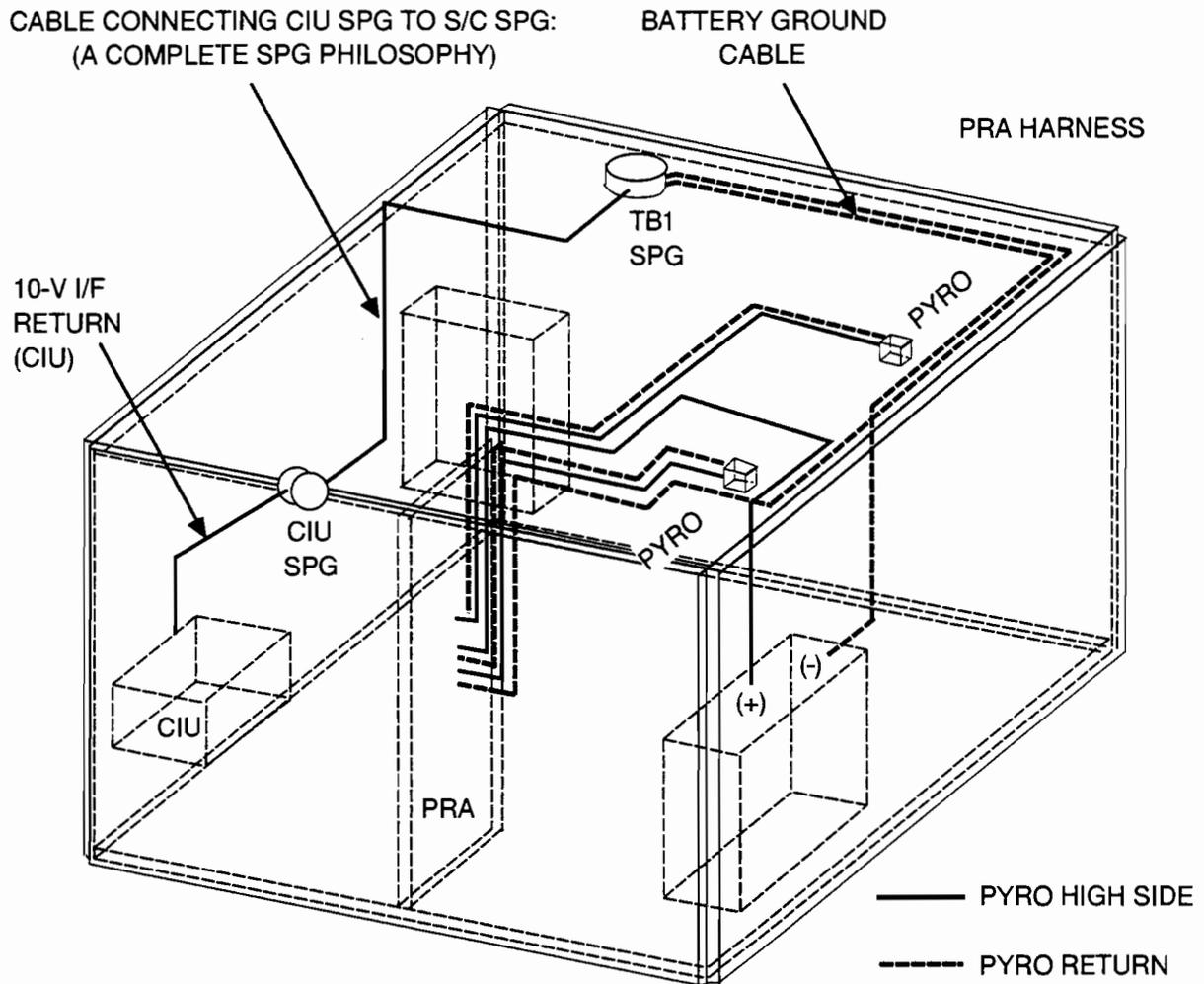


Figure H-6. Geometry of primary current loop from battery through chassis when squib shorts to case. Secondary loop geometries are of similar complexity.

Note the large difference in induced secondary voltage that results from a factor of two change in the distance between the loops; the induced secondary voltage drops from 31.58 to 1.6 V. Although these voltages are on the order of voltages required to induce latch-up, their values are only approximate. Other factors, such as the uncertainty in the area, orientation, and effectiveness of shielding between loops in electronic circuitry and the primary loop will increase the possible range of induced voltages from this coupling mechanism. In addition, since there are several potential secondary loops, larger voltages may result in the logic circuitry. The difficulty of assessing this coupling mechanism will be addressed further in the conclusions and recommendations section of this Appendix.

The primary loop in Figure H-6 is very simple. Other possible loops were considered in the analysis which are much more complex. Figure H-7 shows a more complete analysis of such a loop. Note that the current path of the squib circuit flows

Table H-1. Voltage induced by B-field in secondary loops for two distances between primary and secondary loops.

Culprit dimensions			Victim dimensions			Separation	Forcing function	Results	
Length, m	Height, m	Area, m ²	Length, m	Height, m	Area, m ²	Distance between culprit and victim, m	Culprit current, A	B Field generated by culprit, gauss	Induced voltage by B Field, V
2	2	4	2	1	2×10^{-2}	1	2	1.422×10^{-2}	1.58
2	2	4	2	1	2×10^{-2}	0.5	2	31.84×10^{-2}	31.84

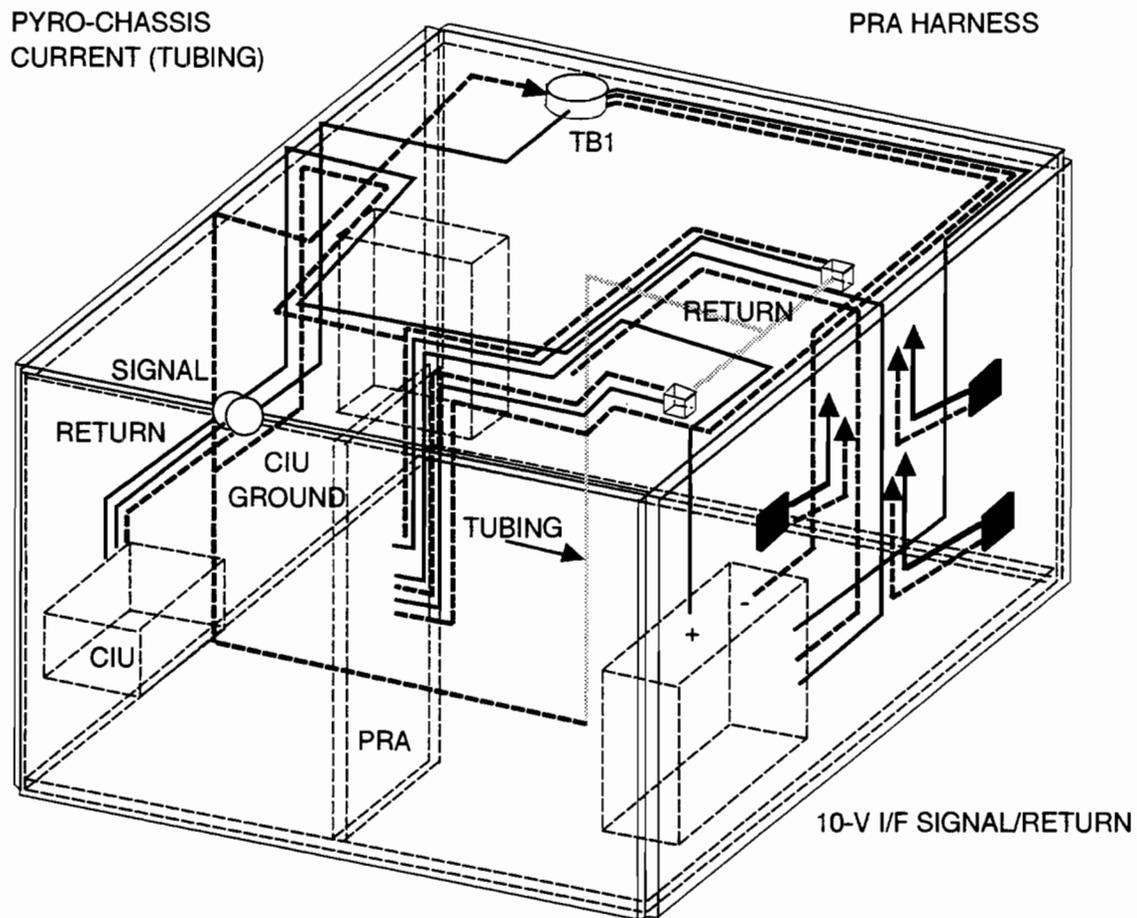


Figure H-7. Culprit and victim loops.

through the chassis, cables and wiring. A detailed analysis must be three-dimensional. A planar view of the primary and secondary loops is shown in Figure H-8 (in this figure two faces of the Mars Observer enclosure are folded flat for simplicity). Note that current from the primary loop goes from the battery, through the pyro valve, tubing, and tank, and then to the chassis. The approximate location of the secondary loop is also shown in this figure. Figure H-9 shows this same configuration, adding additional details for the secondary loop. These figures demonstrate the extreme complexity of the actual current loops in the Mars Observer system.

B. Mechanism 2: Electric-Field Coupling

The second coupling mechanism is electric-field coupling from the voltage induced by the surge of current from the squib into inductance in the ground and other wiring. From elementary considerations, this is $V_{\text{induced}} = L \, dI/dt$, where L is the inductance in the main loop. An approximate calculation of the inductance (with simplified geometry) yields an estimated inductance of 3 μH . For a 10-A, 100-ns current pulse the

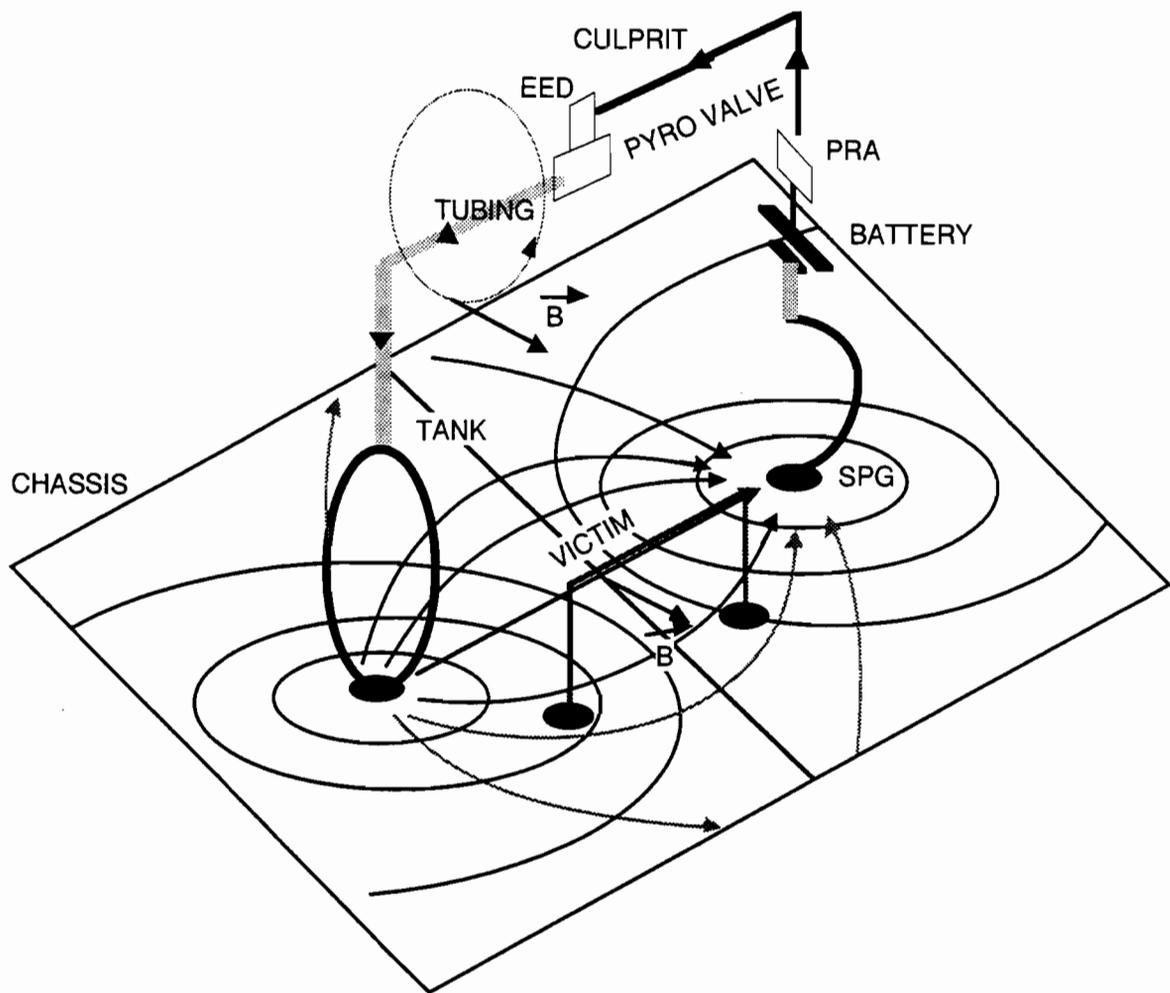


Figure H-8. Loop-to-loop coupling model for Mars Observer pyro-induced chassis current with culprit details.

induced voltage is 300 V; this voltage will occur when the current decays, not during turn-on. Furthermore, its value depends critically on the fall time of the pulse, which can only be estimated. Thus, just as for the first mechanism, this one is subject to large uncertainties because of the dependence on the detailed geometry of the configuration.

The voltage developed in the primary loop will be coupled to secondary loops through capacitance between the secondary and primary loops ($V = C \, dV/dt$). The effectiveness of this coupling depends on the layout of the secondary loop; if it is close to a ground plane, or protected by cable shielding, little coupling will occur. The effective capacitance can only be roughly estimated. For a capacitance of 1 pF, a primary loop voltage of 360 V with 100 ns transition time will produce a secondary voltage of 3.6 mV.⁴ Ringing and faster transients will increase this voltage, but

⁴ This value and the associated induced voltage are considerably lower than the values in T. Nguyen's, notes from briefing to Mars Observer Special Review Board, Foil TTN-40, Jet Propulsion Laboratory, Pasadena, California, October 6, 1993.

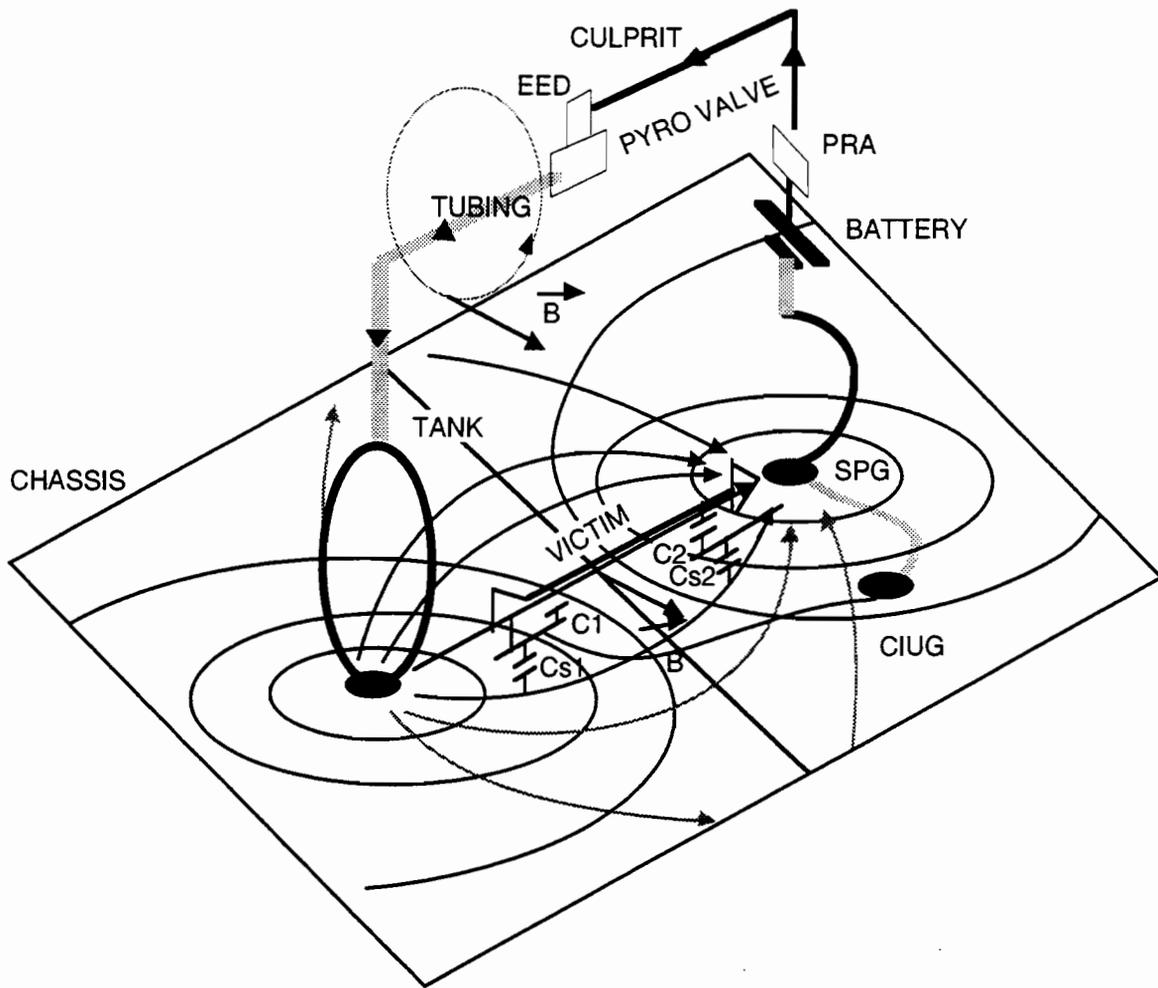


Figure H-9. Loop-to-loop coupling model for Mars Observer pyro-induced chassis current with culprit and victim details.

transitions in the subnanosecond range would be required to produce enough secondary voltage to cause latch-up. Thus, compared with the first mechanism, electric-field coupling seems less likely, particularly since the layout of most circuit boards provides significant shielding from ground planes.

C. Mechanism 3: Resonant Pickup by Ground Wiring

The third mechanism is direct electromagnetic coupling into a giant loop, formed by the ground wire, considering it to be a distributed wire-over-ground transmission line. Two separate effects are considered: first, resonance in the transmission line, which will effectively double the magnitude of the induced voltage; and second, a lumped resonant circuit formed by the line inductance and the discrete 5100-pF capacitor that exists at the interface circuit.

The first effect is essentially just a modified way of looking at magnetic coupling. A resonant transmission line would simply *double* the voltage induced in the ground line from the magnetic-coupling mechanism that was discussed earlier. This would increase the maximum estimated voltage from 31.8 to 63.6 V.

The second effect depends on the magnitude of the electromagnetic field that is produced by the squib current pulse. It is highly frequency dependent. The resonant frequency of the secondary loops is estimated to be between 1 and 10 MHz, which is very near the peak energy of a 100-ns pulse. Thus, resonance could easily result. The maximum voltage then depends on the Q of the circuit, as well as on the electromagnetic energy.

A recent experiment was completed by T. Nguyen using a relay to produce transients in a ground line that approximated the geometry used in the Mars Observer logic. The rise time of current in the primary loop was 10–50 ns. Pulses of 15 V were observed in the simulated logic loop, with ringing at about 10 MHz. This shows that direct electromagnetic coupling is a feasible mechanism.

V. Step 3: Latch-up in Critical CMOS Circuits

Even if sufficient energy is coupled into secondary loops to trigger latch-up in CD4000-series CMOS devices, failure of the Mars Observer will only occur if the latch-up condition is not corrected by redundancy or fault tolerance. The basic logic configuration used within Mars Observer is repeated many times, and for this reason there are many internal points where latch-up can be induced by external signals.

A. Critical Circuits

One critical circuit board contains no redundancy (board A-11). A number of potential single-point failures were identified within the CIU module that could result in system failure if latch-up occurred in a critical circuit. They are summarized in Table H-2.

Table H-2. Single-point failure modes in the CIU module involving CD4000 logic circuits.

Case	Failure Mode
1	CIU CONTROL1 and CONTROL2 signals (SCP in control)
2	I/O Crossed/Not Crossed (C5B)
3	I/O Bus Select (C5C)
4	RPA Lockup (C16)

B. Case 1—SCP In Control (C5A)

The first case, which is also described in Section VII.G.1, is discussed in detail below. The other cases in Table H-2 are discussed in Sections VII.G.2, VII.G.3, and VII.Q in the body of this report.

There are two control signals, CONTROL1 and CONTROL2, that are assumed to be complementary because CONTROL2 is generated by a single inverter, with input = CONTROL1. As shown in Figure H-10, if CONTROL1 is high, SCP-1 is selected; if CONTROL2 is high, SCP-2 is selected. If the inverter is placed in a metastable state because of latch-up, then the circuitry can be in either of two forbidden states, i.e., 0/0 or 1/1; the 0/0 condition could also result if the inverter (or other circuits connected to its decoupling resistor) latched.

Table H-3 presents the four possible logic conditions:

Table H-3. Logic conditions.

Condition	SCP-1	SCP-2	Result
1	1	1	Both SCPs contend control
2	1	0	SCP-1 controls
3	0	1	SCP-2 controls
4	0	0	Both SCPs disabled

Condition 2 was in effect at the start of the sequence. Condition 3 simply shifts control from SCP-1 to SCP-2, and will not affect system performance. However, either condition 1 or 4 will effectively halt command generation, with no RPA turn on and no attitude control.

After the anomaly, ground commands were sent to the spacecraft that would turn off power to SCP-1. Turning off power would have resolved condition 1, where both SCPs are attempting to control the spacecraft, but would be ineffective for condition 4, where neither SCP is active.

Coupling of external signals to internal logic is clearly more likely for circuits that are connected directly to an I/O connector than for circuits that are located at internal locations on a circuit board. The logic circuits that are involved in failure mode 4 above are directly connected to external interfaces, and thus are more likely than the first failure mode, which is not directly connected to an interface.

1. If latch-up occurs, the top protection diode of the inverter is shorted to 5 V.
2. V_{CC} drops to 5 V.
3. The output is now at 5 V (indeterminant—interpreted as “O” by control 2).
4. Pulls output of driver to 5 V (indeterminant—interpreted as “O” by control 1).
5. Therefore, neither SCP-1 nor SCP-2 is active.

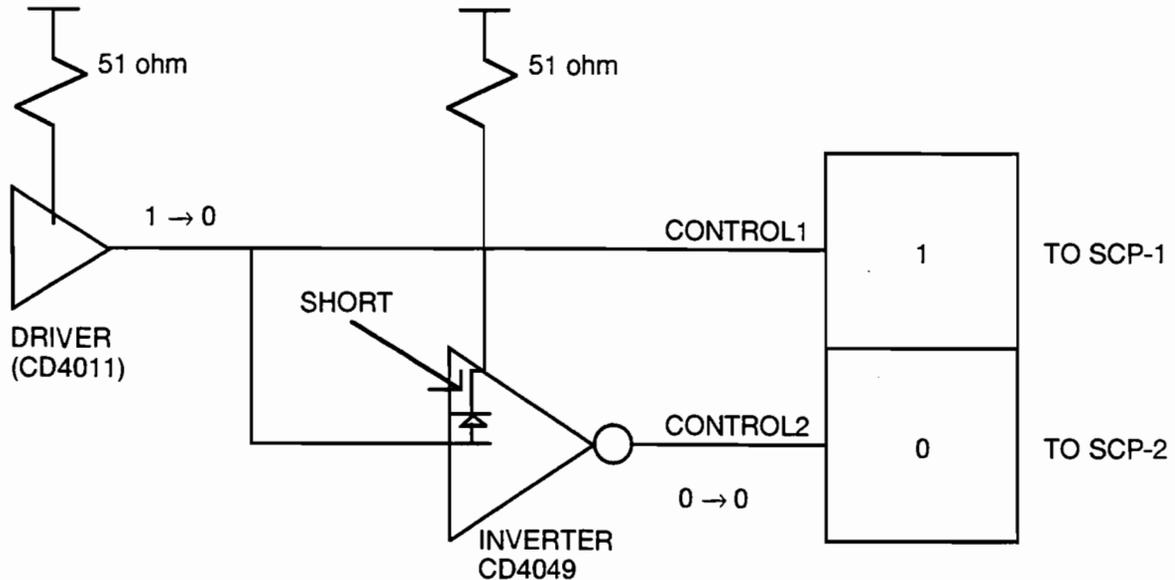


Figure H-10. SCP in control.

VI. The Magellan Incident

A relevant incident⁵ occurred on the Magellan spacecraft during separation of the spent solid rocket casing a few hours after that spacecraft was successfully inserted into Venus orbit. Separation was accomplished by releasing four “explosive bolts” that were driven by eight NSIs, fired four at a time.

At the time of the incident, both computers in the AACS were operating. Memories A and B were being accessed by Processor A, which was in control. At separation, telemetry showed that the A4 bit in memory B was suddenly stuck “high.” Solid rocket motor separation was normal, as were all AACS functions. After several hundred hours elapsed, the stuck bit in this RAM suddenly recovered, and operated normally thereafter.

Each memory of the AACS contained 512 TCC244 RAMs packaged on four circuit boards for a total of 1024 components. Only a single memory circuit was affected during the sequence. Furthermore, operation was normal after all previous NSI firings.

⁵ J. C. Arnett, *Recommended List of Documentation Covering the Magellan Squib Shorting Scenario*, JPL Interoffice Memorandum 5211-93-522, Jet Propulsion Laboratory, Pasadena, California, November 12, 1993.

Ground tests showed that this symptom in the memory could be created by applying a voltage pulse of sufficient magnitude to short circuit the input protection diode in the RAM. After several hundred hours, excessive heating in the diode caused it to burn open, and the RAM then resumed normal operation. This is certainly consistent with the operation of the RAM on Magellan. After the laboratory tests on the RAM, a series of tests were done to investigate chassis current pulses from NSI firings.

The Magellan incident shows that anomalies similar to the hypothesized Mars Observer anomaly have been experienced on other spacecraft. Onboard telemetry showed that they occurred at the same time that the squibs were fired, and hence appear to have been initiated by firing of NSI circuits. This lends additional credibility to the possibility that this failure mechanism occurred in Mars Observer.

VII. Summary and Conclusions

As discussed in the Introduction, three phenomena must occur in order for the firing of the squib circuit in the Mars Observer to cause system failure due to latch-up in CD4000-series CMOS devices:

- (1) The squib must short to the case during the time that it is fired;
- (2) The transient current of the squib must induce sufficient energy into the logic circuit wiring or ground system to cause latch-up in CMOS devices; and
- (3) The latched CMOS circuits must create a failure in the Mars Observer logic circuitry that is not corrected by redundancy, fault tolerance, or ground-command signals.

As verified by laboratory testing, shorting of the squib is quite likely, and produces transient currents of approximately 10 A in the ground system. The waveform has a rise time of 50–100 ns, and produces extensive ringing and noise.

The second effect, coupling of transients from the squib to latch up sensitive circuitry, is strongly dependent upon the geometry of the overall assembly and the specific layout of cabling and shields. Because of this, only approximate estimates can be made of the magnitude of these coupling mechanisms. Initial calculations using simplified geometries indicate that the first and third mechanisms, magnetic-field coupling to secondary current loops, and electromagnetic pickup by resonant circuits, are likely to produce voltages of sufficient magnitude to potentially cause latch-up. Although this does not guarantee that latch-up will occur, it lends strong support to the credibility of squib coupling as a latch-up mechanism.

The main conclusion of this study is that it appears that latch-up in CD4000 logic circuitry could indeed be caused by squib circuit firing. The chief uncertainty is in the coupling mechanisms, which can only be calculated for simple geometries. Although extensive experimental work has been done on latch-up, and work is progressing to investigate squib currents, little work has been done on the more complicated issue of the coupling mechanisms. It is recommended that additional experimental work be done to measure induced voltages in representative Mars Observer circuitry to provide

more direct corroboration of the feasibility of latch-up. The second area that needs more work is the identification of critical paths and single-point failure modes.

A second conclusion is that the main reason for potential sensitivity of the Mars Observer system to this failure mode lies in specific details of the way that the system was designed. The lack of redundancy in critical control logic, use of a current-limiting resistor that inadvertently would produce a metastable logic state if latch-up occurred, and the particular grounding scheme all contributed to the problem. These factors make it difficult to relate successful use of squibs in other spacecraft to Mars Observer.

Finally, examination of the design and mechanisms can be used to put the problem in perspective, and also to make some specific recommendations:

- (1) Thousands of NSI firings have occurred in space, and thus far there has been only one documented anomaly that relates to electronic upset or failure. Clearly new designs should take the possibility of squib-to-case shorts into account when designing the squib firing systems and grounding schemes.
- (2) Based on laboratory tests, the currents being used to fire squib circuits are far greater than needed, which increases the likelihood of electromagnetic coupling. Future designs should consider reducing this current to lower levels.
- (3) Astro has flown more than 20 spacecraft with similar electronic designs, and has never experienced a telemetry error or electronic failure that is attributable to squib firing. However, these spacecraft were physically much different than Mars Observer, which makes it difficult to relate their success to the Mars Observer problem, particularly because the electromagnetic coupling mechanisms depend so strongly on system and subsystem geometry.
- (4) The logic design that was used on Mars Observer had a number of single-point failures, some of which were identified during CDR. Most of these failures could have easily been eliminated during initial planning of the logic and control system. Clearly more attention should be given to avoiding such possibilities, and providing global "work arounds" such as external power control that could be used to recover from latch-up.
- (5) The CD4000-series circuits that were used on Mars Observer are known to be sensitive to electrically induced latch-up, even though they are not sensitive to radiation-induced latch-up. Even though newer designs have smaller feature size, electrically induced latch-up depends mainly on the way that the input and output protection circuits are designed. Thus, there is no reason to suspect that more modern devices are more susceptible to latch-up from electrical transients than CD4000 devices.

It should also be noted that the main focus of this work was on latch-up. Latch-up does not produce part degradation (other than through overheating), and latch-up triggering does not change with repeated applications of electrical pulses that are below the latch-up-triggering threshold. However, other mechanisms are possible—such as electrically induced burnout at I/O circuitry—which are affected by repeated applications of pulses, and might also be initiated by electrical transients from the squib circuit.

APPENDIX I

CAUSAL FACTOR: METEOROIDS

I. Environment Description

The model describes the distribution of interplanetary particles in terms of particle mass, orbital inclination, eccentricity, and distance from the Sun. It includes particles ranging from 10^{-18} to 1 gram in mass and covers the range of 0.1 to 20 AU in heliocentric distance.

The model incorporates data from detectors from Pioneer 10 and 11, Helios 1 and 2, Galileo dust detector, and Ulysses Spacecraft, as well as radar observations and Zodiacal light measurements.

Based upon the orbital elements of the particle population and the trajectory of the spacecraft, the position of the spacecraft and the relative velocity (speed and direction) of the particles can be determined.

Combining the information about particle relative velocity with information about number concentration gives the instantaneous flux (particles/m²/s) for every point on the trajectory. Fluence (particles/m²) is simply the integral of flux over time.

Table I-1 and Figure I-1 display the integral fluence as a function of mass for the interplanetary transit phase. Particle masses below 3.8×10^{-6} are not considered since such particles have no potential for inflicting critical damage upon the spacecraft.

II. Critical Hardware

The bipropellant tanks are critical to the pressurization process because they are repressurized at the end of interplanetary transit after being partially depleted by maneuvers in transit. The MMH tank is well protected by the blanket and does not weaken during flight and therefore is not critical to the pressurization process. The monopropellant and helium tanks are not a pressurization issue since they remain fully pressurized during flight. The valves and pressure lines exposed to the environment are also of interest because they can be affected by the environment. Failure effects on valves and pressure lines were addressed in the same context as propellant tanks. The NTO tank is covered by a blanket and there is appreciable spacing between the tank and the blanket over most of the surface.

The fluence and the area associated with the least effective protection are the drivers in the calculation of the probability of failure. Details of the analysis are given in Footnote 1.¹

¹ R. Aguero, *Probability of Catastrophic Meteoroid Impact on Mars Observer*, JPL Interoffice Memorandum 5215-93-256, Rev. A, Jet Propulsion Laboratory, Pasadena, California, November 22, 1993.

Table I-1. Mars Observer cumulative fluence.

MASS, g	FLUENCE, m ⁻²
3.816×10^{-6}	2.915×10^{-1}
1.294×10^{-5}	1.070×10^{-1}
1.958×10^{-4}	8.944×10^{-3}
6.636×10^{-4}	2.401×10^{-3}
3.160×10^{-3}	3.650×10^{-4}
5.620×10^{-3}	1.777×10^{-4}
1.000×10^{-2}	8.661×10^{-5}
1.780×10^{-2}	4.039×10^{-5}
3.160×10^{-2}	1.885×10^{-5}
5.620×10^{-2}	8.797×10^{-6}
1.000×10^{-1}	4.108×10^{-6}
1.780×10^{-1}	1.907×10^{-6}
3.160×10^{-1}	8.852×10^{-7}
5.620×10^{-1}	4.111×10^{-7}
$1.000 \times 10^{+0}$	1.909×10^{-7}

III. Method of Investigation

To calculate the degradation and immediate penetration of the protection provided for the tank, a double surface-penetration model was used. The fluence responsible for the degradation of the tank is accumulated during the interplanetary transit (Table I-2) in the region limited by the "no degradation," and "immediate penetration" boundaries (Figure I-2). The fluence responsible for the penetration at the end of transit is simply a fraction of the total corresponding to the last 14 minutes. The probability of failure is calculated using the fluences and areas corresponding to the surface-blanket layout of the tanks.

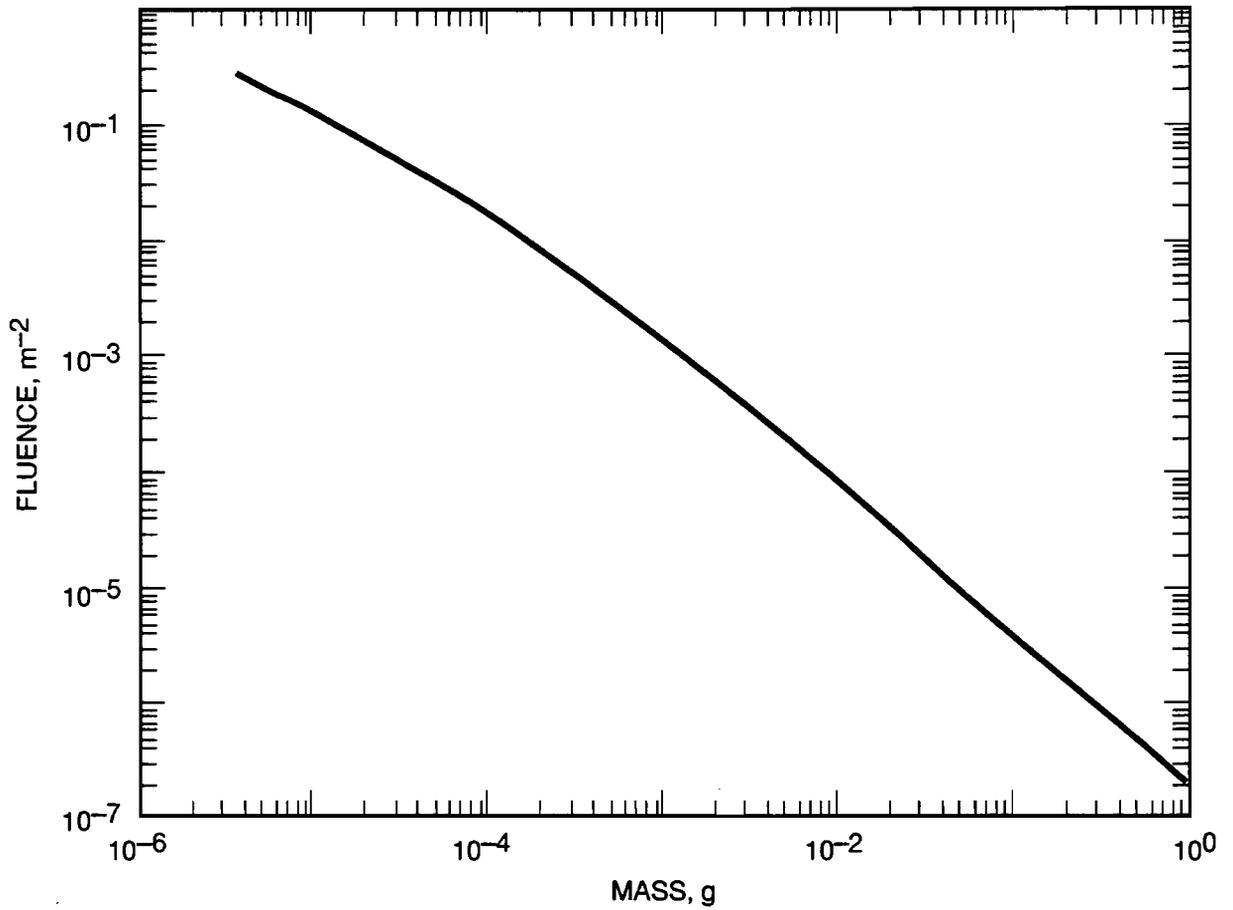


Figure I-1. Mars Observer cumulative micrometeoroid fluence as a function of mass.

Table I-2. Fluences contributing to weakening of the tank velocity (km/s).

	5	12.5	17.5	22.5	27.5	35	40
							3.0×10^{-4}
						1.0×10^{-3}	
					2.2×10^{-3}		
				3.6×10^{-3}			
			4.0×10^{-3}				
		3.7×10^{-3}					
	2.1×10^{-3}						

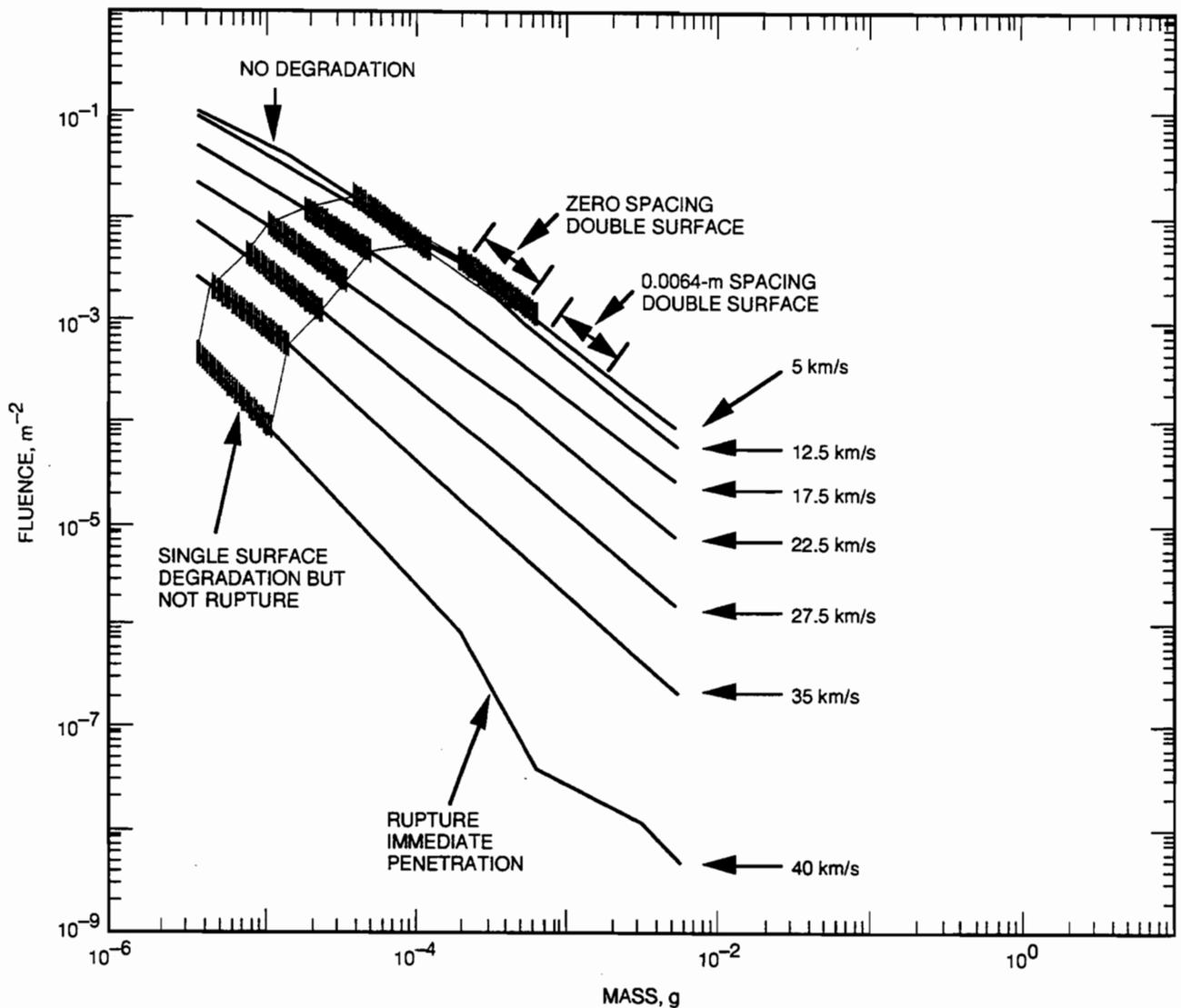


Figure I-2. Meteoroid fluence for Mars Observer for different velocity bins.

IV. Limitations of the Analysis

The fluences of Figure I-2 assume all particles are as damaging as normal to the surface impacts. A factor of 0.304 is used to provide for the effect of off-normal impacts.

The limitations of the analysis are basically driven by the probabilistic nature of the models used. The meteoroid environment, although it includes the most updated data from all sources, produces an uncertainty factor of 2. Although they represent the best estimate, the penetration equations for single and double surface are still results of experimental extrapolations and they have an uncertainty factor ranging from 2 to 3.

V. Results of the Investigation

The probability of being hit by a meteoroid is related to the trajectory of the spacecraft, to the fluence accumulated during flight, and the area exposed to the environment. The following paragraphs summarize the scenarios in which meteoroids could have played a role by hitting Mars Observer and producing the explosion of a tank or an excessive spin rate. The scenarios are mentioned in descending order of probability of failure:

- (1) Meteoroids hit the NTO tank protection during interplanetary transit, weakening but not rupturing the walls. The tank explodes upon pressurization. The probability associated with this event would be less than $P1 = 1.05 \times 10^{-3}$ even if the thermal blanket is in contact over the entire area of the NTO tank, which is not protected by the bus. This is an extreme upper bound since only a small fraction of the area is in contact with the tank.
- (2) A meteoroid hits any of the tanks in the 14-min dead band at the end of the interplanetary transit. The tank explodes upon penetration. The probability associated with this event is $P2 = 2.41 \times 10^{-7}$.
- (3) A meteoroid hits a critical mechanical component in the 14-min dead band at the end of the interplanetary transit. The spacecraft fails critically and it is lost. The probability associated with this event $P3 < 2.41 \times 10^{-8}$.
- (4) A meteoroid hits Mars Observer during the 14-min dead band and penetrates at least 60 mils of aluminum thickness. The meteoroid and/or the scattered debris hits the electronics associated with attitude control and/or spin control. The spin rate is larger than 7.5 rpm. The probability is $P4 \ll 2.41 \times 10^{-8}$.
- (5) A meteoroid large enough, and with enough linear momentum, hits the magnetometer, GRS, or the HGA and induces a spin rate larger than 7.5 rpm. The probability is $P5 \ll 1.2 \times 10^{-13}$.

APPENDIX J

CAUSAL FACTOR: SINGLE-EVENT EFFECTS

I. Overview

There is no as-built parts list for the Mars Observer spacecraft. Therefore, it was not feasible within the scope of the Special Review Board to do a complete spacecraft analysis for single-event effects (SEEs). Some work was done to examine the CIU, CIX, SCP, and CDU for latch-up and single-event upsets (SEUs). The results of that work are documented in this Appendix.

The examination of the FETs in the Power Subsystem for SEB and SEGR is discussed and dismissed in Chapter V.J.3

Single-event effects are not thought to be related to the Mars Observer loss-of-signal anomaly.

II. Introduction

SEUs and single-event latch-ups (SELs) are important effects in modern digital circuits. Laboratory SEE test data are available for all of the digital devices that were used in the CIU, CIX, SCP, and CDU subsystems. These data, however, are not sufficient to determine the SEU or SEL rate in the Mars Observer application. A number of additional steps and assumptions are required in order to calculate SEE rates from laboratory data, including:

- (1) the shape of the cross section versus the linear energy transfer (LET) curve that is used for the analysis (a step function is often used for simplicity, but it is too conservative)
- (2) determining the sensitive charge collection volume, which is required in order to calculate the effective LET of ions that enter the device at other than normal incidence
- (3) the distribution of particles as a function of LET, which depends on solar flares as well as on the background galactic cosmic ray fluence
- (4) the way that the device is used in the system application

The last factor is particularly important for microprocessors, because many of the internal upsets that occur in a typical application program will not necessarily cause errors or malfunctions.

Several different types of devices were considered in the analysis, including CD4000-series logic circuits (CMOS), bipolar logic circuits, two types of CMOS RAMs, a CMOS PROM, and two types of microprocessors.

III. System Overview

The units that were considered in the evaluation of SEU and latch-up rates were the CIU, CIX, SCP, and CDU. All of these units are designed with redundant circuitry, with the exception of one control circuit board in the CIU (board A11). However, redundancy was not considered in evaluating SEU sensitivity. The number of parts included in these units that are potentially susceptible to upset and latch-up are listed in Table J-1 (logic circuit quantities are approximate).

A block diagram showing the way that these subsystems are interconnected is shown in Figure J-1. A serial failure model was adopted which assumes that SEU or latch-up in any of the parts would potentially cause failure of the Mars Observer spacecraft. This is clearly oversimplified, but provides a first-order, conservative assessment of the likelihood that SEEs were a contributing factor.

Table J-1. Distribution of SEE-sensitive parts in Mars Observer subassemblies.

Device type	CIU	CIX	SCP	CDU
CD4000 Family	500	100	—	8
M1750 Microprocessor	—	—	1	—
6617 PROM	—	—	23	2
65C262RH SRAM	—	—	96	—
54LS, 54HS Families	—	—	200	19
80C86RH Microprocessor	—	—	—	1
6514RRH SRAM	—	—	—	4

Note: CD4000 and 54-series figures are approximate.

IV. Environment

The environmental model that was used in the calculations is the standard "Adams 90%" distribution of cosmic rays. A 100-mil spherical aluminum shield was assumed to surround the devices in all applications. The solar flare environment was not included because no energetic solar flares were present during the time of loss of communication with Mars Observer.

In the Adams model, the distribution of cosmic-ray particles decreases rapidly with increasing LET, for LET values above 26 MeV-mg/cm² (the iron threshold). However, higher effective LET occurs in semiconductor devices because of the longer path length that results when ions strike p-n junctions at angles. This increases the effective iron threshold to about 70 MeV-mg/cm².

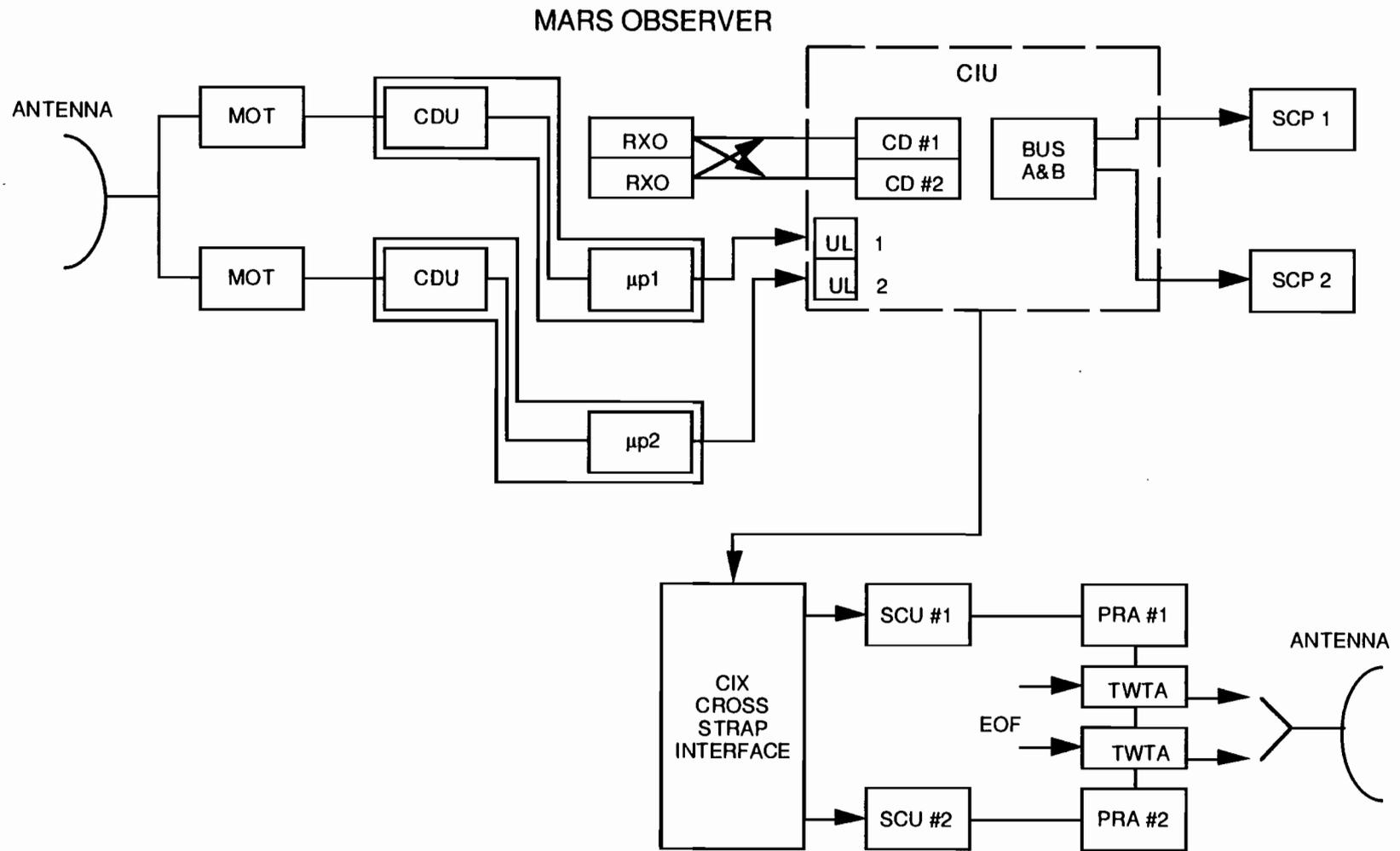


Figure J-1. Spacecraft block diagram with subsystems containing SEU/latch-up sensitive components.

V. Calculation of Upset and Latch-up Rates

A. Basic Approach for SEU Analyses

The basic difficulty in interpreting SEE data is that the laboratory results only apply to single particle energies, with a limited number of angles of incidence, whereas the actual cosmic ray flux consists of a distribution of particles. In order to calculate the actual error rate in space, the LET distribution must be integrated over all angles because the cosmic ray flux is omnidirectional. This requires extrapolation of the small-angle laboratory test data to the large-angle conditions found in space. The extrapolation can only be done with limited accuracy unless specific information is available about the semiconductor structure, including the depth of the diffused junctions, their areas, doping concentrations, and the substrate technology. However, extrapolation methods have been developed that can be used in the absence of specific fabrication details which will yield conservative results, and that was the approach taken in analyzing the devices used in Mars Observer.

Two different approaches were used in calculating SEU rates. The first approach used a simplified method to approximate the cross-section dependence on LET. The second approach applied a correction factor to the upset rate that was based on previous experience for a number of devices for which actual upset rates in space were available.

1. Approach 1

The first approach assumed a step function for the cross section, i.e., zero cross section for low LET values, followed by an abrupt rise in cross section at the LET threshold up to the saturation cross-section value. This approach is conservative, and is also simpler than the alternative approach. These calculations were done for all of the devices in Table J-1. The results obtained by assuming a step-function cross section are denoted by the term "Upper Bound" in the tables.

2. Approach 2

A second approach was used to obtain a better estimate of the expected SEU rate by applying a correction factor to the calculated error rate. The correction factor was based on previous experience with a number of devices (not necessarily devices used on Mars Observer) for which detailed fabrication information was available. These calculations involved a detailed numerical integration of smooth SEU cross-section curves, along with the charged-particle LET distribution and angle distribution. For typical devices, the error rate was reduced by about a factor of three when a smooth cross-section curve was used instead of the step function (Approach 1).

In addition to the calculated SEU error rates, data were also available for the actual upset rate of these devices during space flight. The observed upset rates in space were somewhat lower than the calculated upset rate, even when a smooth cross-section curve

was used in the analysis. For most devices, the measured SEU rates in space were approximately a factor of five lower than the predicted rates from the calculations.

Detailed calculations of the SEU rate with a smooth cross-section curve were done for some of the devices used in Mars Observer, but not for all of them. However, as discussed above, either approach will generally overestimate the upset rate compared to actual results in space. In order to obtain a better estimate of the actual upset rates expected in Mars Observer, the calculated cross sections were reduced by applying correction factors based on previous results. The data in the "best estimate" columns of the tables reduce the worst-case values by a factor of five for cases where numerical integration of a smooth cross section was used to calculate the error rate, and by a factor of 15 for cases where a step-function cross section was assumed.

B. SEU in Microprocessors

The approach used for SEU in microprocessors was essentially the same as that used for logic and memory with one important difference: for best estimate calculations, an additional correction factor was used to account for the fact that, under actual use conditions, many of the internal errors will not affect the microprocessor, either because they are not used during the particular sequence of instructions or because the software is self-correcting. This reduces the microprocessor SEU rate, which is typically based on register-intensive test conditions that assume that errors in any of the registers will cause upset or functional interrupt in the microprocessor, to a value that corresponds more closely to the SEU rate under typical operating conditions. This is discussed in more detail below.

SEU effects in microprocessors are very complex, and depend on the particular application program. Extensive testing of microprocessors has shown that the dominant mechanism involves changes in the status of internal registers. In order to get consistent test results, JPL (and many other users) test these devices in a simplified test mode that is highly sensitive to errors in any of the registers, and report the total cross section corresponding to the total number of registers. This cross section provides an upper bound of the SEU error rate, because most application programs are only sensitive to register errors during a fraction of the instruction sequences. Furthermore, many applications do not use all registers. The net result is that although register testing is a good way to standardize testing, it overestimates the error rate in applications, and skews the effect of SEU on microprocessors compared to SEU effects on more conventional circuits (i.e., logic and memory devices) that can be tested in a way that closely approximates actual use conditions.

Comparisons of microprocessor SEU test results with several different application programs have shown that the SEU rate can be a factor of 10–30 lower than the upper bound provided by register testing. Therefore, the experimental saturation cross section of the microprocessors, which was obtained from register testing, was reduced by an additional factor of 10 for best estimate calculations, and was done to provide microprocessor error rates more consistent with the error rates calculated for other

devices. Thus, the net reduction factor used for best estimates of microprocessors was 50 as compared with the upper bound estimates, whereas a factor of five was used for conventional logic devices and memories.

C. Latch-up

Single-event latch-up has never been observed in any of the parts in Table J-1, even though specific tests for latch-up have been done on all devices. Thus, the probability that any of these devices will exhibit latch-up is very small. However, the maximum LET used for latch-up testing was not the same for all tests (this is due to the fact that the tests were performed at different times and by different experimenters). This makes it somewhat difficult to calculate specific probabilities for latch-up. Strictly speaking, if a device was only tested to an LET of 75 MeV-mg/cm², it could conceivably latch at higher LET values. Table J-2 lists the maximum LET used during latch-up testing for each of the parts.

However, since there is no evidence that any of these parts will exhibit latch-up from single particles, it would be misleading to calculate latch-up probabilities. In all cases, the latch-up probability is very much less than the upset probability. Thus, for these devices, latch-up is negligible in the Mars Observer environment when compared to the overall upset rate for devices used in Mars Observer.

**Table J-2. Maximum LET used for single-event latch-up testing
(note that no devices were observed to latch during any of these tests).**

Device Type	Maximum LET for Latch-up Tests, MeV-cm ² /mg
CD4000 Family	75
M1750 Microprocessor	175
6617 PROM	100
65C262RH SRAM	75
54LS, 54HS Families	75
80C86RH Microprocessor	75
6514RRH SRAM	80

VI. Summary of SEU and Latch-up Results

A summary of the soft-error-rate calculations is shown in Table J-3. The rates in this table are calculated as errors per device-day. The columns include "upper bound," which was calculated from experimental SEE test results, and "best estimate," which is the expected SEU rate after applying a suitable correction factor. A third column, "observed," lists the observed rates for the 80C86 microprocessor and SRAM during the actual Mars Observer mission. Note that the observed rates for these two devices are comparable, even though SEU test data show that the SRAM has a much lower cross section than the microprocessor. This further corroborates the assumption that error

rates during actual use conditions of microprocessors are much lower than predicted from register-intensive test results.

Table J-4 shows calculations of the number of errors expected during 14-minutes, using upper-bound values from Table J-3. Adding the upper-bound numbers together predicts 1.3×10^{-2} SEU-related errors during the 14-minute communication loss period, dominated by errors in the SRAM. Thus, even the most conservative estimates make it unlikely that SEU effects contributed to the Mars Observer communication loss.

The best estimates of error rates for these parts are much lower, as shown in Table J-5. The sum of these error rates predicts about 10^3 SEU-related errors for Mars Observer during the 14-minute period, approximately a factor of 13 lower than the upper-bound numbers. Note that both calculations assume that any SEU during the 14-minute interval would result in loss of communication, which does not take redundancy into account.¹

Table J-3. Calculated soft error rates for various device types (error rates per device-day).

Device Type	Cross Section	Upper Bound	Best Estimate	Observed
CD4000 Family	—	Negligible	Negligible	
M1750 Microprocessor	—	Negligible	Negligible	
6617 PROM	Smooth	4×10^{-5}	8×10^{-6}	
65C262RH RAM	Step function	1.4×10^{-2}	9.3×10^{-4}	1.1×10^{-3}
54LS, 54HS Family	Step function	2.5×10^{-5}	1.7×10^{-6}	
80C86RH μ P	Smooth	1.2×10^{-1}	2.4×10^{-3}	2.5×10^{-3}
6514RRH RAM	—	Negligible	Negligible	

Table J-4. Expected number of soft errors in 14 minutes using upper-bound soft error rates.

Device Type	CIU	CIX	SCP	CDU	Total
CD4000 Family	0	0	0	0	0
M1750 Microprocessor	0	0	0	0	0
6617 PROM	0	0	9.0×10^{-6}	7.8×10^{-7}	9.8×10^{-6}
65C262RH RAM	0	0	1.3×10^{-2}	0	1.3×10^{-2}
54LS, 54HS Family	0	0	4.8×10^{-5}	4.6×10^{-6}	5.3×10^{-5}
80C86RH μ P	0	0	0	1.2×10^{-3}	1.2×10^{-3}
6514RRH RAM	0	0	0	0	0

¹ In actuality, SRAM errors are corrected by EDAC, resulting in a lower error rate than the above calculation. Assuming that EDAC lowers the contribution of the SRAM to negligible levels, the upper-bound rate is then reduced to 1.2×10^{-3} , compared to 1.3×10^{-2} . Similarly, the best estimate error rate is reduced to 2.87×10^{-5} with EDAC, compared to 10^{-3} without it.

Table J-5. Expected number of soft errors in 14 minutes using best-estimate soft error rates.

Device Type	CIU	CIX	SCP	CDU	Total
CD4000 Family	0	0	0	0	0
M1750 Microprocessor	0	0	0	0	0
6617 PROM	0	0	1.8×10^{-6}	1.6×10^{-7}	2.0×10^{-6}
65C262RH RAM	0	0	8.6×10^{-4}	0	8.6×10^{-4}
54LS, 54HS Family	0	0	3.4×10^{-6}	3.2×10^{-7}	3.7×10^{-6}
80C86RH μ P	0	0	0	2.3×10^{-5}	2.3×10^{-5}
6514RRH RAM	0	0	0	0	0

VII. Conclusions

This Appendix provides an assessment of the SEU and latch-up rates expected in the Mars Observer. The predicted error rate is low enough to make it extremely unlikely that SEEs contributed to the loss of communication with Mars Observer during the critical 14-minute period, even when very conservative upper-bound estimates are used. More realistic error rates show that the probability of any SEU event occurring during the 14-minute interval is about 10^{-3} , assuming a serial fault model. Internal operating conditions and redundancy would be expected to reduce the upset rate even further. Thus, it is extremely unlikely that single-particle effects played a role in the loss-of-signal incident on the Mars Observer spacecraft.

APPENDIX K

PROPULSION SYSTEM ANALYSES

This appendix describes the phenomena underlying Hypotheses C1A, C1B, and C1C and the ongoing efforts to quantify critical factors which affect the possibility of failures posed by those hypotheses.

I. NTO Transport Mechanisms

The transport of oxidizer into the Pressurization System during the Mars Observer mission is primarily the result of significant temperature gradients within the pressurization system. Figure K-1 presents the best estimates, based on flight temperature measurements, of the temperatures of the propellant tanks, check valves, low-pressure pyro valves (PV-5 and PV-6), regulator, and high-pressure pyro valves (PV-7 and PV-8). The data of Figure K-1 clearly show that the Pressurization System upstream of the check valves is significantly cooler than the check valves and the oxidizer tank throughout the mission. Furthermore, the coldest temperatures are expected at the high-pressure pyro valves upstream of the regulator.

These temperature gradients are much more severe than expected based on prelaunch thermal control predictions. The propellant tank temperatures predicted before launch were 14 °C; 18 °C colder than observed. No preflight predictions of Pressurization System component temperatures were located.

These temperature gradients provide a mechanism for transport of NTO vapor to the coldest regions of the pressurization system by maintaining a concentration gradient. This concentration gradient is a result of the temperature dependence of NTO vapor pressure on temperature given in Figure K-2. In the presence of nucleation sites on the walls of the pressurization system, it is not possible for the concentration of NTO vapor to exceed the vapor pressure corresponding to the wall temperature without condensing (i.e., the nucleation sites preclude significant supersaturation of the vapor). Therefore, given the temperatures of Figure K-1, there will always be a concentration gradient between the NTO tank and the pressurization system upstream of the check valves. This concentration gradient leads to NTO transport by diffusion through the pressurization system plumbing and permeation/diffusion through the check valve seats.

Diffusion through the feed system plumbing is governed by Fick's Law of Diffusion:

$$\frac{dm}{dt} = DA \frac{dC}{dx} \quad (1)$$

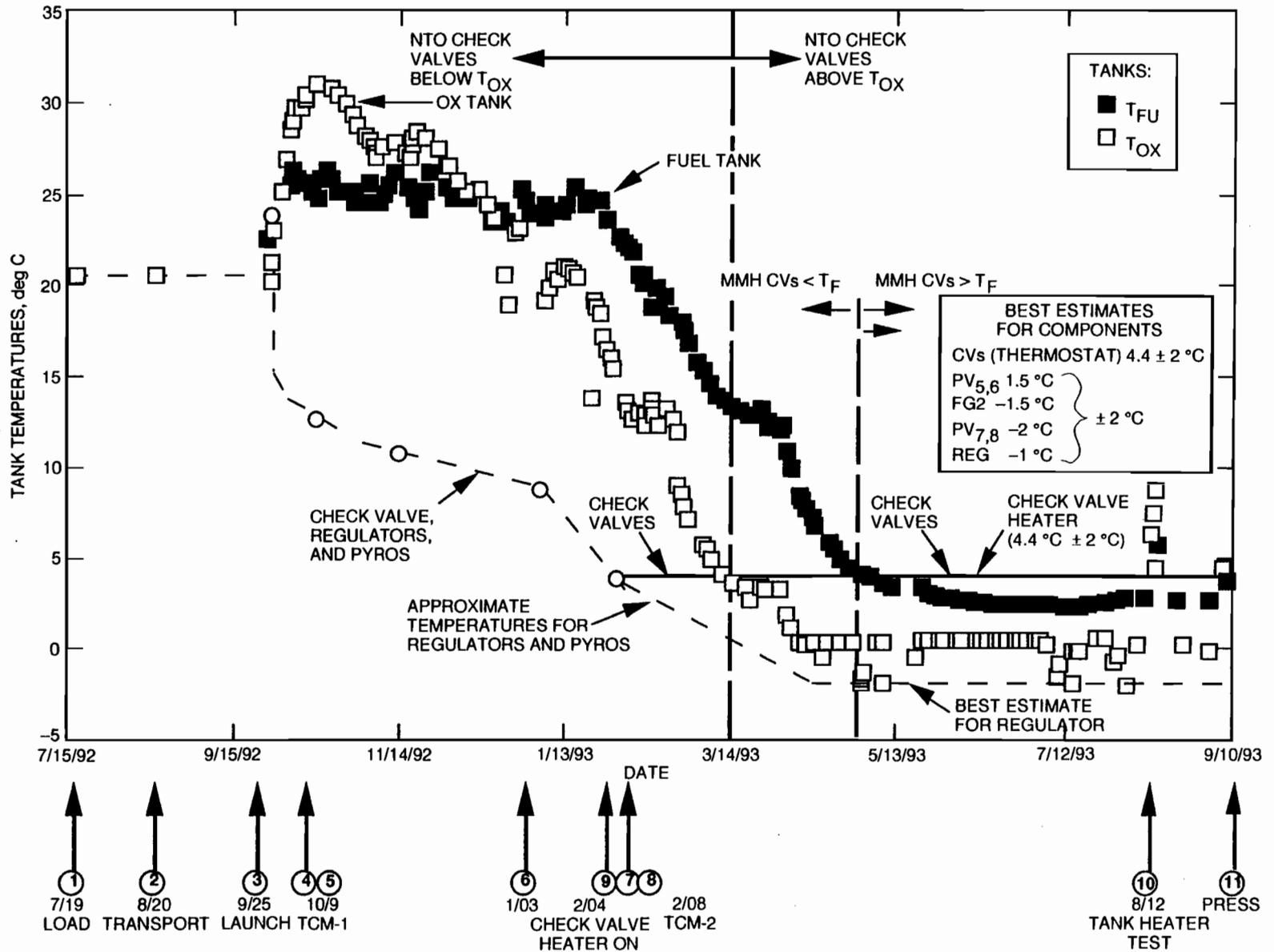


Figure K-1. Tank temperatures versus time.

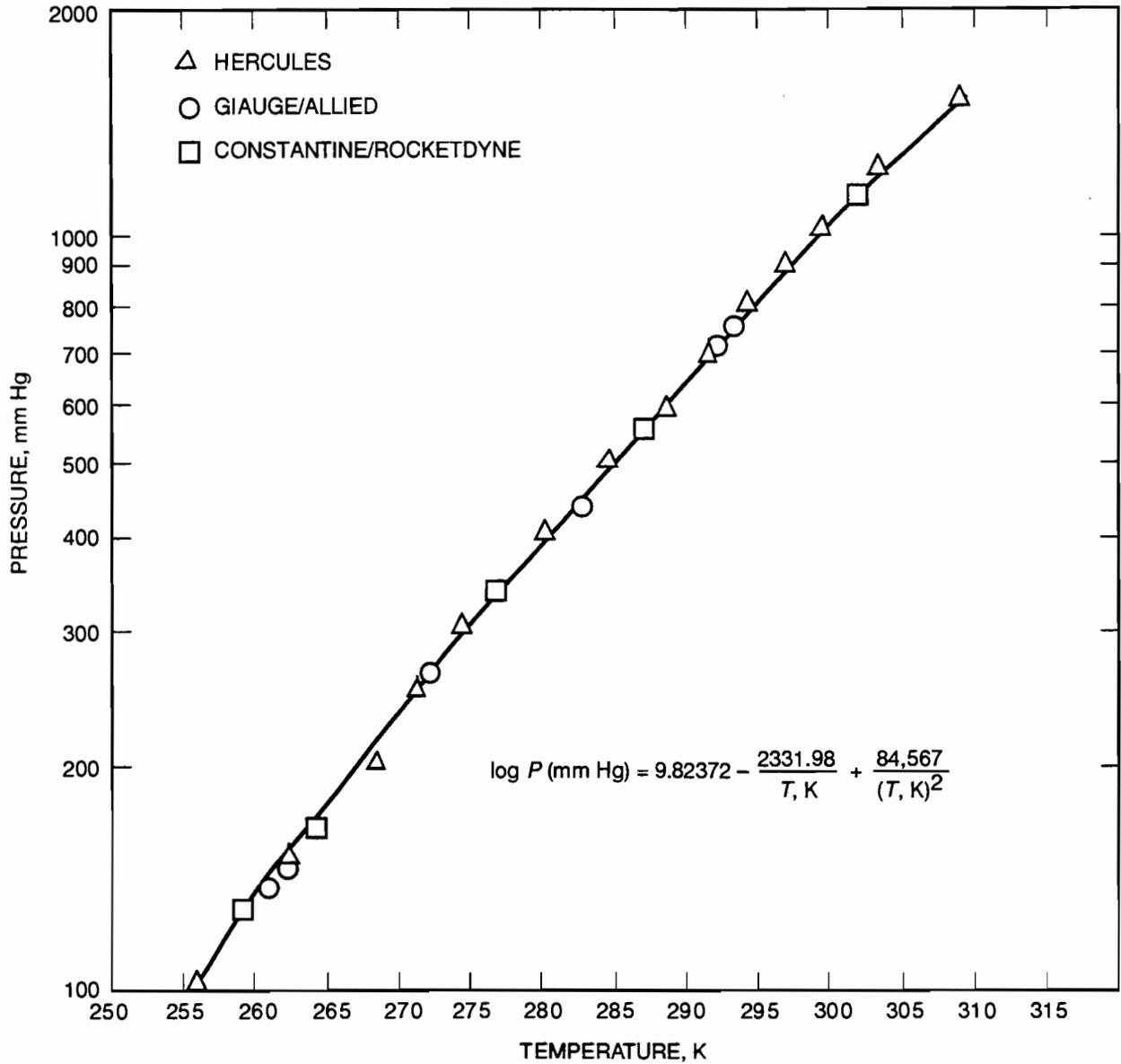


Figure K-2. Vapor pressure versus temperature, liquid nitrogen tetroxide.

where

- dm/dt = mass flow rate
- D = binary diffusion coefficient
- A = flow area in the plumbing
- dC/dx = concentration gradient

The binary diffusion coefficients for NTO vapor (NTO dissociates to NO_2 in the vapor phase) and MMH in GHe are approximately $0.023 \text{ cm}^2/\text{s}$ and $0.019 \text{ cm}^2/\text{s}$,

respectively, at a pressure (P_0) of 276 psia and temperature (T_0) of 298 K.¹ The NTO diffusion coefficient has essentially been validated by an experimental program.² The actual quantity of NTO diffused through an experimental test apparatus exceeded values computed using these diffusion coefficients by 80 percent. The measured diffusion coefficients may be artificially high due to convective effects in the Earth's gravity. The diffusion coefficients may be corrected to other pressure and temperature conditions in accordance with Gilliland's equation:

$$D = D_0 (T/T_0)^{1.5} (P_0/P) \quad (2)$$

NTO transport through the check valve seats is due to a combination of permeation through the seat material itself and diffusion through any leak paths which may be present around the seat. These phenomena are modeled by the following relations:

$$(dm/dt)_{\text{permeation}} = r(A_p/l_p) RT \Delta C \quad (3)$$

where

- r = permeation constant of the seat material (generally a function of T)
- A_p/l_p = ratio of permeation flow area to permeation path length
- R = gas constant of vapor
- T = absolute temperature
- ΔC = concentration (i.e., NO₂ density) change across the check valve seat

$$(dm/dt)_{\text{diffusion}} = D(A_d/l_d) \Delta C \quad (4)$$

where

A_d/l_d = ratio of diffusion flow area to diffusion path length

Due to their similar forms, Equations (3) and (4) can be combined to model permeation and diffusion through the check valves in terms of one empirical quantity:

$$(dm/dt)_{\text{total}} = K_{cv} \Delta C \quad (5)$$

where the empirical check valve parameter K_{cv} is a function of the check valve design, temperature, and operating pressure. Empirical characterization of K_{cv} for the check valve types used in the Mars Observer Pressurization System will be documented.³ As of this writing, the experimental program to characterize NO₂ transport through the check valves is still in progress. The full program will characterize the transport of NO₂

¹ E. F. Cuddihy, A. Yavrouian, and G. Blue, *Diffusion Modeling of the MO Liquid Propulsion Subsystem*, JPL Interoffice Memorandum EFC-514-19-92, Jet Propulsion Laboratory, Pasadena, California, March 26, 1992.

² C. Jennings and R. French, *Mars Observer Check Valve Test Report*, JPL Interoffice Memorandum 353MO-93-029, Jet Propulsion Laboratory, Pasadena, California, to be released.

³ Ibid.

across both types of check valves (Vacco and Futurecraft) used in the MO Pressurization System with and without liquid present at the check valve seat and at two temperatures. To date, data have only been reduced and analyzed for one ambient temperature test of a Vacco check valve with liquid present at the valve seat. This test yielded a value for K_{cv} of approximately $1.5 \text{ cm}^3/\text{hr}$.

This value of K_{cv} is significantly larger than had been expected, but is considered credible. It is possible that the continuing test program will lead to significant revisions in the value of K_{cv} for the Futurecraft check valve design and/or under other conditions. However, this value of $1.5 \text{ cm}^3/\text{hr}$ will be used as the best value available at the deadline for material changes to this report. (Note: Subsequent test results are exhibiting some scatter, but, with one exception, are slightly lower than the preliminary result used in this report.)

Given the temperature data of Figure K-1, pressurization system geometry scaled from drawings, and the check valve characterization data described above, it is possible to compute the NTO transport and condensation in the feed system. The model developed to perform this calculation will be documented in a JPL memo.⁴ The resulting best estimate is that 1.2 grams of NTO could diffuse into the Pressurization System, with 1.0 gram condensing in the pressurization system prior to the pressurization event, assuming that both NTO check valves operate like the test unit.

After integration of the check valves into the Mars Observer Propulsion System, it was no longer possible to verify that both series redundant check valve assemblies were functioning properly. Errors in test procedures described under PFR F0796 were believed by the former Astro employee who conducted that test and the regulator manufacturer to be of a type which has been observed to lead to strong dynamic interactions between the regulator and check valves. Although subsequent leak checks and regulator functional tests indicated no damage, it is not known whether one of the series-redundant check valve assemblies was damaged.

The integrity of one of the check valve assemblies manufactured by Futurecraft, Inc., is also suspect because of the use of Kalrez 1050 elastomer as the sealing material. This material uses carbon black as a filler and is not considered suitable for long-term use in an NTO environment by its manufacturer (DuPont). No long-term propellant compatibility data have been located for this material, but Kalrez 1045, a similar elastomer which uses titanium dioxide filler, has been evaluated in tests of up to 80 days.⁵ The conclusions of that study include that (1) there was "clear evidence of an irreversible chemical change in the material" and (2) "These results indicate that Kalrez cannot withstand indefinite exposure to N_2O_4 ."

⁴ R. French, *Mars Observer Propellant Migration Analysis*, JPL Interoffice Memorandum 353MO-93-025, Jet Propulsion Laboratory, Pasadena, California, to be released.

⁵ M. P. Easton, et al., "Effects of Nitrogen Tetroxide Exposure on DuPont Kalrez 1045," *POLYMER*, vol. 34, no. 7, 1993.

For these reasons, the potential impacts of NTO which condensed in the Mars Observer Pressurization System have been evaluated assuming that one of the series-redundant check valves may have failed. This would result in approximately 2.4 g of NTO diffusing into the Pressurization System, with 2.2 g condensing, so that the results presented below are conservative. The failure of both of the series-redundant check valve assemblies was considered extremely unlikely and was not studied in detail.

Since no check valve testing has been conducted using MMH, the results of the NTO diffusion calculations were scaled by the ratio of MMH to NTO vapor pressures at 5 °C. This is considered reasonable because both vapors have the same molecular weight. Assuming that both MMH check valves operated identically, this results in 0.05 g of MMH condensing between the MMH check valves and the low-pressure pyro valves PV-5 and PV-6. Allowing for the possible failure of one check valve, 0.10 g of MMH could have condensed at this location.

II. Hydrodynamic Impact Damage ("Liquid Bullet") Mechanisms

The temperature estimates of Figure K-1 support the hypothesis that the bulk of the liquid NTO that condensed in the Pressurization System may have collected upstream of the regulator. Even though some liquid may have initially condensed downstream of this point, the dependence of oxidizer surface tension on temperature would promote migration of these condensed liquids toward the coldest portion of the system. No rate calculations have been made for this liquid migration, but it seems reasonable to assume that most of the possible migration would occur in times short in comparison to a month.

The geometry of the Pressurization System upstream of the regulator is shown in Figure K-3. As shown in the figure, a slug of condensed NTO (i.e., a "liquid bullet") could be located just downstream of the primary high-pressure pyro valve (PV-7). Given the uncertainties in the thermal analysis, it is also possible that this condensed NTO would be in other locations, but this is the worst-case location from the standpoint of hydrodynamic damage. In this situation, the opening of PV-7 would suddenly allow the helium tank pressure of 3726 psia to drive the slug of condensed NTO into the pressurization system tubing, which contains helium at a pressure of approximately 170 psia. If the liquid remains intact, it can be accelerated to very high velocities. Parametric analysis of this situation⁶ produced theoretical impact pressures from 2 to 3.3 times the theoretical burst pressure of the tubing (37,000 psia) and fittings (18,000 psia) used in this portion of the Pressurization System.

This analysis treated the slug as a rigid body, but accounted for the wall friction factor, the expansion wave that will propagate upstream of PV-7, and the shock wave which will propagate downstream of the slug. Impact pressures at the fitting identified as "Impact Point" in Figure K-3 were estimated by the relations normally used to

⁶ P. Garrison, *Mars Observer—"Liquid Bullet" Theory*, JPL Interoffice Memorandum 353A-93-352, Jet Propulsion Laboratory, Pasadena, California, October 26, 1993.

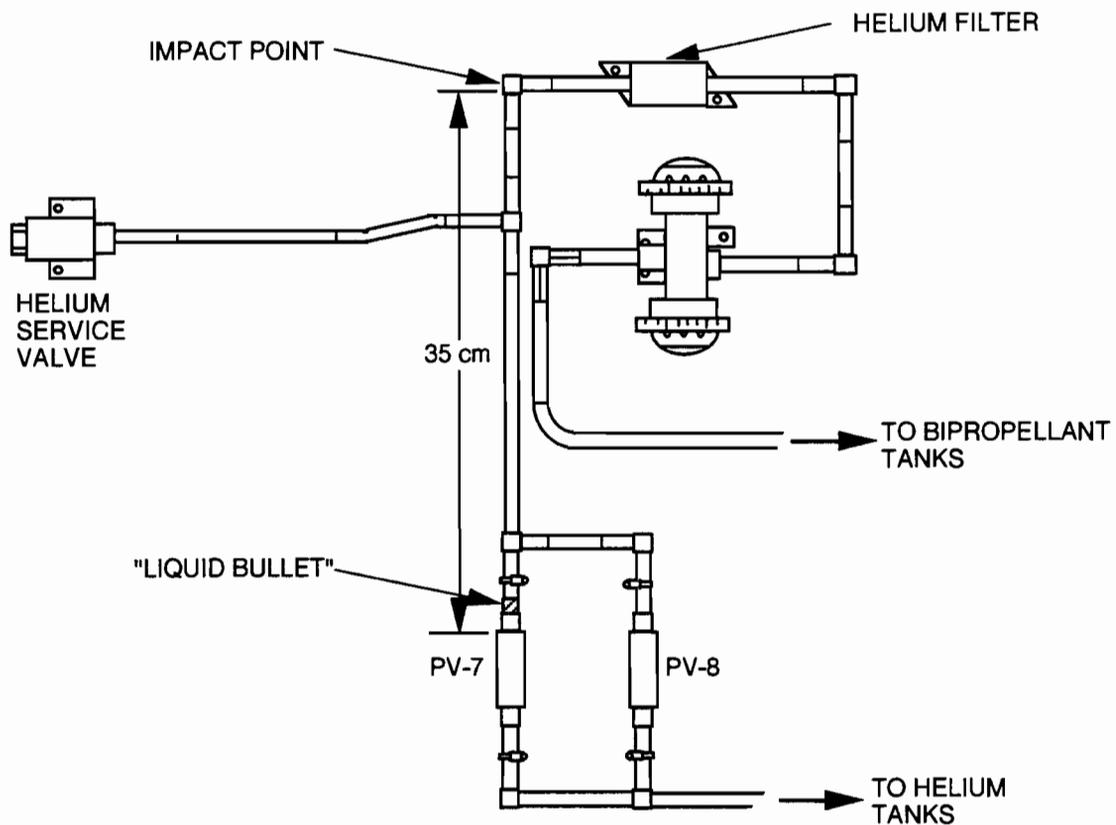


Figure K-3. Geometry of the Pressurization System upstream of the regulator.

compute water hammer overpressures. This is conservative in that it assumes the slug is constrained from expanding in a radial direction by elastic tube walls. In fact, some of the flow will expand into the turn, the slug may not be in contact with the tube walls at impact, and the Pressurization System tubing may yield, all of which will tend to reduce the overpressure. Most fluid mechanics experts consulted were essentially certain that the liquid slug would, in fact, be atomized by the pressure differential across it. Other potentially mitigating effects not considered in the analysis are the potential reduction in driving force due to diversion of helium to plumbing leading to PV-8 and the Helium Service Valve shown in Figure K-3 and the finite (order of 0.1 ms) opening time of the pyro valve.

In order to eliminate the conservatism associated with analysis of this scenario, tests have been conducted.⁷ These tests were conducted using flight-like tubing and fittings to determine whether damage was incurred when NTO slugs of various sizes were accelerated into the "impact point." Two tests have been conducted using one and two grams of NTO; no damage was detected by visual inspection, proof, or leak tests.

⁷ H. Long, *Liquid Bullet Test Results*, JPL Interoffice Memorandum 353MO-93-026, Jet Propulsion Laboratory, Pasadena, California, to be released.

Although further tests could prove to the contrary, engineering judgment suggests that failure of the Pressurization System by this mechanism is not very credible. However, the effects of such a hypothetical rupture would probably be consistent with the observables in the Mars Observer loss-of-signal anomaly, as discussed below.

If the Pressurization System were to rupture due to liquid NTO impingement at the impact point shown in Figure K-3, the contents of the helium tank would be vented in about 90 s, as shown in Figure K-4. This result is from an analysis by Garrison.⁸ That reference also predicts that the peak pressure within the spacecraft thermal blankets is approximated by:

$$P_{\text{blanket}} = 66.4 \text{ lbf} / A_{\text{vent}}$$

where A_{vent} is the total vent area of the thermal blanket. The total vent area of 50 square inches⁹ would therefore yield an internal blanket pressure of 190 psf, which is more than enough to produce major tears in blanket seams. The maximum pressure capability of the blanket is given as 6 psf¹⁰ and was validated by test on another program (per discussion with R. Becker). Therefore, it is likely that the helium would be vented in essentially one direction. The total impulse associated with this venting is given by Garrison as approximately 5000 N s.

Assuming this impulse would act over a moment arm of the order of 1 m yields a minimum angular rate of 92 deg/s if the rotation is about the Y-axis. Rotation about other axes would be faster, and the geometry of Figure K-3 implies that the rotation would be primarily about the X- and Z- axes, with the largest moment arm about the X-axis. At these rotation rates, it would not have been possible to detect a downlink signal from Mars Observer, even on the LGA.

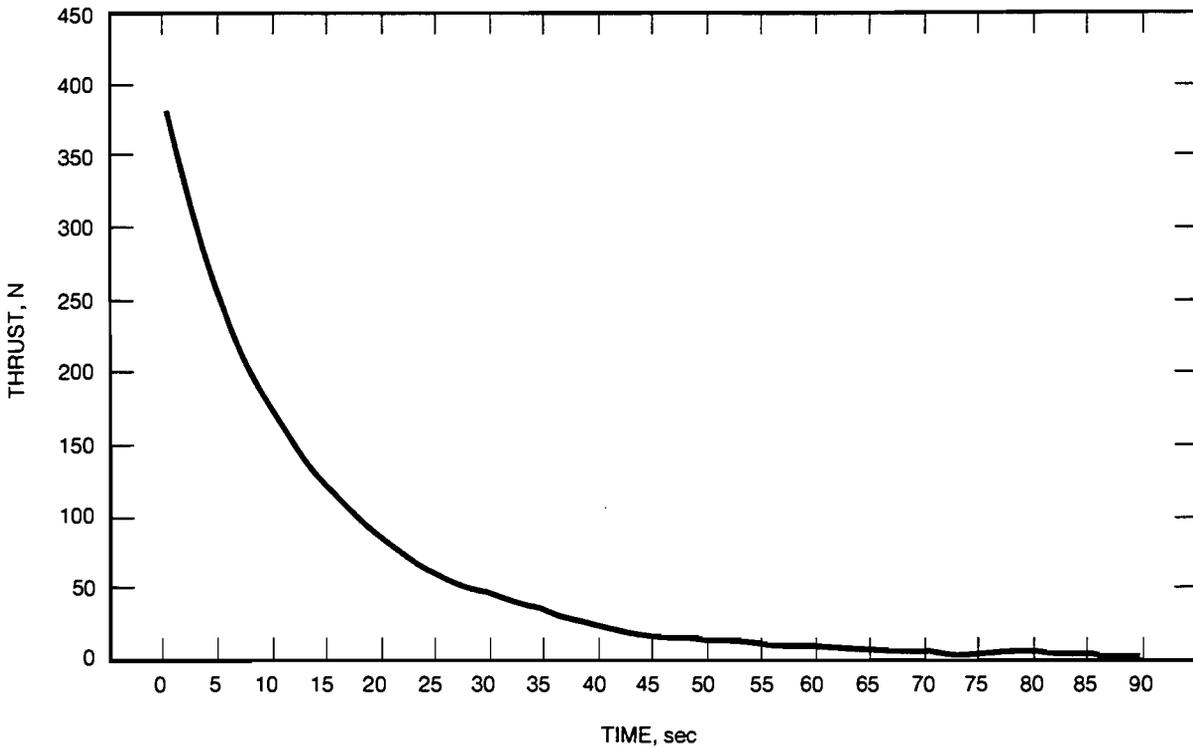
III. NTO/MMH Reactions in the Pressurization System

Figure K-5 shows the layout of the Pressurization System downstream of the regulator. Upon firing of high-pressure pyro valve PV-7 (not shown in Figure K-5), helium pressurant and any condensed NTO will flow from the regulator toward low-pressure pyro valves PV-5 and PV-6 as shown in Figure K-5. Shortly before reaching those pyro valves, there is a "T" fitting which branches off toward the NTO check valves and NTO tank. After an initial transient, most of the helium pressurant will make this 90° turn. However, the liquid NTO (whether in the form of a slug or droplets) will tend to collect in the dead-end tubing upstream of pyro valve PV-6. This inertial effect is similar to that used in inertial separators of all sorts. Once in this relatively quiescent dead volume, the NTO will tend to remain there except for vaporization and diffusion effects. Therefore, it is reasonable (but conservative) to assume that a significant fraction of the

⁸ P. W. Garrison, *Mars Observer—Disturbance Produced by Rupture of Pressurization System Line*, JPL Interoffice Memorandum 353A-93-351, October 26, 1993.

⁹ O. Liu, *Revised Response to AI#3 (ver. B)*, MO Thermal Subsystem CDR, 9-26-89, GE IOM MO-AI-103-B, September 5, 1991.

¹⁰ *Ibid.*



TIME, sec	PRESSURE, N/m ²	TEMPERATURE, K	THRUST, N	FLOW, kg/sec	Is, m/sec
0	2.569×10^{-7}	269	385.1	0.288	1338
5	1.696×10^{-7}	228	254.3	0.206	1232
10	1.156×10^{-7}	196	173.3	0.152	1141
15	8.101×10^{-8}	170	121.4	0.114	1062
20	5.811×10^{-8}	149	87.1	0.088	994
25	4.256×10^{-8}	131	63.8	0.068	934
30	3.174×10^{-8}	117	47.6	0.054	881
35	2.406×10^{-8}	104	36.1	0.043	833
40	1.851×10^{-8}	94	27.7	0.035	791
45	1.442×10^{-8}	85	21.6	0.029	752
50	1.137×10^{-8}	77	17.0	0.024	717
55	9.066×10^{-9}	71	13.6	0.020	685
60	7.299×10^{-9}	65	10.9	0.017	656
65	5.929×10^{-9}	60	8.9	0.014	630
70	4.856×10^{-9}	55	7.3	0.012	605
75	4.008×10^{-9}	51	6.0	0.010	582
80	3.332×10^{-9}	47	5.0	0.009	561
85	2.788×10^{-9}	44	4.2	0.008	541
90	2.347×10^{-9}	41	3.5	0.007	523

ASSUMPTIONS:

$L = 3.5$ m

$L/D_{bends} = 408$

Figure K-4. Effects of blowdown of the helium tank.

NTO condensed in the feed system would be in this dead-ended section when PV-5 was fired to pressurize the MMH tank. (Note that the designation of PV-5 and PV-6 in mechanical design drawings differs from that given in electrical cabling drawings, introducing some uncertainty as to which valve was actually fired.)

As discussed above, up to 0.10 g of liquid MMH may have condensed between the MMH check valves and PV-5. Per the temperature estimates of Figure K-1, the most likely place for this MMH to have accumulated is near the filter FG-2 shown in Figure K-5. Reaction of this MMH with the NTO from upstream would be possible in this filter. The peak pressures required to expel the reaction products from the filter have been estimated by evaluating the stagnation pressure required to force the reaction products through the Pressurization System lines at sonic velocity. This calculation was performed using the One-Dimensional Equilibrium (ODE) computer code.¹¹ Calculations were made to compute the density and velocity of sonic flow for stagnation pressures of 1000, 5000, and 20,000 psia. The mass flow through the pressurization lines at each pressure is the product of the sonic density, velocity, and the tube flow area (0.6 cm²). The rate at which reaction products must be expelled from the filter is roughly estimated by dividing the total quantity of reactants (conservatively assumed to be 2.3 g) by the reaction time over which the propellants are assumed to combust. The results of these calculations are presented in Figure K-6. This figure indicates that pressures internal to the MMH filter are unlikely to exceed 5000 psia unless the reaction time is less than 1 ms. This is essentially because the reaction is significantly limited by the small amount of MMH which may be available upstream of the check valves. This conclusion, however, depends on the assumption that the reaction of the MMH and NTO is unlikely to occur in under 1.0 ms. This is based on the engineering judgments of a number of people familiar with hypergolic reactions who were interviewed during this investigation. It must also be admitted that the simplified analysis method used here could produce nonconservative results, although conservative reactant quantities were used. Experimental investigations are underway at the USAF Phillips Laboratory to validate these engineering judgments and reduce analytical uncertainty.

Discussion with the filter vendor (Vacco, Inc.) revealed that the theoretical burst pressure of this filter is approximately 15,000 psia. Pending receipt of Vacco analyses to this effect, it is tentatively concluded that even if this reaction had occurred it is unlikely that the filter would have burst. Similarly, the burst pressure of the tubing and fittings exceeds 10,000 psia (based on burst test data of weld samples), and the burst pressure of the check valves is claimed by the vendors to exceed 15,000 psi.

The next opportunity for the NTO ingested into the MMH Pressurization System to react with MMH is at the service valve "T" shown in Figure K-5. Because of the large temperature gradient between the MMH tank and check valves early in the mission (see

¹¹ S. Gordon and B. J. McBride, *Computer Program for Calculation of Complex Chemical Equilibrium Compositions, Rocket Performance, Incident and Reflected Shocks, and Chapman-Jouguet Detonations*, NASA SP-273, 1971.

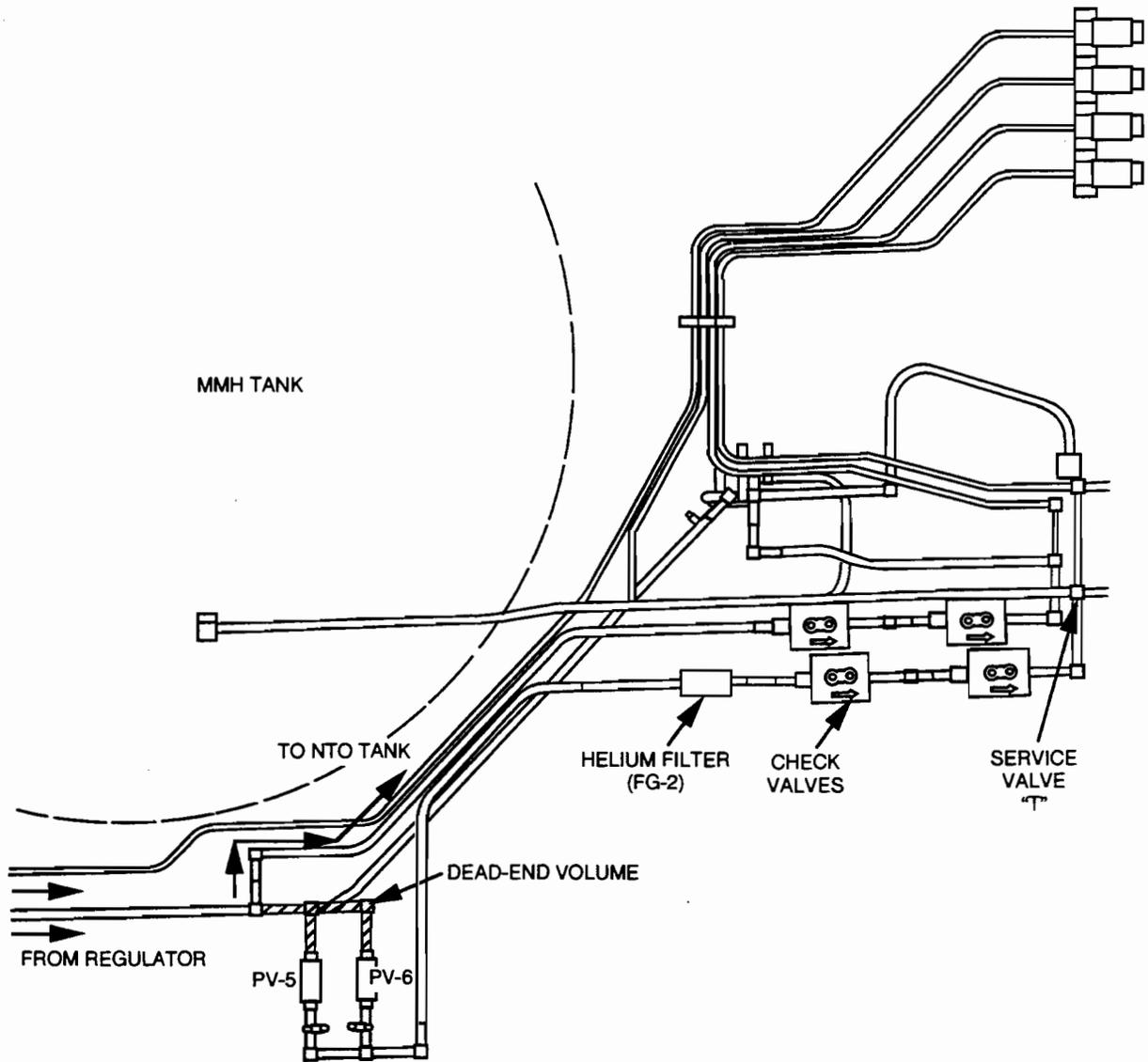


Figure K-5. Pressurization System plumbing layout.

Figure K-1), there is a significant chance that liquid MMH accumulated in large quantities in the vicinity of this "T" prior to pressurization. Therefore, the quantity of MMH which could react with the NTO in this location is not readily bounded.

The line pressures which could result from reactions in this portion of the Pressurization System were computed by using ODE thermochemical calculations in a manner similar to that described for computing pressures in the filter FG-2. Two cases were analyzed to consider the effect of varying quantities of MMH which might be present: (1) stoichiometric, with an oxidizer-to-fuel ratio (O/F) of 2.5, and (2) a case where equal quantities of each propellant are present ($O/F = 1$). The results of these calculations are shown as a function of reaction times in Figures K-7 and K-8, respectively.

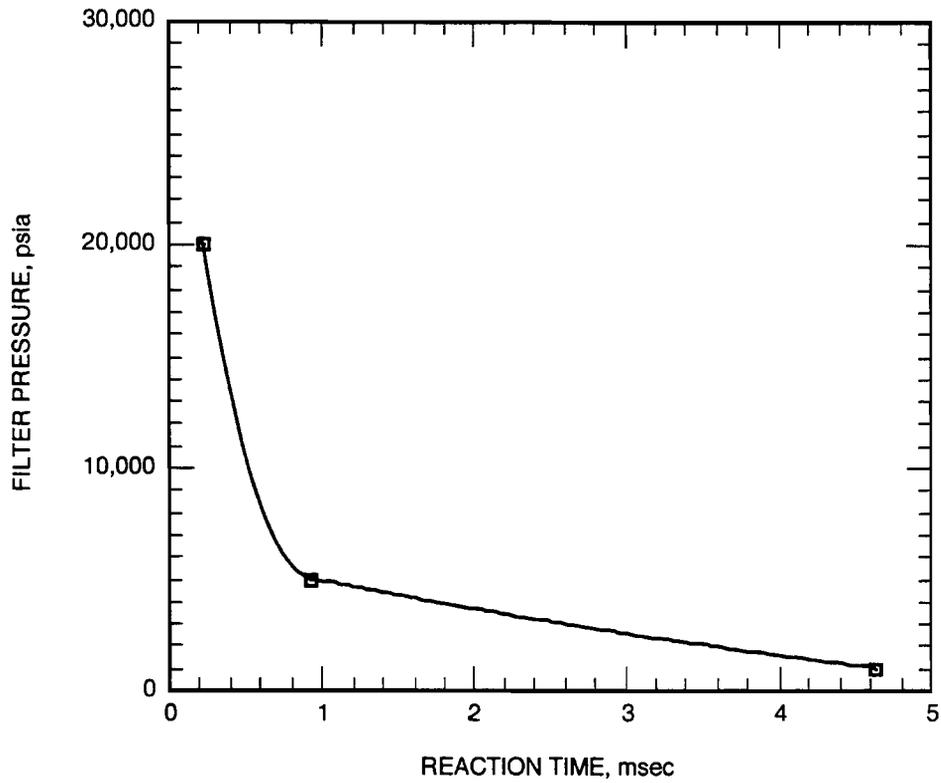


Figure K-6. Estimated pressure in filter FG-2 (reactants are 2.2 g NTO and 0.1 g MMH).

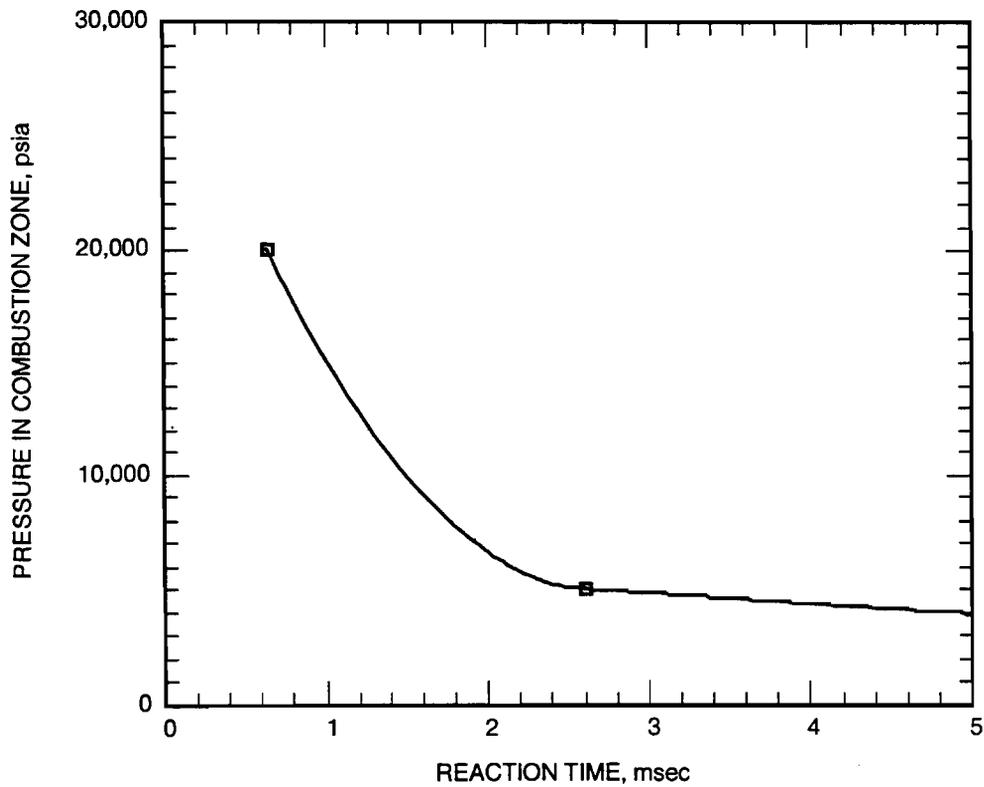


Figure K-7. Estimated line pressures for the oxidizer-to-fuel ratio = 2.5 reaction at "T" (reactants are 2.2 g NTO and 0.9 g MMH).

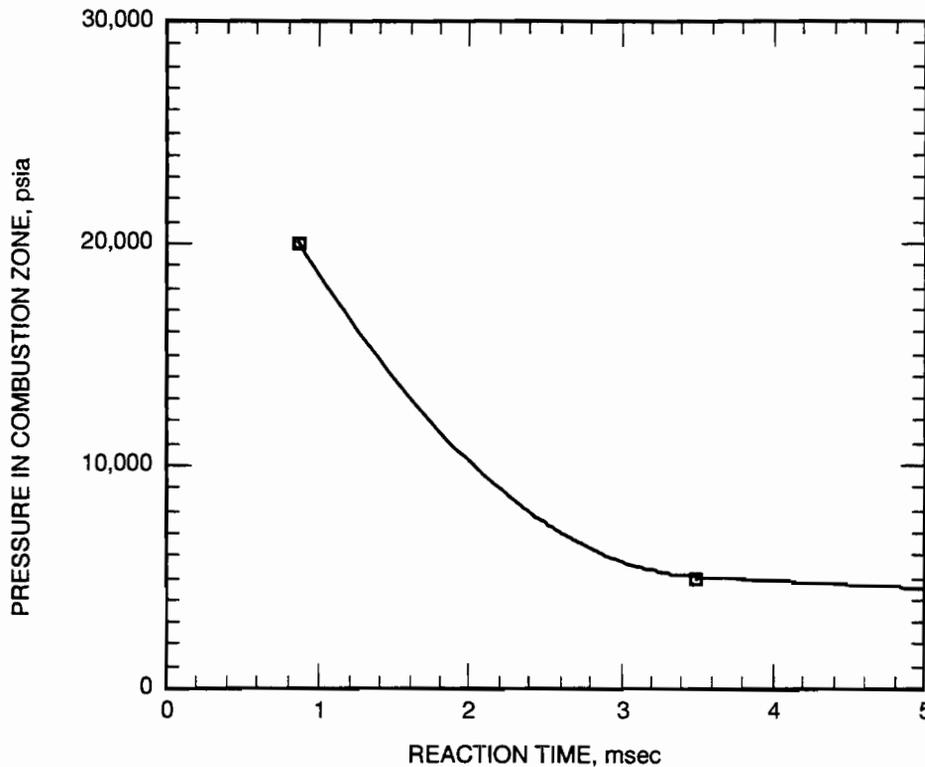


Figure K-8. Estimated line pressures for the oxidizer-to-fuel ratio = 1 reaction at "T" (reactants are 2.2 g NTO and 2.2 g MMH).

A comparison of Figures K-7 and K-8 reveals a fairly weak dependence of the predicted pressure on the *O/F* ratio, but indicates that the predicted pressures are highly sensitive to reaction rate. As discussed above, reaction times of the order of 1 ms are considered credible and, in the results presented in Figures K-7 and K-8, result in pressures above the theoretical burst pressure of the lines (12,000 psia) and the minimum measured burst pressures of weld samples (10,000 psia).

It has been suggested that any reactions which may occur upstream of the MMH check valves may reduce the quantity of NTO available for combustion in this region of the line. This is true, but the amount of MMH available upstream of the check valves should only be able to react about 10 percent of the oxygen in the NTO. The remaining oxygen, in the form of residual NTO droplets and/or hot combustion gases, will still be available for reaction downstream of the check valves.

Rupture of pressurant lines downstream of the MMH check valves therefore appears to be possible. The credibility of this conclusion depends strongly on the actual quantity of NTO which may condense in the pressurization system and the reaction rate which could occur. The ongoing check valve experiments at JPL and the combustion experiments being conducted at the USAF Phillips Laboratory may serve to reinforce or diminish the credibility of this failure. Based on the information available at the deadline for this report and engineering judgment, this failure is thought to be credible.

The effect of a line or fitting rupture in this portion of the feed system would include venting of helium and large quantities of MMH into the volume within the spacecraft thermal blankets. The potential for impulses of up to 5000 N s due to helium venting would still exist, but the venting would occur over nearly 1800 s due to the flow restrictor orifice in the regulator. The maximum pressure within the blankets for this case would be only $1.8 \text{ lbf}/A_{\text{vent}}$ (= 5 psf for the 50-square-inch venting area of Footnote 8), so there is a good chance that the helium would pass through numerous small vent paths in the thermal blankets; the effective angular impulse would be much less than in the case of a rupture upstream of the regulator. However, even if the torque impulse were reduced by an order of magnitude, the resulting rates could be sufficient to preclude detection of a downlink signal. As a minimum, attitude disturbances would probably be severe enough to preclude HGA downlink. The corrosion effects of massive MMH venting have not been evaluated in detail, but could reasonably inflict critical physical damage on the spacecraft. However, tests in which insulated wires were exposed to propellants¹² indicate that such corrosion effects could be very slow in comparison to the 14-min period the transmitters should have been turned off.

The ultimate opportunity for liquid NTO (or reaction products from partial reactions upstream) to interact with MMH is in the MMH tank. Based on ODE calculation of final tank conditions, such a reaction is extremely unlikely to threaten the integrity of the tank unless a significant fraction of the MMH decomposes even for NTO quantities as high as 20 grams. The majority of experts consulted believe this is extremely unlikely. Decomposition of a quantity of MMH does provide enough energy to decompose a larger quantity of MMH, leading to the possibility of a decomposition flame in the MMH tank. Such decomposition flames have been observed in monopropellant hydrazine, but have never been observed in MMH. It is likely that the kinetics of MMH decomposition preclude sustaining such a decomposition flame, but this has never been rigorously verified. The NTO/MMH interaction tests being conducted at the Phillips Laboratory have as a key objective determining whether such a flame is possible in geometries similar to those of the potential interactions in the Mars Observer spacecraft Propulsion System. Rupture of the MMH tank would cause critical physical damage to the spacecraft, but, contingent on the results of the Phillips Laboratory experiments, such a rupture by this mechanism is considered almost impossible.

¹² M. Anderson, *MO Wires Exposed to NTO and MMH: Electrical Short Test*, JPL Interoffice Memorandum 355-615-93:MA, Jet Propulsion Laboratory, Pasadena, California, October 28, 1993.

APPENDIX L

FRACTURE MECHANICS DESIGN OF BIROPELLANT TANKS

There are five pressure vessels in the Mars Observer Propulsion System: one helium (GHe) pressurant tank, two hydrazine tanks, one nitrogen tetroxide (NTO) tank, and one monomethylhydrazine (MMH) tank. All of these pressure vessels, except the pressurant tank, are made of a titanium alloy (Ti-6Al-4V STA). The pressurant tank is of a graphite overwrap design, with a stainless steel liner. Since the two bipropellant (NTO and MMH) tanks were being pressurized when the loss-of-signal (LOS) anomaly occurred, safe-life design of these tanks is of special interest and was thoroughly reviewed.

Fracture mechanics analyses of the Mars Observer bipropellant tanks, which formed the safe-life design of these tanks, were performed by Foster Engineering,¹ using the 1989 version of the software NASA/FLAGRO². NASA/FLAGRO, which was developed by a joint effort of NASA centers, the Air Force, and the European Space Agency, is well accepted by the industry and is considered to be the best safe-life analysis software available.

NASA/FLAGRO calculates the safe life by integrating the crack growth rate for the tank material, which is described by the generalized Forman equation, over the service life spectrum of the tank. The Forman equation relates the crack growth rate, da/dN , to the stress intensity factor K . The value of K at the critically stressed locations was determined internally in NASA/FLAGRO, based on the standard solution for a part-through semi-elliptic flaw in a finite-width plate. The stresses of the Mars Observer bipropellant tanks were obtained from closed-form solutions for the membrane region and from finite-element models for the ring, weld, inlet, and outlet regions.³ The constants in the Forman equation available in the NASA/FLAGRO database for the tank material, Ti-6Al-4V STA, were used, and they were generated from test data for different temperatures and processes (e.g., aged, stress-relieved) and account for crack closure by Newman's model.

The service life spectrum that was used for the Mars Observer bipropellant tank analyses consisted of (1) the pressure-induced loads during room temperature proof tests, cryogenic proof test, leak checks, pressurization for spacecraft vibration tests, and the launch and mission and (2) the dynamic loads during vibration tests and launch, all of which occurred during the time interval beginning with the determination of the initial crack size used in the analysis through to the completion of launch. The effect of stress-corrosion cracking under sustained loading following launch and during the interplanetary cruise was also considered in Foster Engineering's analyses.

¹ H. M. Braund, *Fracture Mechanics Analysis of the Mars Observer Bipropellant Tanks, Revision B*, Foster Engineering Company Report No. 89-005B, November 1989.

² Fatigue Crack Growth Computer Program—NASA/FLAGRO, JSC-22267, 1989.

³ L. J. Hicks, *Structural Analysis of the Mars Observer Bipropellant Tanks, Revision A*, Foster Engineering Company Report No. 88-066A, February 1989.

The initial crack sizes used in the safe-life analyses were the smallest cracks screened by any of the three non-destructive examination (NDE) methods that were employed for the Mars Observer bipropellant tanks, namely (1) cryogenic proof pressure tests, (2) dye-penetrant inspection, and (3) radiography. The initial crack sizes based on the cryogenic proof test were estimated using the option provided in NASA/FLAGRO, which iteratively calculates a critical crack size, given a critical K value at the cryogenic temperature. The initial crack sizes established from dye-penetrant or radiographic inspection correspond to the special levels used for the NASA Space Transportation System (STS) orbiter.

In the safe-life analyses, the end of life for the tank is signaled by one of the following three conditions: (1) the semi-elliptic part-through crack growing to become an unstable crack when K reaches a critical value (i.e., a burst); (2) the part-through crack grows through the thickness of the tank (a leak); or (3) the part-through crack growing due to stress corrosion if $K > K_{ISCC}$, where K_{ISCC} is the threshold value of K for the initiation of stress-corrosion cracking. The stress corrosion due to sustained stress was checked by comparing the maximum K for the crack existing after launch with K_{ISCC} for the material. When a part-through crack in the tank grows through the thickness of the tank before its growth becomes unstable, the tank is said to have a leak-before-burst mode of failure. Both Mars Observer bipropellant tanks are leak-before-burst in the membrane region.

The safe-life analyses were performed by Foster Engineering at three critical regions; namely, the membrane region of $t = 0.036$ in. (0.9144 mm), the most critical parent material section of $t = 0.040$ in. (1.016 mm), and the weld of $t = 0.060$ in. (1.524 mm). For the parent material section and the weld, different analyses were performed for a flaw being in the inner and outer walls. In each case, two extreme semi-elliptic flaw shapes were used, $a/c = 0.4$ and $a/c = 1.0$, which would bound the possible shapes of the initial flaw and hence their outcomes. The depth of these initial flaws was established by the cryogenic proof tests or the NDE inspections.

Compared to proof testing at the ambient, the advantage of a cryogenic proof test is that cracks of smaller sizes can be screened. This is due to the fact that the fracture toughness of the material decreases at lower temperatures (-320 °F for Mars Observer bipropellant tanks), and it also allows higher proof pressures to be employed (600 psi used for Mars Observer bipropellant tanks) because yield and ultimate strengths for the tank material are higher at lower temperatures. The minimum of the smallest crack size screened by the cryogenic proof test and that screened by radiography and follow-on dye-penetrant inspection was used. For all of the cases in the membrane region and the parent material section, the cryogenic proof test established the initial flaw size used in the analysis. In the weld region, cryogenic proof test provided the initial flaw size used in the safe-life analysis for the crack on the outer wall with an $a/c = 0.4$. For other cracks in the weld, the radiographic inspections established the initial crack depth of 60 percent of weld thickness. The initial flaw sizes established by radiography and dye-penetrant inspections were considered to be suspect because (1) the detection sensitivity of the radiographic method was greatly reduced for these tanks since two walls of the structure were being inspected at the same time, and (2) the dye-penetrant inspection

that follows radiography could not detect embedded cracks or cracks that are on the inner surface of the weld.

Two safe-life analyses of Mars Observer bipropellant tanks were conducted for each location and crack configuration. The first used a safety factor (SF) of 1.0, and the crack growth life was verified to be greater than four times the service life. The second was with an SF of 1.35, and the crack growth life was verified to be greater than a single service life. In all the cases analyzed, the safe-life requirements were met, and it was verified that crack growth was stable until the flaw grew all the way through the thickness (i.e., satisfied the leak-before-burst criterion).

At the end of the service life in each crack growth analysis, the value of the stress intensity factor K at the maximum expected operating pressure (MEOP) of 300 psi and for the final crack size a_f was compared with the threshold value K_{ISCC} to check whether stress-corrosion cracking would occur following launch during the interplanetary transit. The largest K value was 24.1 kris in the membrane region for an initial $a/c = 1.0$, and this value was below the threshold $K_{ISCC} = 38$ kris. Thus, it was verified that stress-corrosion cracking was not possible for the bipropellant tanks during the Mars Observer mission.

In addition to meeting the safe-life requirements by analysis, the design of the tanks was also test-qualified per the requirements in MIL-STD-1522A.⁴ This included acceptance tests, pressure cycling, sine and random vibration tests, leak rate tests, and the burst test. The acceptance tests required room-temperature and cryogenic proof tests and radiographic and dye-penetrant inspections, which were performed before and after the proof tests. The pressure cycle life test required surviving 50 pressure cycles at MEOP (300 psi). The tank satisfied all qualification and acceptance requirements, and the final burst pressure was over 600 psi, which was much higher than the required 450 psi (1.5 x MEOP).

Several weeks prior to the Titan III launch of Mars Observer, the bipropellant tanks were pressurized to a level of 285 to 315 psi. The tank pressures gradually decreased to a launch level of 250 to 260 psi, and then increased to 265 to 285 psi right after launch. During the 11 months of interplanetary transit, the pressures of the bipropellant tanks again decreased to a level of 160 to 170 psi, due to lower tank temperatures and greater ullage from three TCMs. The target pressure of the tanks for MOI pressurization was 260 psi as controlled by the regulators. The fact that neither a rupture nor a leak was detected during and after the launch events leads to the conclusion that structural integrity, including fracture mechanics design, of the bipropellant tanks was adequate for the Mars Observer mission. It is extremely unlikely that an error related to the design, analysis, fabrication, or quality control of the bipropellant tanks has caused the LOS anomaly. However, this does not preclude the probability that one of the tanks was weakened, either by meteoroid impacts or by impacts of the fragments of another

⁴ MIL-STD-1522A, *Standard General Requirements for Safe Design and Operation of Pressurized Missile and Space Systems*, May 1984.

failed Mars Observer component, and ruptured catastrophically during the MOI pressurization.

Two of the hypotheses that are related to tank rupture, C3A and C3B, assume the existence of a near-through-the-thickness flaw that became a through-the-thickness flaw during the MOI pressurization cycle. These hypotheses also assume that the through-the-thickness flaw grows under stress corrosion until failure because the leak rate of the tank is slower than that of the regulator. A JPL report⁵ contains the analyses related to these assumptions.

⁵ S. Sutharshana, R. Bamford, and N. Moore, *Fracture Mechanics Calculation in Support of the MO Bipropellant Tank Failure Hypothesis*, JPL Interoffice Memorandum 3542-93-310, Jet Propulsion Laboratory, Pasadena, California, October 28, 1993.

APPENDIX M

MARS OBSERVER APPROVED SFP WAIVER SUMMARY

Table M-1 is a summary listing of single failure points approved prior to launch that are pertinent to the hypotheses for the Mars Observer loss-of-signal anomaly. Table M-2 is a summary listing of all Mars Observer SFPs approved prior to launch.

**Table M-1. SFPs addressed in Mars Observer downlink
loss-of-signal anomaly.**

SFP number	Failure	Hypothesis
BO19138	Hybrid coupler fails (no input to TWT)	C11
BO19629	Corrupt gyro data on all axes (IMU function lost) (IMU I/F select erratic)	C15
BO19628	Corrupt data on one axis (IMU function lost) (Gyro channel select erratic)	C15
WD20860	IMU spin motor short (IMU function lost)	N2
BO19627	Erratic clock into CIU (Erratic activity on RXO select line)	S3. C15
BO19103	Regulator fails to open (tank burst)	C2
BO19101 BO19745 BO19746	Tank flaws	C3
WD21123	Open motor shunt (spacecraft power loss)	S2
BO19733	Short pulls 28-V bus below spacecraft operating voltage	S2

Table M-2. Mars Observer approved SFP waiver summary (listing by subsystem).

S/S WAIVER #	SUMMARY DESCRIPTION:	MISSION IMPACT:	RISK ASSESSMENT:
** SUBSYSTEM: AACS WD20860	IMU SPIN MOTOR WINDING SHORT DURING MOI REMOVES AC POWER SUPPLY OUTPUT FROM ALL 3 GYROS CAUSING LOSS OF S/C ATTITUDE CONTROL FUNCTION	LOSS OF MISSION DUE TO DEPENDENCE OF MOI MANEUVER ON GYRO DATA	SOFTWARE CORRECTION PROPOSED BY GE POTENTIALLY CAN NOT CORRECT ERROR BY DETECTING AND REMOVING THE FAULTED GYRO QUICKLY ENOUGH TO RECOVER MOI BIT PROJ ACCEPTED ON BASIS OF LOW PROBABILITY OF FAULT
B020202	1) CSA optic path not redundant 2) All detectors embedded on common substrate. Failed CSA prior to Mapping Orbit will not allow inertial attitude determination	Failure at launch due to vibration or blockage of optical path prior to Mapping Orbit results in Loss of Mission	Design improved by moving CSA to S/C bulkhead. Mtg bracket analyzed & redesigned temperature control initiated special workmanship controls to prevent lens blockage No failure heritage of substrate
** SUBSYSTEM: CADH B019627	Erratic activity on the RXO Backup Select Line due to open circuit (Cracked PWB trace or solder joint) can generate erratic clock into CIU, and disrupt C&DHS Timing	Loss of Spacecraft function	Risk accepted based on adherence to workmanship standards, planned thermal cycling during assembly testing, normal redundancy management, and low calculated failure rate (See JPL IOM 3484-90-225)
B019628	Erratic activity on the Gyro Channel Select Line due to open circuit (cracked PWB trace or solder joint) or internal chip fault in IC can corrupt data on one Gyro axis	Loss of S/C attitude control; inability to orient the S/C for proper communications and therefore, loss of mission	Risk accepted based on adherence to workmanship standards, planned thermal cycling during assembly testing, normal redundancy management; and low calculated failure rate (See JPL IOM 3484-90-225)
B019629	Erratic activity on the IMU interface select line due to open circuit (cracked PWB trace or solder joint) or internal chip fault in digital IC can corrupt gyro data for all axes	Loss of attitude control and hence of mission	Risk accepted based on adherence to workmanship standards, planned thermal cycling of assemblies during testing, normal redundancy management, and low calculated failure rate (see IOM 3484-90-225)
** SUBSYSTEM: POWR B019144	Solar Array Gimbal Actuator nonredundant with potential bind/seizure of motor bearings or mech failure of harmonic drive (from foreign particulates) causing inability to orient solar array	Degradation of solar array power output or complete loss of solar array bus, leading to loss of mission	GE estimated probability of failure of bearings and harmonic drive to be 2.9×10^{-4} and 2.6×10^{-3} assuming 100% duty factor flight duty cycle expected to be 16.25%/actuator Proj Appvd
B019145	Failure of Delay Interpanel Assy could prevent 33% of the Solar Array from deploying. See also Waiver # B019148	Significant degradation of delivered solar array power, loss of ability to handle S/C load demands, leading to loss of mission	Waiver acceptance recommended by JPL Tech Spec per IOM 3524-91-196, based on design features to prevent jamming, structural failure & external contamination & on planned deployment tests & heritage

Table M-2. Mars Observer approved SFP waiver summary (listing by subsystem) (continued).

S/S	WAIVER #	SUMMARY DESCRIPTION:	MISSION IMPACT:	RISK ASSESSMENT:
	B019148	Failure of Delay Interpanel Assy could prevent 33% of the Solar Array from deploying. See also Waiver # B019145	Loss of Solar Array bus power and therefore loss of mission	Waiver acceptance recommended by JPL Tech Specialist / IOM 3524-91-196, based on design features to prevent jamming, structural failure & external contamination & on planned deployment tests & heritage
	B019149	Failure of Delay Bracket Assy could prevent 100% of Solar Array from deploying correctly.	Complete loss of Solar Array bus power and therefore loss of mission	Waiver acceptance recommended by JPL Tech Specialist / IOM 3524-91-196, based on design features to prevent jamming, structural failure & external contamination & on planned deployment tests & heritage
	B019733	BVR HAS ONE TRANSISTOR/CHANNEL IN PRIMARY AND BACKUP CIRCUITS. IF TRANSISTOR SHORTS, BATT V INPUT > 28 V BUS OUTPUT DROPS CAUSING FAILURE OF S/C POWER BUS. (See deleted Cap short Waiver B019734)	Loss of ability to maintain voltage on S/C 28V bus and therefore potential loss of S/C function/mission	JPL Tech Spec. recommended Rej. Waiver pending GE supply analysis of max/min voltage & current required to "Burn-to-open" any short, w/o other damage to other parts of single channel (eg. harneaux)
	B020215	FAIL OF THE SKIP 2 DELAY ASSY COULD PREVENT 66% OF THE ARRAY FROM DEPLOYING	LOSS OF MISSION	Appvd Waiver Accept. rationale same as for Skip 4 hinges see IOM 3524-91-96, based on design features to prevent jamming, stru failure, & external contamination & on planned deployment tests & heritage
	WD21123	PSE has Solar Array meter shunt sensor studs attached with mech. fasteners that if pre-load torques loosen under launch vibration env. could cause open circuit of Solar Array.	Open circuit of Solar Array would cause loss of array bus power and loss of mission	Analyses provided of PSE shunt temperatures to qualify torque levels and procedures JPL Tech Specialist recommended waiver approval cont. pending revision to torque sequence and certs. of use on Flt H/W
** SUBSYSTEM: PROP	B019101	Potential rupture of fuel leak of non-redundant tank prevents delivery of fuel to main engine	Loss of Mission due to inability to perform MOI, Possible catastrophic loss of S/C due to tank rupture	JPL Tech. Specialists recommended Waiver be conditionally-accepted pending review of Frac. Mech Analysis. NO evidence that analysis received or reviewed by JPL
	B019102	SAFETY "FACTORS" PRESENTED BY GE ARE SAFETY "MARGINS" NOT MEETING AF 127-1	PRESSURIZATION OVERSTRESS COULD RUPTURE TANK AND CAUSE LOSS OF MISSION	JPL TECH SPECIALISTS RECOMMENDED ONLY CONDITIONAL APPROVAL PENDING DETAIL REVIEW OF FRACTURE MECHANICS ANALYSIS AND QUAL TEST RESULTS NO EVIDENCE IN PACKAGE THAT DOCUMENTS RECEIVED OR REVIEWED BY JPL
	B019103	DUE TO POTENTIAL REGULATOR a) NO PRESSURE COND. b) RUPTURE 1.5 MEOP TEST	LOSS OF MISSION	JPL TECH SPECIALISTS RECOMMENDED CONDITIONAL APPROVAL ONLY. PENDING REVIEW OF FRACTURE MECHANICS ANALYSIS AND QUAL TEST RESULTS NO EVIDENCE THAT DOCUMENTATION RECEIVED OR REVIEWED BY JPL

Table M-2. Mars Observer approved SFP waiver summary (listing by subsystem) (continued).

S/S	WAIVER #	SUMMARY DESCRIPTION:	MISSION IMPACT:	RISK ASSESSMENT:
	8019106	DUE TO POTENTIAL HP FILTER a) RUPTURE. b) CLOGGED ANALYSIS/TEST REQD	LOSS OF MISSION	JPL TECH SPECIALISTS RECOMMENDED CONDITIONAL ACCEPTANCE PENDING REVIEW OF SAFETY MARGINS AND ANALYSIS TO VALIDATE A 520% MARGIN TO PREVENT CLOGGING OF FILTER ANALYSIS NOT PROVIDED IN WAIVER PACKAGE
	8019107	DUE TO POTENTIAL LP FILTER a) RUPTURE. b) CLOGGED INABILITY TO PRESURIZE SYSTEM RESULTS IN NO DELIVERY OF FUEL & OXIDIZER TO ENGINE	LOSS OF MISSION	JPL TECH SPECIALISTS RECOMMENDED CONDITIONAL ACCEPTANCE PENDING REVIEW OF SAFETY FACTORS AND ANALYSIS TO VALIDATE 300% MARGIN TO PREVENT CLOGGING OF FILTER ANALYSIS NOT PROVIDED IN WAIVER PACKAGE
	8019746	LOSS OF HE PRESSURANT DUE TO TANK LEAK PREVENTS PRESURIZATION OF FUEL AND OXIDIZER TANKS WITH NO DELIVERY TO ENGINE	LOSS OF MISSION	TANK QUALIFIED TO MIL-STD-1522A LEAK-BEFORE-BURST DESIGN VERIFIED BY TEST JPL TECH SPEC. RECOMMEND REJ. WAIVER UNTIL STRUCTURE AND FRACTURE MECHANICS ANALYSES REVIEWED BY JPL
	8019746	BIPROP TANK RUPTURES OR LEAKS, OR PROP. MANAGEMENT DEVICE FAILS PREVENTING FLOW OF FUEL OR OXIDIZER TO ENGINE	LOSS OF MISSION	ANALYSES NOT PROVIDED TANK QUALIFIED TO MIL-STD-1522A JPL TECH SPECIALISTS RECOMMENDED REJ WAIVER PENDING REVIEW OF VENDOR DATA, PROOF TEST RESULTS, X-RAY INSP PLUS STRUCTURAL & FRAC. MECH ANALYSES DATA NOT IN PACKAGE
** SUBSYSTEM: TCS	8017378	Single HGA. With no redundancy, with potential feed misalignments or cracks in Polarizer ferrites due to Launch environment(Vibration), see also Waiver 8019147 for materials selection info	Loss of ability to transmit engineering data in Outer Cruise Phase or Science data during Mapping Phase potential loss of mission science return	Proj. Appvd. Documentation includes info on ACTS antenna thermal shock and radiation testing, materials description and plan for Vib and T/V testing see also Waivers 8019147 & W002650
	8019138	HYBRID COUPLER CONNECTS BOTH TRANSPONDERS TO INPUT OF TWTAS NONE-TRANSPNDR RF SIG IS LOW. TESTS AT HIGHER LEVEL. VIB TESTS ALSO DONE.	RF or Mechanical failure would prevent either MOT from exciting the TWTAs thus preventing radiometric tracking, ranging, and return of engineering or science data therefore potential loss of mission	MOT RF signals are low power level but tested at relatively high level. Vendor plans vibration test/GE ENV RQM 3271152 No-failure flight history JPL requested VSMR/insertion loss check during VIB
	8019140	Heritage design has non-redundant damper and bearing can seize or bind due to mechanical failure	Loss of ability to position HGA and therefore seriously degraded or no communications capability leading to loss of mission	Cond-APP is based on assumption that the wrist hinge/rotary joint assy will be mechanically (deployment) and RF functional tested at assy level under Cold Protoflight conditions in thermal-vac test
	8019141	+Y TXMT LGA (EARTH FACING) IS NON-REDUNDANT	Loss of +Y Transmit LGA would prohibit communications for acquisition and emergency modes therefore potential loss of mission	Only failure mode identified by GE is structural detachment from S/C System level Dynamics test will have LGA attached to S/C No JPL risk assessment in Waiver Project accepted w/o conditions

Table M-2. Mars Observer approved SFP waiver summary (listing by subsystem) (continued).

S/S	WAIVER #	SUMMARY DESCRIPTION:	MISSION IMPACT:	RISK ASSESSMENT:
	BO19142	Diplexer is in HGA transmission/reception path. Potential degradation of isolation between HGA and LOA paths	Degraded performance of HGA transmission/reception paths and isolation from LOA path could disrupt communications to earth and result in loss of science and/or engineering data	Diplexer is waveguide assembly with internal ports. JPL Cog E recommended Conditional approval due to concern that GE needs to address use of tuning screws which can leave metallic particles Proj. Appvd
	BO19143	FAIL OF NON-REDUNDANT +Y RECEIVE LOA (EARTH FACING) PRECLUDES RECEP OF DSN SIGNAL AND COMMAND DATA FROM EARTH AND TWO-WAY ACQUISITION. RECEPTION OF DSN TRANSMISSION DURING EMERGENCY OR SAFE MODE	LOSS OF MISSION SINCE WOULD BE UNABLE TO COMMAND THE S/C TO REORIENT TO POINT -Y LOA TO EARTH	JPL COG E. CONCLUDED +Y LOA WAS ROBUST DESIGN. OF OPEN ENDED WAVEGUIDE CONSTRUCTION & EXPECTED TO WITHSTAND LAUNCH VIB LOADS SYSTEM VIB TEST WILL HAVE LOA INSTALLED DYNAMIC ANALYSIS NOT IN PACKAGE Proj. Appvd
	BO19147	Single HGA, with no redundancy, with potential feed misalignments or cracks in Polarizer ferrites due to launch environment(vibration), see also Waivers BO17378 and WDO2650	Loss of ability to transmit Engineering data in Outer Cruise Phase or Science data during Mapping Phase potential loss of mission science return	No documentation included in waiver package see related HGA waivers WDO2650 & BO17378 Proj Appvd
	BO19742	Failure of non-redundant parts of Wrist Hinge Assy due to bearing seizure or damper fluid loss would prevent deployment of HGA to its proper orientation in the Mapping configuration.	Loss of ability to position HGA for transmission of Science and engineering data from Mars orbit, and interference with attitude control capability of S/C, therefore potential loss of mission	JPL Tech Specialists recommended rej of waiver pending resolution of issues on selection, reliability, lifetime of components 70 non-redundant bearings in MO design GE response not found Proj Appvd
	BO19743	Failure of non-redundant parts of Inboard Hinge Assy due to bearing seizure or damper fluid loss would prevent deployment of the HGA into its proper Cruise or Mapping configurations.	Loss of ability to position HGA for transmission of Science and engineering data during Cruise or Mapping, and interference with attitude control capability of S/C, therefore possible loss of mission	JPL Tech Specialists recommended rej of waiver pending resolution of issues on selection, reliability, lifetime of components 70 non-redundant bearings in MO design GE response not found Proj Appvd
	BO19744	Failure of the non redundant parts of Mid-Boom Hinge Assy due to seizure of bearings or loss of damper fluid prevents the deployment of the HGA to its proper orientation in the Cruise	Loss of ability to position HGA for transmission of Science and Engring data during Cruise or Mapping, and/or interference with attitude control capability of S/C, therefore possible loss of mission	JPL Tech Specialists recommended rej of waiver pending resolution of issues on selection, reliability, lifetime of components 70 non-redundant bearings in MO design GE response not found Proj Appvd
	WDO2650	Single HGA, with no redundancy, with potential feed misalignments or cracks in Polarizer ferrites due to Launch environment(Vibration), see also Waivers WD17378 & BO19147	Loss of ability to transmit Engineering data in Outer Cruise Phase or Science data during Mapping Phase potential loss of mission science return	Initially rej. by JPL Tech spec due to inadequate thermal shock analysis, and lack of acoustic test or analysis addressing sine, random & acoustic env. Test revealed 3 new failure modes see IOMs

APPENDIX N
RECOVERY COMMANDS

Commands Radiated Since Loss of Downlink

Bit-One Radiation Time	GCMD	Duration	Msgs	CMD RQST #	SCMF	Title / Commands
93-234/05:09:59.5	qrpan201	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) *** STRPAN
93-234/05:23:08.1	qrpan202	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) *** STRPAN
93-234/05:35:02.3	qrpan203	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) *** STRPAN
93-234/05:44:36.8	qrpan204	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) *** STRPAN
93-234/05:53:16.5	qrpan205	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) *** STRPAN
93-234/06:04:42.3	qrpan206	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) *** STRPAN
93-234/06:32:08.5	qrpnh0	2.5	1	92-CNTG-0022	QRPNH1	RPA Beam On, STRPAN (@ 125) *** STRPAN
93-234/06:44:01.0	qrpnh101	2.5	1	92-CNTG-0022	QRPNH1	RPA Beam On, STRPAN (@ 125) *** STRPAN
93-234/06:55:23.3	qrpnh102	2.5	1	92-CNTG-0022	QRPNH1	RPA Beam On, STRPAN (@ 125) *** STRPAN
93-234/07:07:24.6	qrpnh103	2.5	1	92-CNTG-0022	QRPNH1	RPA Beam On, STRPAN (@ 125) *** STRPAN
93-234/07:16:52.2	qrpnh104	2.5	1	92-CNTG-0022	QRPNH1	RPA Beam On, STRPAN (@ 125) *** STRPAN
93-234/07:27:24.9	qrpnh106	40:02.5	5	92-CNTG-0022(A)	QRPNH1	RPA Beam On, STRPAN (x5) (@ 125) *** STRPAN (x5)
93-234/08:19:22.5	q001c0	17.5	2	92-CNTG-0147	Q001C1	Arm & Go to Contingency Mode (@ 125) *** SCCMDA, SCGCNT
93-234/08:39:50.1	q001e1	100.0	2	92-CNTG-0148	Q001E1	Arm & Go to Contingency Mode (@ 7.8) *** SCCMDA, SCGCNT
93-234/09:49:05.4	q6251702	40.0	1	93-TELEC-0821	Q62517	CDU 1 to 62.5 bps (@7.8 bps) *** TCC1BS("BPS062")
93-234/11:54:08.9	rpacon01	2:24:40.0	12	92-CNTG-0001(A)	QRPAN2 & Q001E1	RPA Beam On + Arm & Go Contingency Mode (4x) (@7.8) *** (STRPAN, SCCMDA, SCGCNT) (x4)
93-234/20:37:52.9	it0109aa	1:32:37.0	20	93-TELEC-1164	IT0109	Set CDU 1 & 2 to 7.8 bps (@ 62.5) *** (TCC1BS("BPS7.8"), TCC2BS("BPS7.8")) (x10)
93-234/22:25:21.4	it0113aa	1:40:40.0	20	93-TELEC-1165	IT0113	Set CDU 1 & 2 to 7.8 bps (@ 7.8) *** (TCC1BS("BPS7.8"), TCC2BS("BPS7.8")) (x10)
93-235/00:09:55.2	qrpfl201	40.0	1	93-TELEC-1200	QRPFL2	Turn RPA Beam Off (@ 7.8) *** STRPAF
93-235/00:30:04.7	qrpfl202	40.0	1	93-TELEC-1200	QRPFL2	Turn RPA Beam Off (@ 7.8) *** STRPAF
93-235/01:35:29.0	it011001	10:40.0	8	93-TELEC-1167	IT0110	Hardware CMDs to Turn On RPA 1 *** TCM1EF, TCM2EF, TCR1BF, TCR2BF, TCR1FN, TCR2FN, TCR1BN, TCM1EN
93-235/01:50:35.7	it011002	10:40.0	8	93-TELEC-1167	IT0110	Hardware CMDs to Turn On RPA 1 *** TCM1EF, TCM2EF, TCR1BF, TCR2BF, TCR1FN, TCR2FN, TCR1BN, TCM1EN
93-235/03:34:59.0	it011003	10:40.0	8	93-TELEC-1167	IT0110	Hardware CMDs to Turn On RPA 1 *** TCM1EF, TCM2EF, TCR1BF, TCR2BF, TCR1FN, TCR2FN, TCR1BN, TCM1EN
93-235/04:38:47.0	it011101	10:40.0	8	93-TELEC-1168	IT0111	Hardware CMDs to Turn On RPA 2 *** TCM1EF, TCM2EF, TCR1BF, TCR2BF, TCR1FN, TCR2FN, TCR2BN, TCM2EN
93-235/04:54:51.0	it011102	10:40.0	8	93-TELEC-1168	IT0111	Hardware CMDs to Turn On RPA 2 *** TCM1EF, TCM2EF, TCR1BF, TCR2BF, TCR1FN, TCR2FN, TCR2BN, TCM2EN
93-235/05:54:37.2	it011501	6:40.0	7	93-TELEC-1169	IT0115	RF Switch to Pos B; RPA 2 On *** TCM1EF, TCM2EF, TCR1BF, TCR2BF, TCRF2B, TCR2BN, TCM2EN
93-235/06:08:32.4	it011502	6:40.0	7	93-TELEC-1169	IT0115	RF Switch to Pos B; RPA 2 On *** TCM1EF, TCM2EF, TCR1BF, TCR2BF, TCRF2B, TCR2BN, TCM2EN
93-235/07:05:14.5	it011401	6:40.0	7	93-TELEC-1166	IT0114	RF Switch to Pos A; RPA 1 On *** TCM1EF, TCM2EF, TCR1BF, TCR2BF, TCRF2A, TCR1BN, TCM1EN
93-235/07:20:18.2	it011402	6:40.0	7	93-TELEC-1166	IT0114	RF Switch to Pos A; RPA 1 On *** TCM1EF, TCM2EF, TCR1BF, TCR2BF, TCRF2A, TCR1BN, TCM1EN
93-235/13:45:47.3	it011701	9:40.0	10	93-TELEC-1172	IT0117	S/W RPA Beam Off / H/W Filament 1 On *** STRPAF (x5), TCR1FN (x5)
93-235/13:55:51.0	it011901	9:40.0	10	93-TELEC-1174	IT0119	Beam 1 Off / Beam 2 Off *** TCR1BF (x5), TCR2BF (x5)
93-235/14:05:52.3	it012101	9:40.0	10	93-TELEC-1176	IT0121	Exciter 1/2 Off *** TCM1EF (x5), TCM2EF (x5)
93-235/14:15:53.0	it012301	9:40.0	10	93-TELEC-1178	IT0123	Beam 1 On / Exciter 1 On *** TCR1BN (x5), TCM1EN (x5)
93-235/15:42:49.9	it011702	9:40.0	10	93-TELEC-1172	IT0117	S/W RPA Beam Off / H/W Filament 1 On *** STRPAF (x5), TCR1FN (x5)
93-235/15:52:52.8	it012103	9:40.0	10	93-TELEC-1176	IT0121	Exciter 1/2 Off *** TCM1EF (x5), TCM2EF (x5)
93-235/16:02:52.7	it011903	9:40.0	10	93-TELEC-1174	IT0119	Beam 1 Off / Beam 2 Off *** TCR1BF (x5), TCR2BF (x5)
93-235/16:13:02.9	it012302	9:40.0	10	93-TELEC-1178	IT0123	Beam 1 On / Exciter 1 On *** TCR1BN (x5), TCM1EN (x5)
93-235/17:59:27.4	it012501	4:40.0	5	93-TELEC-1180	IT0125	Turn On Filament 2 *** TCR2FN (x5)
93-235/18:04:30.5	it012102	9:40.0	10	93-TELEC-1184	IT0121	Exciter 1/2 Off *** TCM1EF (x5), TCM2EF (x5)
93-235/18:14:31.5	it011902	9:40.0	10	93-TELEC-1182	IT0119	Beam 1 Off / Beam 2 Off *** TCR1BF (x5), TCR2BF (x5)
93-235/18:24:32.1	it0115e5	4:40.0	5	93-TELEC-1188	IT0115	RF Switch to Position B *** TCRF2B (x5)
93-235/18:29:34.5	it012801	9:40.0	10	93-TELEC-1186	IT0128	Beam 2 On / Exciter 2 On *** TCR2BN (x5), TCM2EN (x5)
93-235/21:09:45.2	it012104	9:40.0	10	93-TELEC-1184	IT0121	Exciter 1/2 Off *** TCM1EF (x5), TCM2EF (x5)
93-235/21:23:35.2	it011904	9:40.0	10	93-TELEC-1182	IT0119	Beam 1 Off / Beam 2 Off *** TCR1BF (x5), TCR2BF (x5)
93-235/21:37:13.6	it012802	9:40.0	10	93-TELEC-1186	IT0128	Beam 2 On / Exciter 2 On *** TCR2BN (x5), TCM2EN (x5)
93-235/22:39:13.8	it013201	29:40.0	30	93-C&DH-1189	IT0132	Select Backup RXO (PRI) (Primary uplink processor) *** HRXOBU (x30)

Commands Radiated Since Loss of Downlink

Bit-One Radiation Time	GCMD	Duration	Msgs	CMD RQST #	SCMF	Title / Commands
93-235/23:55:49.6	it011005	10:40.0	8	93-TELEC-1167	IT0110	Hardware CMDs to Turn On RPA 1 *** TCM1EF, TCM2EF, TCR1BF, TCR2BF, TCR1FN, TCR2FN, TCR1BN, TCM1EN
93-236/00:48:22.0	it011104	10:40.0	8	93-TELEC-1168	IT0111	Hardware CMDs to Turn On RPA 2 *** TCM1EF, TCM2EF, TCR1BF, TCR2BF, TCR1FN, TCR2FN, TCR2BN, TCM2EN
93-236/01:56:38.9	it013202	29:40.0	30	93-C&DH-1189	IT0132	Select Backup RXO (PRI) (Primary uplink processor) *** HRXOBU (x30)
93-236/03:40:24.4	it011703	9:40.0	10	93-TELEC-1172	IT0117	S/W RPA Beam Off / H/W Filament 1 On *** STRPAF (x5), TCR1FN (x5)
93-236/03:51:42.4	it011201	4:40.0	5	93-C&DH-1170	IT0112	Reset EDF (x5) *** SCEDFC (x5)
93-236/04:00:03.2	uemrg801	3:40.0	4	93-C&DH-1191	UEMRG8	EDF to Emergency Mode *** SCEDFC("EMR"), CDXPG1("42.3"), CDXPG2("42.3"), STMOTC("EDF1")
93-236/04:05:40.5	qrpan207	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) *** STRPAN
93-236/04:32:45.1	it013203	29:40.0	30	93-C&DH-1189	IT0132	Select Backup RXO (PRI) (Primary uplink processor) *** HRXOBU (x30)
93-236/06:45:42.8	qscp2602	40.0	1	93-C&DH-1213	QSCP26	Select SCP 2 *** HSSCP2
93-236/06:51:47.2	qrpan208	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) *** STRPAN
93-236/07:19:26.0	qscp2603	40.0	1	93-C&DH-1213	QSCP26	Select SCP 2 *** HSSCP2
93-236/07:22:19.2	qrpan209	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) *** STRPAN
93-236/07:26:58.6	qscp2604	40.0	1	93-C&DH-1213	QSCP26	Select SCP 2 *** HSSCP2
93-236/07:30:22.8	qrpan210	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) *** STRPAN
93-236/07:48:35.8	qscp2605	40.0	1	93-C&DH-1213	QSCP26	Select SCP 2 *** HSSCP2
93-236/07:51:05.0	qrpan211	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) *** STRPAN
93-236/08:20:59.8	qscp2606	40.0	1	93-C&DH-1213	QSCP26	Select SCP 2 *** HSSCP2
93-236/08:23:19.3	qrpan212	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) *** STRPAN
93-236/10:30:28.6	q001e1aa	40.0	1	92-CNTG-0148(A)	Q001E1	Arm Contingency Mode (@7.8) *** SCCMDA
93-236/10:33:49.2	uans06aa	2:40.0	3	93-AACS-1215	UANS06	Go ANS *** SAYMUX, SAPMUX, SAGANS
93-236/10:44:30.7	q001e1ab	40.0	1	92-CNTG-0148(A)	Q001E1	Arm Contingency Mode (@7.8) *** SCCMDA
93-236/12:24:13.5	q001e1ac	40.0	1	92-CNTG-0148(A)	Q001E1	Arm Contingency Mode (@7.8) *** SCCMDA
93-236/12:26:44.1	uans06ab	2:40.0	3	93-AACS-1215	UANS06	Go ANS *** SAYMUX, SAPMUX, SAGANS
93-236/13:15:05.2	q008n101	40.0	1	93-AACS-0803(A)	Q008N1	Go Sun Star Init (@7.8) *** SAGSSI
93-236/13:30:44.8	q008n102	40.0	1	93-AACS-0803(A)	Q008N1	Go Sun Star Init (@7.8) *** SAGSSI
93-236/13:45:04.1	q008n103	40.0	1	93-AACS-0803(A)	Q008N1	Go Sun Star Init (@7.8) *** SAGSSI
93-236/14:00:02.2	q008n104	40.0	1	93-AACS-0803(A)	Q008N1	Go Sun Star Init (@7.8) *** SAGSSI
93-236/14:15:01.4	q008n105	40.0	1	93-AACS-0803(A)	Q008N1	Go Sun Star Init (@7.8) *** SAGSSI
93-236/14:30:48.4	q008n106	40.0	1	93-CNTG-0024(A)	Q008N1	Go Sun Star Init *** SAGSSI
93-236/14:39:17.4	gt010501	8:22.4	4	93-C&DH-1199	GT0105	Backup Pressurization Sequence (Fire All Pyros) *** (Load & Go Minisequence): (STRPAF, TCR1FF, TCR2FF, PYECAE, PYECBE, PYECAA, PYECBA, PRP7PR, PRP5PR, PRP8BR, PRP6BR, PYECAD, PYECBD, PYECAX, PYECBX, STRPAN)
93-236/15:00:10.3	q008n107	40.0	1	93-CNTG-0024(A)	Q008N1	Go Sun Star Init *** SAGSSI
93-236/15:11:19.6	gt010502	8:22.4	4	93-C&DH-1199	GT0105	Backup Pressurization Sequence (Fire All Pyros) *** (Load & Go Minisequence): (STRPAF, TCR1FF, TCR2FF, PYECAE, PYECBE, PYECAA, PYECBA, PRP7PR, PRP5PR, PRP8BR, PRP6BR, PYECAD, PYECBD, PYECAX, PYECBX, STRPAN)
93-236/15:30:04.9	q008n108	40.0	1	93-CNTG-0024(A)	Q008N1	Go Sun Star Init *** SAGSSI
93-236/15:45:51.9	q008n109	40.0	1	93-CNTG-0024(A)	Q008N1	Go Sun Star Init *** SAGSSI
93-236/16:00:23.4	q008n110	40.0	1	93-CNTG-0024(A)	Q008N1	Go Sun Star Init *** SAGSSI
93-237/00:34:04.8	it016301	7:40.0	8	93-C&DH-1216	IT0163	Set Backup RXO, Clk Div, I/O Bus, SCP *** HRXOBU, HRXOBU, HSCLK2, HSCLK2, HSI0BB, HSI0BB, HSSCP2, HSSCP2
93-237/00:55:07.8	IT016501	47.2	1	93-C&DH-1217	IT0165	Set EDF Time to 1993/237-01:15:00 *** SCEDFC("SETTIME", 0X19AC, 0X171E,.)
93-237/01:04:04.8	it013601	40.0	1	93-C&DH-1205	IT0136	Set SCP Time to EDF Time *** SESTET
93-237/01:11:09.6	q008n111	40.0	1	93-CNTG-0024(A)	Q008N1	Go Sun Star Init *** SAGSSI
93-237/01:11:09.6	q008n111	40.0	1	92-CNTG-0024(A)	Q008N1	Go Sun Star Init *** SAGSSI
93-237/01:17:23.3	it011704	9:40.0	10	93-TELEC-1172	IT0117	S/W RPA Beam Off / H/W Filament 1 On *** STRPAF (x5), TCR1FN (x5)
93-237/01:29:13.9	it012502	4:40.0	5	93-TELEC-1180	IT0125	Turn On Filament 2 *** TCR2FN (x5)
93-237/01:34:46.5	it012105	9:40.0	10	93-TELEC-1176	IT0121	Exciter 1/2 Off *** TCM1EF (x5), TCM2EF (x5)
93-237/01:45:54.9	it011905	9:40.0	10	93-TELEC-1174	IT0119	Beam 1 Off / Beam 2 Off *** TCR1BF (x5), TCR2BF (x5)
93-237/01:57:42.9	it013101	14:40.0	15	93-TELEC-1195	IT0131	RF Switch A, RPA 1 On, MOT 2 On *** TCRF2A (x5), TCR1BN (x5), TCM2EN (x5)

Commands Radiated Since Loss of Downlink

Bit-One Radiation Time	GCMD	Duration	Msgs	CMD RQST #	SCMF	Title / Commands
93-237/07:10:00.5	it011706	9:40.0	10	93-TELEC-1172	IT0117	S/W RPA Beam Off / H/W Filament 1 On *** STRPAF (x5), TCR1FN (x5)
93-237/07:20:36.3	it012503	4:40.0	5	93-TELEC-1180	IT0125	Turn On Filament 2 *** TCR2FN (x5)
93-237/07:26:27.2	it012106	9:40.0	10	93-TELEC-1176	IT0121	Exciter 1/2 Off *** TCM1EF (x5), TCM2EF (x5)
93-237/07:36:56.1	it011906	9:40.0	10	93-TELEC-1174	IT0119	Beam 1 Off / Beam 2 Off *** TCR1BF (x5), TCR2BF (x5)
93-237/07:47:24.8	it013001	14:40.0	15	93-TELEC-1196	IT0130	RF Switch B, RPA 2 On, MOT 1 On *** TCRF2B (x5), TCR2BN (x5), TCM1EN (x5)
93-237/09:06:00.5	q001e1ad	40.0	1	92-CNTG-0148(A)	Q001E1	Arm Contingency Mode (@ 7.8) *** SCCMDA
93-237/09:08:01.5	uans06ad	2:40.0	3	93-AACS-1215	UANS06	Go ANS *** SAYMUX, SAPMUX, SAGANS
93-237/13:39:15.2	q008n112	40.0	1	92-CNTG-0024(A)	Q008N1	Go Sun Star Init *** SAGSSI
93-237/13:42:11.7	it011707	9:40.0	10	93-TELEC-1172	IT0117	S/W RPA Beam Off / H/W Filament 1 On *** STRPAF (x5), TCR1FN (x5)
93-237/13:52:40.7	it012504	4:40.0	5	93-TELEC-1180	IT0125	Turn On Filament 2 *** TCR2FN (x5)
93-237/13:58:09.2	it012107	9:40.0	10	93-TELEC-1176	IT0121	Exciter 1/2 Off *** TCM1EF (x5), TCM2EF (x5)
93-237/14:09:22.6	it011907	9:40.0	10	93-TELEC-1174	IT0119	Beam 1 Off / Beam 2 Off *** TCR1BF (x5), TCR2BF (x5)
93-237/14:20:58.3	it013102	14:40.0	15	93-TELEC-1195	IT0131	RF Switch A, RPA 1 On, MOT 2 On *** TCRF2A (x5), TCR1BN (x5), TCM2EN (x5)
93-237/15:28:38.9	q001e1ae	40.0	1	92-CNTG-0148(A)	Q001E1	Arm Contingency Mode (@ 7.8) *** SCCMDA
93-237/16:44:24.4	uans06ae	2:40.0	3	93-AACS-1215	UANS06	Go ANS *** SAYMUX, SAPMUX, SAGANS
93-237/17:44:13.1	it011708	9:40.0	10	93-TELEC-1172	IT0117	S/W RPA Beam Off / H/W Filament 1 On *** STRPAF (x5), TCR1FN (x5)
93-237/19:21:49.3	it012506	4:40.0	5	93-TELEC-1180	IT0125	Turn On Filament 2 *** TCR2FN (x5)
93-237/19:28:58.6	it012108	9:40.0	10	93-TELEC-1176	IT0121	Exciter 1/2 Off *** TCM1EF (x5), TCM2EF (x5)
93-237/19:39:52.7	it011908	9:40.0	10	93-TELEC-1174	IT0119	Beam 1 Off / Beam 2 Off *** TCR1BF (x5), TCR2BF (x5)
93-237/19:51:39.8	it013002	14:40.0	15	93-TELEC-1196	IT0130	RF Switch B, RPA 2 On, MOT 1 On *** TCRF2B (x5), TCR2BN (x5), TCM1EN (x5)
93-237/20:28:56.9	it012109	9:40.0	10	93-TELEC-1176	IT0121	Exciter 1/2 Off *** TCM1EF (x5), TCM2EF (x5)
93-237/20:39:13.5	it011909	9:40.0	10	93-TELEC-1174	IT0119	Beam 1 Off / Beam 2 Off *** TCR1BF (x5), TCR2BF (x5)
93-237/20:49:14.8	it012303	9:40.0	10	93-TELEC-1178	IT0123	Beam 1 On / Exciter 1 On *** TCR1BN (x5), TCM1EN (x5)
93-237/22:04:00.4	qrpan213	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) *** STRPAN
93-237/22:14:00.0	qrpan214	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) *** STRPAN
93-237/22:24:20.7	qrpan215	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) *** STRPAN
93-237/22:34:01.1	qrpan216	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) *** STRPAN
93-237/22:43:59.8	qrpan217	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) *** STRPAN
93-237/22:52:15.0	q001e101	100.0	2	92-CNTG-0148	Q001E1	Arm & Go to Contingency Mode (@ 7.8) *** SCCMDA, SCGCNT
93-237/22:57:54.7	q001e102	100.0	2	92-CNTG-0148	Q001E1	Arm & Go to Contingency Mode (@ 7.8) *** SCCMDA, SCGCNT
93-238/02:03:52.7	ic060701	1:40.0	2	93-C&DH-1227	IC0607	Set SCU Outer Cruise Latch Relays *** HOUTCR, HOUTCR
93-238/02:19:02.3	ic060702	1:40.0	2	93-C&DH-1227	IC0607	Set SCU Outer Cruise Latch Relays *** HOUTCR, HOUTCR
93-238/02:34:00.7	ic060703	1:40.0	2	93-C&DH-1227	IC0607	Set SCU Outer Cruise Latch Relays *** HOUTCR, HOUTCR
93-238/04:13:09.9	it012110	9:40.0	10	93-TELEC-1176	IT0121	Exciter 1/2 Off *** TCM1EF (x5), TCM2EF (x5)
93-238/04:24:00.7	it011910	9:40.0	10	93-TELEC-1174	IT0119	Beam 1 Off / Beam 2 Off *** TCR1BF (x5), TCR2BF (x5)
93-238/04:35:00.2	it131p21	9:40.0	10	93-TELEC-1195(A)	IT0131	RPA 1 On, MOT 2 On *** TCR1BN (x5), TCM2EN (x5)
93-238/06:50:13.5	q001e1af	40.0	1	92-CNTG-0148(A)	Q001E1	Arm Contingency Mode (@ 7.8) *** SCCMDA
93-238/06:53:15.6	uans06af	2:40.0	3	93-AACS-1215	UANS06	Go ANS *** SAYMUX, SAPMUX, SAGANS
93-238/07:37:58.8	it012111	9:40.0	10	93-TELEC-1176	IT0121	Exciter 1/2 Off *** TCM1EF (x5), TCM2EF (x5)
93-238/07:49:01.6	it011911	9:40.0	10	93-TELEC-1174	IT0119	Beam 1 Off / Beam 2 Off *** TCR1BF (x5), TCR2BF (x5)
93-238/08:00:01.5	it012803	9:40.0	10	93-TELEC-1186	IT0128	Beam 2 On / Exciter 2 On *** TCR2BN (x5), TCM2EN (x5)
93-238/22:00:00.2	qrpan218	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) *** STRPAN
93-238/22:09:59.9	qrpan219	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) *** STRPAN
93-238/22:20:00.1	qrpan220	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) *** STRPAN
93-238/22:29:59.0	qrpan221	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) *** STRPAN
93-238/22:40:00.7	qrpan222	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) *** STRPAN
93-238/22:49:59.9	qrpan223	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) *** STRPAN
93-238/23:00:00.3	qrpan224	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) *** STRPAN
93-238/23:10:00.6	qrpan225	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) *** STRPAN
93-238/23:20:01.1	qrpan226	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) *** STRPAN
93-238/23:30:00.9	qrpan227	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) *** STRPAN
93-239/01:34:59.3	qrpan228	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) (Capture Predict) *** STRPAN
93-239/01:45:00.2	qrpan229	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) (Capture Predict) *** STRPAN
93-239/01:55:00.4	qrpan230	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) (Capture Predict) *** STRPAN
93-239/02:05:00.3	qrpan231	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) (Capture Predict) *** STRPAN
93-239/02:15:00.2	qrpan232	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) (Capture Predict) *** STRPAN

Commands Radiated Since Loss of Downlink

Bit-One Radiation Time	GCMD	Duration	Msgs	CMD RQST #	SCMF	Title / Commands
93-239/02:25:00.0	qrpan233	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) (Capture Predict) *** STRPAN
93-239/02:36:48.2	qrpan234	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) (Capture Predict) *** STRPAN
93-239/02:46:14.6	qrpan235	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) (Capture Predict) *** STRPAN
93-239/02:54:59.6	qrpan236	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) (Capture Predict) *** STRPAN
93-239/03:10:15.8	qrpan237	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) (Capture Predict) *** STRPAN
93-239/05:29:59.7	it016801	8:40.0	9	93-C&DH-1228	IT0168	Power Off, On & Select SCP 1 (Bad Predict) *** HSCPPF (x3), HSCPPN (x3), HSSCP1 (x3)
93-239/05:58:05.9	it016802	8:40.0	9	93-C&DH-1228	IT0168	Power Off, On & Select SCP 1 (Bad Predict) *** HSCPPF (x3), HSCPPN (x3), HSSCP1 (x3)
93-239/07:07:01.6	it016803	8:40.0	9	93-C&DH-1228	IT0168	Power Off, On & Select SCP 1 (Flyby Predict) *** HSCPPF (x3), HSCPPN (x3), HSSCP1 (x3)
93-239/07:35:11.2	it016804	8:40.0	9	93-C&DH-1228	IT0168	Power Off, On & Select SCP 1 (Flyby Predict) *** HSCPPF (x3), HSCPPN (x3), HSSCP1 (x3)
93-239/08:03:29.5	it016805	8:40.0	9	93-C&DH-1228	IT0168	Power Off, On & Select SCP 1 (Flyby Predict) *** HSCPPF (x3), HSCPPN (x3), HSSCP1 (x3)
93-239/08:34:01.8	qonse101	1:40.0	2	93-C&DH-1229	QONSE1	SCP 1 PWR On, Select SCP 1 (Flyby Predict) *** HSCPPN, HSSCP1
93-239/08:40:01.1	qonse102	1:40.0	2	93-C&DH-1229	QONSE1	SCP 1 PWR On, Select SCP 1 (Flyby Predict) *** HSCPPN, HSSCP1
93-239/08:46:00.1	qonse103	1:40.0	2	93-C&DH-1229	QONSE1	SCP 1 PWR On, Select SCP 1 (Flyby Predict) *** HSCPPN, HSSCP1
93-239/08:52:01.2	qonse104	1:40.0	2	93-C&DH-1229	QONSE1	SCP 1 PWR On, Select SCP 1 (Flyby Predict) *** HSCPPN, HSSCP1
93-239/08:58:00.7	qonse105	1:40.0	2	93-C&DH-1229	QONSE1	SCP 1 PWR On, Select SCP 1 (Flyby Predict) *** HSCPPN, HSSCP1
93-239/09:04:00.3	qonse106	1:40.0	2	93-C&DH-1229	QONSE1	SCP 1 PWR On, Select SCP 1 (Flyby Predict) *** HSCPPN, HSSCP1
93-239/09:10:01.3	qonse107	1:40.0	2	93-C&DH-1229	QONSE1	SCP 1 PWR On, Select SCP 1 (Flyby Predict) *** HSCPPN, HSSCP1
93-239/10:26:01.5	it016806	8:40.0	9	93-C&DH-1228	IT0168	Power Off, On & Select SCP 1 (Capture Predict) *** HSCPPF (x3), HSCPPN (x3), HSSCP1 (x3)
93-239/10:55:14.6	it016807	8:40.0	9	93-C&DH-1228	IT0168	Power Off, On & Select SCP 1 (Capture Predict) *** HSCPPF (x3), HSCPPN (x3), HSSCP1 (x3)
93-239/11:26:06.6	it016808	8:40.0	9	93-C&DH-1228	IT0168	Power Off, On & Select SCP 1 (Capture Predict) *** HSCPPF (x3), HSCPPN (x3), HSSCP1 (x3)
93-239/11:53:59.6	qonse108	1:40.0	2	93-C&DH-1229	QONSE1	SCP 1 PWR On, Select SCP 1 (Capture Predict) *** HSCPPN, HSSCP1
93-239/12:00:01.0	qonse109	1:40.0	2	93-C&DH-1229	QONSE1	SCP 1 PWR On, Select SCP 1 (Capture Predict) *** HSCPPN, HSSCP1
93-239/12:06:00.1	qonse110	1:40.0	2	93-C&DH-1229	QONSE1	SCP 1 PWR On, Select SCP 1 (Capture Predict) *** HSCPPN, HSSCP1
93-239/12:12:00.4	qonse111	1:40.0	2	93-C&DH-1229	QONSE1	SCP 1 PWR On, Select SCP 1 (Capture Predict) *** HSCPPN, HSSCP1
93-239/12:18:01.2	qonse112	1:40.0	2	93-C&DH-1229	QONSE1	SCP 1 PWR On, Select SCP 1 (Capture Predict) *** HSCPPN, HSSCP1
93-239/12:24:01.0	qonse113	1:40.0	2	93-C&DH-1229	QONSE1	SCP 1 PWR On, Select SCP 1 (Capture Predict) *** HSCPPN, HSSCP1
93-239/12:30:01.9	qonse114	1:40.0	2	93-C&DH-1229	QONSE1	SCP 1 PWR On, Select SCP 1 (Capture Predict) *** HSCPPN, HSSCP1
93-242/03:29:37.5	qonse115	1:40.0	2	93-C&DH-1232	QONSE1	SCP 1 PWR On, Select SCP 1 (Flyby Predict) *** HSCPPN, HSSCP1
93-242/03:32:03.7	it011202	40.0	1	93-C&DH-1233	IT0112	Reset EDF (Flyby Predict) *** SCEDFC
93-242/03:33:57.2	qrpan238	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (@7.8) (Flyby Predict) *** STRPAN
93-242/11:02:49.5	qonse116	1:40.0	2	93-C&DH-1232	QONSE1	SCP 1 PWR On, Select SCP 1 (Capture Predict) *** HSCPPN, HSSCP1
93-242/11:05:54.4	it011203	40.0	1	93-C&DH-1233	IT0112	Reset EDF (Capture Predict) *** SCEDFC
93-242/11:07:58.4	qrpan239	40.0	1	92-CNTG-0001	QRPAN2	RPA Beam On (Capture Predict) *** STRPAN
93-250/21:12:57.9	qrpan245	3:10:40.0	20	92-CNTG-0001(B)	QRPAN2	RPA Beam On (Flyby Predict) *** STRPAN (x20)
93-251/01:29:29.6	it017101	1:50:40.0	30	93-C&DH-1240	IT0171	SCP 1 Off, Arm & Go C-Mode (U/L 2) (Flyby Predict) *** (HSCPPF, SCCMDA, SCGCNT) (x10)
93-251/03:29:31.7	it017104	1:31:40.0	20	93-C&DH-1240	IT0171	SCP 1 Off, Arm & Go C-Mode (U/L 2) - (built from wrong file - QONSE101)(aborted) *** (HSCPPF, SCCMDA, SCGCNT) (x10)

Commands Radiated Since Loss of Downlink

Blt-One Radiation Time	GCMD	Duration	Msgs	CMD RQST #	SCMF	Title / Commands
93-251/09:38:19.8	it017107	1:50:40.0	30	93-C&DH-1240	IT0171	SCP 1 Off, Arm & Go C-Mode (U/L 2) (Flyby Predict) *** (HSCPPF, SCCMDA, SCGCNT) (x10)
93-251/11:38:20.8	it017108	1:50:40.0	30	93-C&DH-1240	IT0171	SCP 1 Off, Arm & Go C-Mode (U/L 2) (suspended after 16 elements) *** (HSCPPF, SCCMDA, SCGCNT) (x10)
93-251/12:58:49.7	it017201	1:50:05.0	30	93-C&DH-1241	IT0172	SCP 1 Off, Arm & Go C-Mode (U/L 2) (@62.5) (Flyby Predict) *** (HSCPPF, SCCMDA, SCGCNT) (x10)
93-251/15:01:03.2	it017202	1:50:05.0	30	93-C&DH-1241	IT0172	SCP 1 Off, Arm & Go C-Mode (U/L 2) (@62.5) (suspended after 18 elements) *** (HSCPPF, SCCMDA, SCGCNT) (x10)
93-251/16:37:52.4	it017301	1:50:02.5	30	93-C&DH-1242	IT0173	SCP 1 Off, Arm & Go C-Mode (U/L 2) (Flyby Predict) *** STRPAN (x10)
93-251/18:33:41.3	it017302	1:50:02.5	30	93-C&DH-1242	IT0173	SCP 1 Off, Arm & Go C-Mode (U/L 2) (@125) (suspended after 3 elements) *** (HSCPPF, SCCMDA, SCGCNT) (x10)
93-251/19:03:04.0	it017401	1:30:40.0	10	93-TELEC-1243	IT0174	RPA Beam On (U/L 2) (Flyby Predict) *** STRPAN (x10)
93-251/20:43:42.4	it017402	1:30:40.0	10	93-TELEC-1243	IT0174	RPA Beam On (U/L 2) (suspended after 6 elements) *** STRPAN (x10)
93-251/23:40:59.1	qonse121	1:40:40.0	20	93-C&DH-1244	QONSE1	SCP 1 PWR On, Select SCP 1 (Flyby Predict) (suspended after 16 elements) *** (HSCPPN, HSSCP1) (x10)
93-252/01:29:43.4	qonse122	1:40:40.0	20	93-C&DH-1244	QONSE1	SCP 1 PWR On, Select SCP 1 (Flyby Predict) (suspended after 12 elements) *** (HSCPPN, HSSCP1) (x10)
93-252/03:59:01.5	qrpan246	3:10:40.0	20	92-CNTG-0001(B)	QRPAN2	RPA Beam On (Capture Predict) *** STRPAN (x20)
93-252/09:37:09.4	it017109	1:50:40.0	30	93-C&DH-1240	IT0171	SCP 1 Off, Arm & Go C-Mode (U/L 2) (Capture Predict) *** (HSCPPF, SCCMDA, SCGCNT) (x10)
93-252/11:37:09.1	it017110	1:50:40.0	30	93-C&DH-1240	IT0171	SCP 1 Off, Arm & Go C-Mode (U/L 2) (suspended after 18 elements) *** (HSCPPF, SCCMDA, SCGCNT) (x10)
93-252/12:58:21.6	it017203	1:50:05.0	30	93-C&DH-1241	IT0172	SCP 1 Off, Arm & Go C-Mode (U/L 2) (@62.5) (Capture Predict) *** (HSCPPF, SCCMDA, SCGCNT) (x10)
93-252/14:41:52.0	it017204	1:50:05.0	30	93-C&DH-1241	IT0172	SCP 1 Off, Arm & Go C-Mode (U/L 2) (@62.5) (suspended after 18 elements) *** (HSCPPF, SCCMDA, SCGCNT) (x10)
93-252/16:24:14.7	it017303	1:50:02.5	30	93-C&DH-1242	IT0173	SCP 1 Off, Arm & Go C-Mode (U/L 2) (@125) (Capture Predict) *** (HSCPPF, SCCMDA, SCGCNT) (x10)
93-252/18:06:35.3	it017304	1:50:02.5	30	93-C&DH-1242	IT0173	SCP 1 Off, Arm & Go C-Mode (U/L 2) (@125) (suspended after 9 elements) *** (HSCPPF, SCCMDA, SCGCNT) (x10)
93-252/19:09:45.0	it017403	1:30:40.0	10	93-TELEC-1243	IT0174	RPA Beam On (U/L 2) (Capture Predict) *** STRPAN (x10)
93-252/20:43:30.6	it017404	1:30:40.0	10	93-TELEC-1243	IT0174	RPA Beam On (U/L 2) (Capture Predict) (suspended after 6 elements) *** STRPAN (x10)
93-253/01:22:19.1	qonse123	1:40:40.0	20	93-C&DH-1244	QONSE1	SCP 1 PWR On, Select SCP 1 (Capture Predict) *** (HSCPPN, HSSCP1) (x10)
93-253/03:03:21.3	qonse124	1:40:40.0	20	93-C&DH-1244	QONSE1	SCP 1 PWR On, Select SCP 1 (Capture Predict) (suspended after 12 elements) *** (HSCPPN, HSSCP1) (x10)
93-253/04:36:19.0	qrpf1203	20:40.0	3	93-TELEC-1238C	QRPFL2	Turn Off RPA Beam (Capture Predict) *** STRPAF (x3)
93-253/05:01:17.9	it017601	25:40.0	18	93-TELEC-1234C	IT0176	Disable RPA 1 & 2 Fault Protection (Capture Predict) *** (TCR1TE, TCR2TE, TCR1HX, TCR2HX, TCR1IX, TCR2IX) (x3)
93-253/05:31:20.6	qrpan243	20:40.0	3	93-TELEC-1239C	QRPAN2	Turn RPA Beam On (Capture Predict) *** STRPAN (x3)
93-253/09:39:42.4	it017703	21:40.0	6	93-TELEC-1235C	IT0177	Enable RPA 1 & 2 Helix Current Trip (Capture Predict) *** (TCR1HE, TCR2HE) (x3)
93-253/10:05:42.9	it017803	21:40.0	6	93-TELEC-1236C	IT0178	Enable RPA 1 & 2 Input Power Trip (Capture Predict) *** (TCR1IE, TCR2IE) (x3)
93-253/10:31:43.2	it017903	21:40.0	6	93-TELEC-1237C	IT0179	Enable RPA Timer (Capture Predict) *** (TCR1TX, TCR2TX) (x3)
93-253/11:52:46.4	qrpf1204	1:30:40.0	10	93-TELEC-1238F	QRPFL2	Turn Off RPA Beam (Flyby Predict) *** STRPAF (x10)
93-253/13:27:46.0	it017602	1:35:40.0	60	93-TELEC-1234F	IT0176	Disable RPA 1 & 2 Fault Protection (Flyby Predict) *** (TCR1TE, TCR2TE, TCR1HX, TCR2HX, TCR1IX, TCR2IX) (x10)
93-253/15:08:11.6	qrpan244	1:30:40.0	10	93-TELEC-1239F	QRPAN2	Turn RPA Beam On (Flyby Predict) *** STRPAN (x10)
93-253/19:25:04.4	it017704	1:31:40.0	20	93-TELEC-1235F	IT0177	Enable RPA 1 & 2 Helix Current Trip (Flyby Predict) *** (TCR1HE, TCR2HE) (x10)
93-253/21:00:04.0	it017804	1:31:40.0	20	93-TELEC-1236F	IT0178	Enable RPA 1 & 2 Input Power Trip (Flyby Predict) *** (TCR1IE, TCR2IE) (x10)
93-253/22:32:48.4	it017904	1:31:40.0	20	93-TELEC-1237F	IT0179	Enable RPA Timer (Flyby Predict) *** (TCR1TX, TCR2TX) (x10)
93-257/23:12:02.6	rxos01	11:40.0	12	93-C&DH-1252C	IT0180 & IT0168 & QONSE1	RXO Primary, Power Off, On, & Select SCP 1, SCP 1 PWR On, Select SCP 1 (Capture Predict) *** HRXOPR, HSCPPF (x3), HSCPPN (x3), HSSCP1 (x3), HSCPPN, HSSCP1

Commands Radiated Since Loss of Downlink

Bit-One Radiation Time	GCMD	Duration	Msgs	CMD RQST #	SCMF	Title / Commands
93-257/23:28:01.4	rxos02	11:40.0	12	93-C&DH-1252C	IT0180 & IT0168 & QONSE1	RXO Primary. Power Off. On, & Select SCP 1, SCP 1 PWR On. Select SCP 1 (Capture Predict) *** HRXOPR, HSCPPF (x3), HSCPPN (x3), HSSCP1 (x3), HSCPPN, HSSCP1
93-257/23:45:00.9	rxos03	11:40.0	12	93-C&DH-1252C	IT0180 & IT0168 & QONSE1	RXO Primary. Power Off. On, & Select SCP 1, SCP 1 PWR On. Select SCP 1 (Capture Predict) *** HRXOPR, HSCPPF (x3), HSCPPN (x3), HSSCP1 (x3), HSCPPN, HSSCP1
93-258/00:07:00.7	rxos04	11:40.0	12	93-C&DH-1252C	IT0180 & IT0168 & QONSE1	RXO Primary. Power Off. On, & Select SCP 1, SCP 1 PWR On. Select SCP 1 (Capture Predict) *** HRXOPR, HSCPPF (x3), HSCPPN (x3), HSSCP1 (x3), HSCPPN, HSSCP1
93-258/00:24:01.8	rxos05	11:40.0	12	93-C&DH-1252C	IT0180 & IT0168 & QONSE1	RXO Primary. Power Off. On, & Select SCP 1, SCP 1 PWR On. Select SCP 1 (Capture Predict) *** HRXOPR, HSCPPF (x3), HSCPPN (x3), HSSCP1 (x3), HSCPPN, HSSCP1
93-258/00:51:00.8	qonse125	1:40:40.0	20	93-C&DH-1255	QONSE1	SCP 1 On / Select SCP 1 (suspended after 2 elements) (Capture Predict) *** (HSCPPN, HSSCP1) (x10)
93-258/01:58:08.5	qons125a	1:40:40.0	20	93-C&DH-1255	QONSE1	SCP 1 On / Select SCP 1 (Capture Predict) *** (HSCPPN, HSSCP1) (x10)
93-258/03:43:04.4	qrpan247	20:40.0	3	93-TELEC-1247	QRPAN2	RPA Beam On (Capture Predict) *** STRPAN (x3)
93-258/16:52:29.6	rxos06	11:40.0	12	93-C&DH-1252F	IT0180 & IT0168 & QONSE1	RXO Primary. Power Off. On, & Select SCP 1, SCP 1 PWR On. Select SCP 1 (Flyby Predict) *** HRXOPR, HSCPPF (x3), HSCPPN (x3), HSSCP1 (x3), HSCPPN, HSSCP1
93-258/17:08:30.7	rxos07	11:40.0	12	93-C&DH-1252F	IT0180 & IT0168 & QONSE1	RXO Primary. Power Off. On, & Select SCP 1, SCP 1 PWR On. Select SCP 1 (Flyby Predict) *** HRXOPR, HSCPPF (x3), HSCPPN (x3), HSSCP1 (x3), HSCPPN, HSSCP1
93-258/17:24:30.9	rxos08	11:40.0	12	93-C&DH-1252F	IT0180 & IT0168 & QONSE1	RXO Primary. Power Off. On, & Select SCP 1, SCP 1 PWR On. Select SCP 1 (Flyby Predict) *** HRXOPR, HSCPPF (x3), HSCPPN (x3), HSSCP1 (x3), HSCPPN, HSSCP1
93-258/18:50:00.5	qonse126	1:40:40.0	20	93-C&DH-1255	QONSE1	SCP 1 On / Select SCP 1 (Flyby Predict) *** (HSCPPN, HSSCP1) (x10)
93-258/20:35:00.2	qrpan248	20:40.0	3	93-TELEC-1247	QRPAN2	RPA Beam On (Flyby Predict) *** STRPAN (x3)
93-260/09:42:26.8	scd21001	1:32:39.9	30	93-C&DH-1258	IT0183	Select Clock Divider 2 (@7.8) x 10 (Flyby Predict) *** (HSCLK2, SCREDF("CLOCK"), SIPIOL("CU2138",0XBFFF,0X0000)) (x10)
93-260/13:15:54.3	rxocdr01	1:31:40.0	20	93-C&DH-1259	IT0112 & QRPAN2	Reset EDF & Turn RPA Beam On (@7.8) x 10 (Flyby Predict) *** (SCEDFC, STRPAN) (x10)
93-261/09:35:30.0	scd21002	1:32:39.9	30	93-C&DH-1260	IT0183	Select Clock Divider 2 (Flyby Predict) *** (HSCLK2, SCREDF("CLOCK"), SIPIOL("CU2138",0XBFFF,0X0000)) (x10)
93-261/11:35:30.8	scd21003	1:32:39.9	30	93-C&DH-1260	IT0183	Select Clock Divider 2 (Flyby Predict) *** (HSCLK2, SCREDF("CLOCK"), SIPIOL("CU2138",0XBFFF,0X0000)) (x10)
93-261/13:35:16.8	scd21004	1:32:39.9	30	93-C&DH-1260	IT0183	Select Clock Divider 2 (Flyby Predict) *** (HSCLK2, SCREDF("CLOCK"), SIPIOL("CU2138",0XBFFF,0X0000)) (x10)
93-261/15:35:28.7	scd21005	1:32:39.9	30	93-C&DH-1260	IT0183	Select Clock Divider 2 (Flyby Predict) *** (HSCLK2, SCREDF("CLOCK"), SIPIOL("CU2138",0XBFFF,0X0000)) (x10)
93-261/18:50:02.6	scd21006	1:32:39.9	30	93-C&DH-1260	IT0183	Select Clock Divider 2 (Flyby Predict) *** (HSCLK2, SCREDF("CLOCK"), SIPIOL("CU2138",0XBFFF,0X0000)) (x10)
93-261/20:55:10.2	scd21007	1:32:39.9	30	93-C&DH-1260	IT0183	Select Clock Divider 2 (Flyby Predict) *** (HSCLK2, SCREDF("CLOCK"), SIPIOL("CU2138",0XBFFF,0X0000)) (x10)
93-262/09:40:03.5	rxocdr02	1:31:40.0	20	93-C&DH-1261	IT0112 & QRPAN2	Reset EDF & Turn RPA Beam On (Flyby Predict) *** (SCEDFC, STRPAN) (x10)
93-262/11:40:02.3	rxocdr03	1:31:40.0	20	93-C&DH-1261	IT0112 & QRPAN2	Reset EDF & Turn RPA Beam On (Flyby Predict) *** (SCEDFC, STRPAN) (x10)
93-262/13:54:49.2	rxocdr04	1:31:40.0	20	93-C&DH-1261	IT0112 & QRPAN2	Reset EDF & Turn RPA Beam On (Flyby Predict) *** (SCEDFC, STRPAN) (x10)
93-262/15:56:07.9	rxocdr05	1:31:40.0	20	93-C&DH-1261	IT0112 & QRPAN2	Reset EDF & Turn RPA Beam On (Flyby Predict) (suspended after 2 elements) *** (SCEDFC, STRPAN) (x10)
93-262/17:00:05.0	rxocdr06	1:31:40.0	20	93-C&DH-1261	IT0112 & QRPAN2	Reset EDF & Turn RPA Beam On (Flyby Predict) *** (SCEDFC, STRPAN) (x10)
93-262/19:04:28.2	rxocdr07	1:31:40.0	20	93-C&DH-1261	IT0112 & QRPAN2	Reset EDF & Turn RPA Beam On (Flyby Predict) *** (SCEDFC, STRPAN) (x10)

Commands Radiated Since Loss of Downlink

Bit-One Radiation Time	GCMD	Duration	Msgs	CMD RQST #	SCMF	Title / Commands
93-262/21:09:10.5	rxocdr08	1:31:40.0	20	93-C&DH-1261	IT0112 & QRPAN2	Reset EDF & Turn RPA Beam On (Flyby Predict) *** (SCEDFC, STRPAN) (x10)
93-262/23:10:00.1	rxocdr09	1:31:40.0	20	93-C&DH-1261	IT0112 & QRPAN2	Reset EDF & Turn RPA Beam On (Flyby Predict) *** (SCEDFC, STRPAN) (x10)
93-265/02:20:40.3	mbrbon01	2:02:40.0	15	93-MBR-1262	IT0184	Turn On MBR Beacon (Capture Predict) *** (MBPWRE, MBPWRN, MBMCBO("BECNON")) (x5)
93-265/04:52:40.1	mbrbon02	2:02:40.0	15	93-MBR-1262	IT0184	Turn On MBR Beacon (Capture Predict) *** (MBPWRE, MBPWRN, MBMCBO("BECNON")) (x5)
93-265/07:24:40.8	mbrbon03	2:02:40.0	15	93-MBR-1262	IT0184	Turn On MBR Beacon (Capture Predict) (suspended after 12 elements) *** (MBPWRE, MBPWRN, MBMCBO("BECNON")) (x5)
93-265/09:33:00.0	mbrbon04	2:02:40.0	15	93-MBR-1262	IT0184	Turn On MBR Beacon (Flyby Predict) *** (MBPWRE, MBPWRN, MBMCBO("BECNON")) (x5)
93-265/12:05:00.5	mbrbon05	2:02:40.0	15	93-MBR-1262	IT0184	Turn On MBR Beacon (Flyby Predict) *** (MBPWRE, MBPWRN, MBMCBO("BECNON")) (x5)
93-265/14:37:04.9	mbrbon06	2:02:40.0	15	93-MBR-1262	IT0184	Turn On MBR Beacon (Flyby Predict) *** (MBPWRE, MBPWRN, MBMCBO("BECNON")) (x5)
Total Files Radiated:		251	Total Commands Radiated:		2143	

APPENDIX O

TIME DELAYS TO TRANSFER TO LGA

The following information is provided to describe how the times shown in Figure 4-2 were computed. This information describes the different ways (and associated times) that the Mars Observer spacecraft could have established downlink communications on the +Y LGA either by autonomous action or by ground command.

Time Delays to Transfer to LGA by Spacecraft Autonomous Action

A. CMDLOS Time Out

- Earliest possible CMDLOS Time Out (assumes no recovery CMDS received)
 - Last CMD sent before pressurization
 - Set Telecom Normal (QLGXH1)

93-232/21:18:24.3	Transmit Time
+ 2.5	CMD Duration
+ 5/00:00:00.0	CMDLOS Timer Value
+ 38:12.0	RTLTL
<hr/>	
93-237/21:56:38.8	ERT

- Latest CMDLOS Time Out (first 5-day time period with no CMDS transmitted)
 - Last CMD sent before time gap
 - RPA Beam On (QRPAN2)

93-242/11:07:58.4	Transmit Time
+ 40.0	CMD Duration
+ 5/00:00:00.0	CMDLOS Timer Value
+ 38:48.0	RTLTL
<hr/>	
93-247/11:47:26.4	ERT

B. Contingency Mode (CM) Entry

- Earliest

Assumes Sun Ephemeris violation at STRPAN+4:02.5 in nominal sequence due to something (e.g., a serious AACS problem such as gyro motor short)

93-234/00:31:18.631	STRPAN Start
+ 4:04.000	STRPAN Beam On Then CM Turns Off
+ 4:08.000	CM Configures LGA's & Turns RPA On
+ 18:58.000	OWLT

93-234/00:58:28.631 ERT

(Note: CM entry between STRPAN-4.0 and + 4:04.0 will not establish LGA downlink)

- Nominal

Assumes Sun Ephemeris violation about 10 hours (based on observed bias drift) after ANS CMD in nominal sequence due to an AACS control loss

Earliest time + 10 hours + 1 second of additional OWLT

93-234/10:54:26.131 ERT

C. Safe Mode Entry

- Earliest

Assumes a S/C POR is induced at the first pyro firing in the nominal sequence and no uplink commands are received

93-234/00:26:05.631	Fire Pyro 7 & Enter Safe Mode
+ 2/17:00:00.000	Safe Mode Phone Home Delay
+ 4:08.000	RPA Turn On
+ 19:04.000	OWLT

93-236/17:49:17.631 ERT

- Latest

Assumes Safe Mode entry when enabled in the nominal sequence and no reception of the CMDS transmitted between 237/00:34 and 239/03:11

93-236/20:54:38.685	Safe Mode Enable & Entry
+ 2/17:00:00.000	Safe Mode Phone Home Delay
+ 4:08.000	RPA Turn On
+ 19:09.000	OWLT

93-239/14:17:55.685 ERT

Time Delays to Transfer to LGA By Ground Command

A. Contingency Mode Entry

Assumes Arm & Go To Contingency Mode CMD (Q001C1) received

93-234/08:19:22.5	Transmit Time
+ 17.5	CMD Duration
<u>+ 37:58.0</u>	RTLT
93-234/08:57:38.0	ERT

B. Safe Mode entry via SCP 1 Off/On/Select uplink CMDS (IT0168)

Assumes U/L CMDS are received, but RAM S/W problem prevents downlink being established

93-239/11:26:06.6	SCP 1 CMD'd Back On & Selected
+ 3:40.0	CMD Duration
+ 4:08.0	Safe Mode Entry & RPA Beam On Time
<u>+ 38:19.9</u>	RTLT
93-239/12:12:14.5	ERT

C. Swap to RPA 1

Assumes hardware CMDS to turn on RPA 1 (IT0110) received

93-235/01:35:29.0	Transmit Time
+ 10:40.0	CMD Duration Incl. RPA Beam On Time
<u>+ 38:00.0</u>	RTLT
93-235/02:24:09.0	ERT

D. Rotary Switch Position Changed

Assumes Rotary Switch Position B Select CMD (IT115) received

93-235/05:54:37.2	Transmit Time
+ 6:40.0	CMD Duration
<u>+ 38:00.0</u>	RTLT
93-235/06:39:17.2	ERT

APPENDIX P

PYRO VALVE FAILURE MODES

This Appendix describes the investigation of the potential for failure of pyro valves 5 and 7, which could have occurred during the Mars Observer pressurization sequence as described under Hypothesis C4. The two principal sources of information available are: (1) data on similar failures observed on the European Space Agency (ESA) Cluster spacecraft program and (2) analysis and examination of the pyro valves fired during the Mars Observer pyro shock testing.

I. Cluster Program Failures

J. B. Bruggemann of ESA/ESTEC (European Space Research and Technology Center) visited JPL on October 15, 1993, to discuss the failures encountered in the Cluster spacecraft program. This section provides a synopsis of the data he provided.

The Cluster program uses 3/8-in. OEA Pyronetics pyro valves (Model 1467-24) for propellant isolation during launch. However, during testing ESA used Model 1467-15 valves, which are very similar to the flight valves. These valves are also very similar to the models 1467-19 and 1467-20 pyro valves used on Mars Observer. Specifically, the location, retention, size, and composition of the booster charge is the same for all of these valves, as is the upper part of the housing holding the booster charge.

During pyro shock testing in July 1993, one of these Model 1467-15 valves was fired and its initiator was ejected. The lock wire holding the initiator in place was broken, and the initiator, its connector, and the spacecraft wiring harness were thrown several feet, impacting the spacecraft solar panel. A bracket and pipe hold-down were also broken. The trajectory appeared to be essentially a straight line aligned with the axes of the two initiators. This pyro valve used a booster charge of the same size as the Mars Observer flight booster charge.

The velocity of the initiator was estimated to be 200 m/s, based on the measured distance and recorded accelerometer data, which allowed identification of the time of pyro firing, the time of initiator ejection, and the time at which the solar panel was struck. It was noted that the shock signature seen when the initiator was ejected was much more severe than that seen in a normal pyro valve firing.

Examination of the failed pyro valve showed that the threads in the titanium valve body had failed, allowing the initiator to be expelled. The titanium valve body threads holding the other initiator and the booster cap in place were also seen to be heavily damaged, as shown in Figures P-1 and P-2. It appears that the hot combustion gases attacked and eroded the titanium threads; little deterioration was seen on the initiator threads, which are made of Inconel.

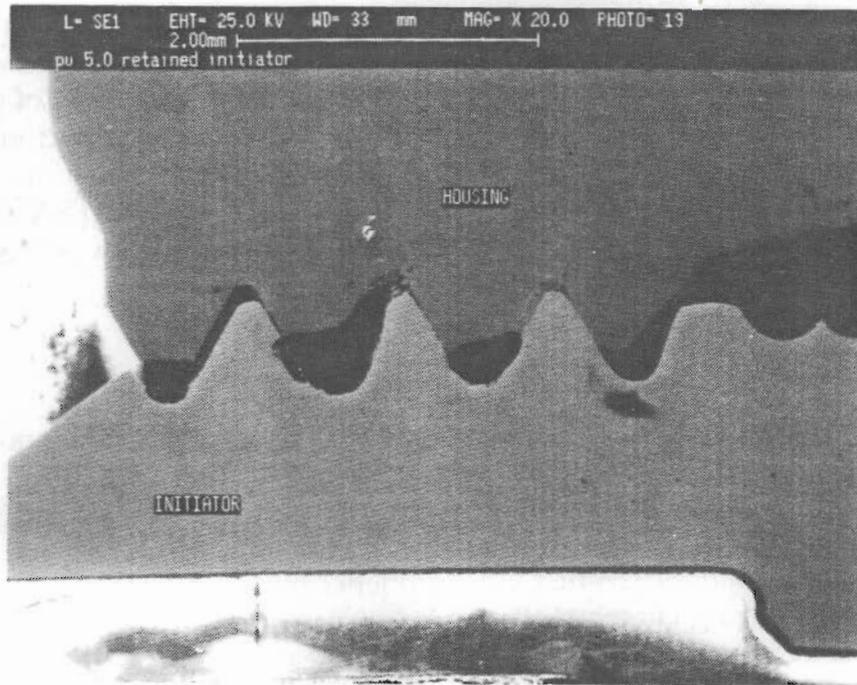


Figure P-1. Detail of the thread of the passive initiator, showing erosion damage to the Ti-alloy thread and to the Inconel 718 thread.

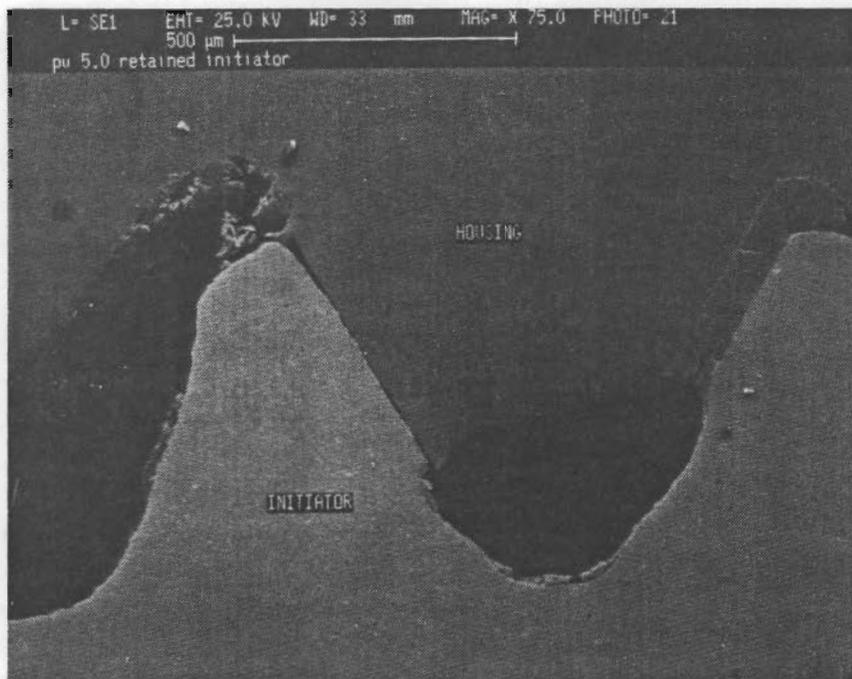


Figure P-2. Detail of eroded initiator and housing threads. In every case, the Ti-alloy thread is eroded at the top of a tooth and the Inconel at the opposite side at the root of the thread. Firing residue can be seen between the threads.

Similar, but less extensive, thread damage was seen on a 1467-10 valve which did not eject its initiator. Therefore, although the 1467-10 contains a smaller booster charge and did not actually fail, similar concerns could exist for that valve as well.

Two subsequent tests were performed using model 1467-15 valves, using 100 percent of the flight booster charge load, with no design modifications. All ejected their initiator, except for one which was held together by external brackets. In this unit, extensive erosion and blow-by of the titanium threads indicated that a failure could have occurred had the initiators not been restrained.

On October 14, 1993, a test was performed using a simulated pyro valve body to test the remedial actions recommended by the valve vendor: (1) boron nitride was applied to the threads as a sealant, and (2) the aluminum booster retainer cage used previously was replaced with a stainless steel cage. In order to demonstrate margin, a booster charge 130 percent of the flight load was used in this test. The result was that an initiator was ejected.

In the Cluster application, the firing command to the two redundant initiators is separated by more than 10 ms for power reasons. When the first initiator is fired electrically, the second regularly fires "sympathetically" due to exposure to the hot gases produced by the first initiator and combustion of the booster charge. This is similar to the situation on Mars Observer, in which only one initiator was wired to the pyro relay assembly in order to reduce mass.

Sympathetic firing of the second initiator may be related to the failures experienced on the Cluster program. Figure P-3 shows the pressure history of the simulated pyro valve firing of October 14, 1993. About 1.09 ms after the firing signal was sent, the first initiator ignited, producing the rapid pressure rise seen in the next 85 μ s. Then the booster charge began to combust, raising the cavity to a peak pressure of 33,000 psia in another 730 μ s. Bruggemann hypothesizes that this peak is enhanced by the sympathetic firing of the second initiator during this time frame. This seems to be a reasonable hypothesis. There is certainly no evidence to suggest that firing of the second initiator took place after this peak pressure, as the pressure trace did not show a secondary peak in the following 2.3 ms. At that time (4.23 ms after the fire command) the first initiator was ejected. The ESA hypothesis holds that the ejection of the initiator is a result of the higher peak pressure induced by sympathetic firing and/or impingement of the second initiator effluent directly on the first initiator, producing enhanced erosion of the threads of the first initiator.

In each of the four incidents of initiator expulsion, the initiator that was fired electrically was expelled. However, the threads holding the other initiator were so badly eroded that it is not clear whether this (ejection of the electrically fired initiator) was a causal relationship or coincidence. One argument for coincidence is that examination of the qualification unit Cluster valves (in which the initiators were fired simultaneously) revealed significant erosion of the titanium housing—at one point the

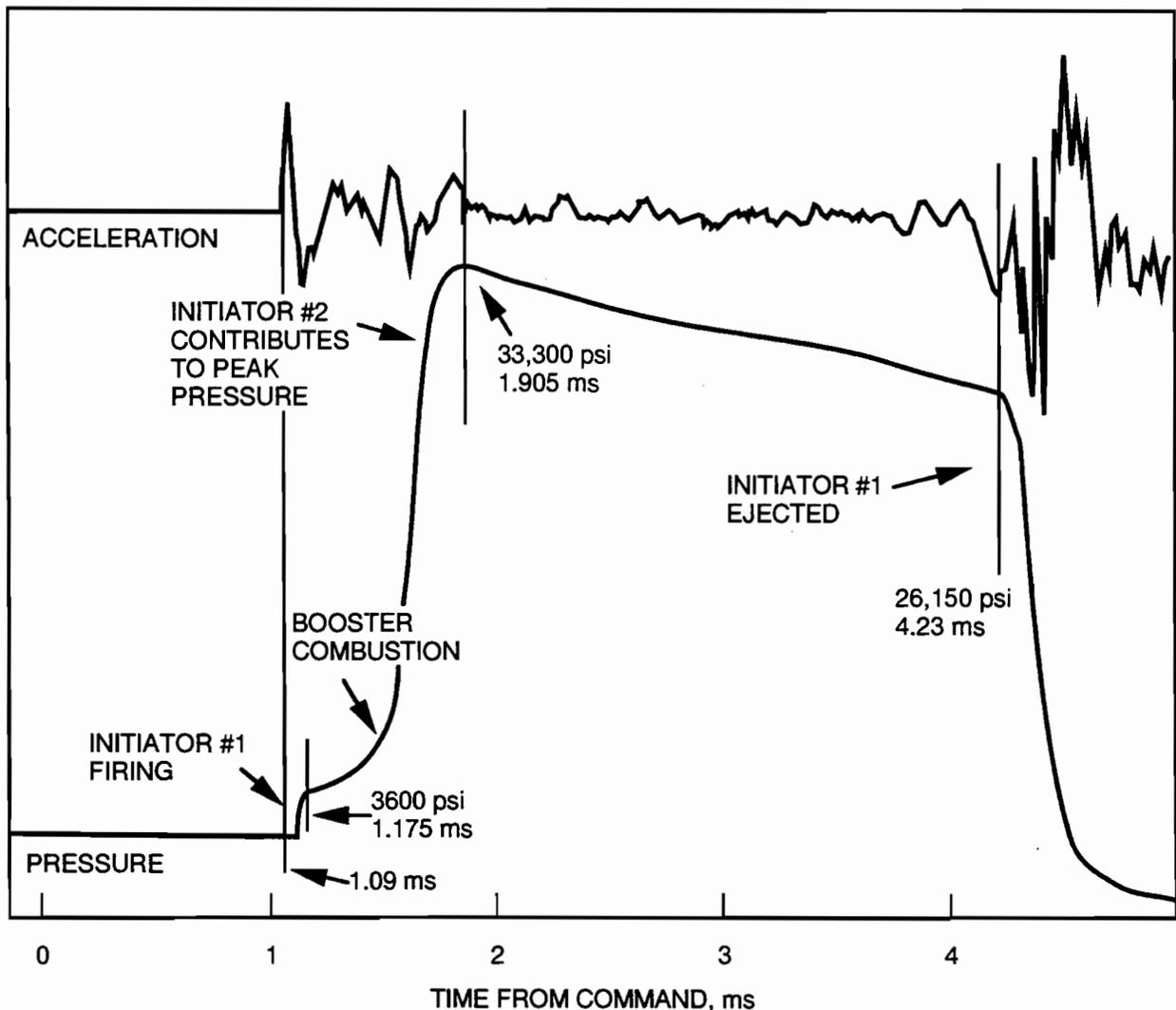


Figure P-3. Pressure history from simulated pyro firing valve.

hot combustion gasses had eroded through over 60 percent of the housing thickness. This appears to indicate a fundamental incompatibility between the titanium housing material and the hot products of combustion. This observation leads to the speculation that these failures could have led to the ejection of either initiator. Bruggemann agreed that this was certainly possible. Unfortunately, the qualification units were not sectioned in a plane that would allow inspection of the threads which retained the initiators.

That the ejection of the initiator is not strictly deterministic is further supported by an additional test of a simulated 1467-15 valve with sympathetic firing of OEA initiators (model 4704) and a 130-percent booster charge conducted at OEA on October 15, 1993. The pressure trace of Figure P-4 shows that the peak pressure was actually higher than that of the October 14, 1993, test (and much higher than the original failures using 100-percent booster charge loads), but neither initiator was expelled.

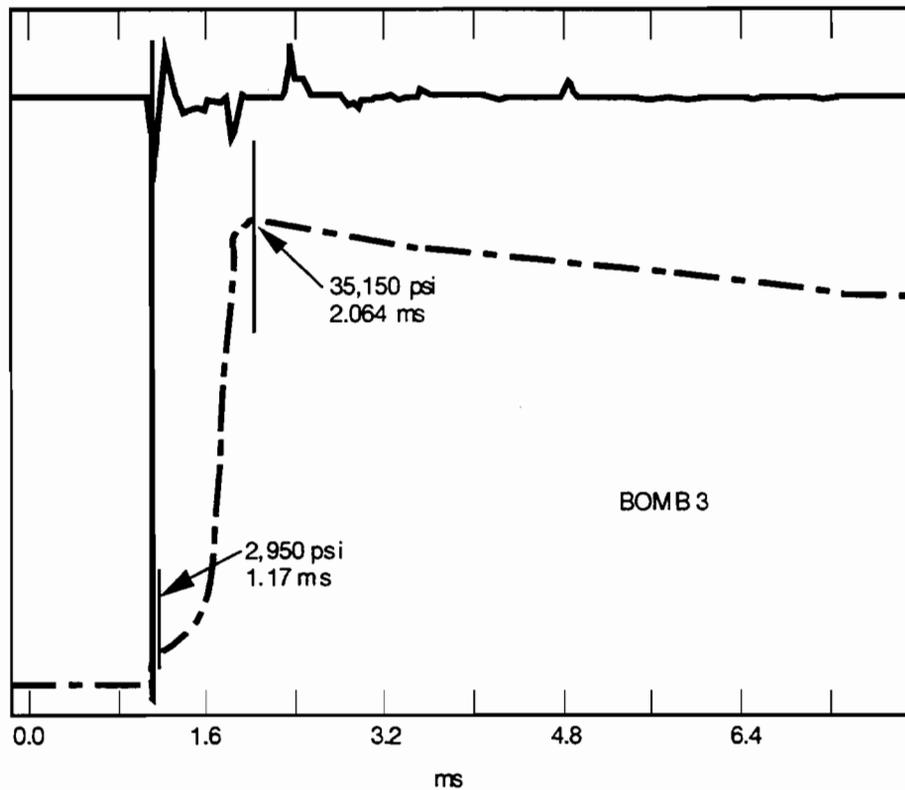


Figure P-4. Pressure history from simulated pyro valve firing #2 using OEA initiators.

The pyro valve vendor and others have speculated that these failures could have been the result of using initiators manufactured by OEA Pyronetics rather than NASA Standard Initiators (NSIs). This is possible, but only if the valve design is on the verge of failure even when NSIs are used. This is because the OEA initiators and NSIs are very similar. The composition and amount of propellant used in the OEA initiators is the same as a NSI, and the mechanical configurations are nearly identical. Bruggemann provided the following data from lot acceptance testing of 59 OEA initiators and 22 NSIs:

	NSI	OEA 4704
Peak pressure, psia	634	690
Standard deviation, psia	19	21
Time to peak, ms	2.2	3.2

These data provide the peak pressures generated by firing the initiators into a 10-cm³ volume. The specified maximum for NSIs is 750 psia. Subsequent bomb test data provided by OEA indicate that the peak pressures with 130-percent booster charges are reduced about 10–15 percent when NSIs are used. This is insignificant as compared with the difference in peak pressure between a 100-percent booster charge (the original Cluster failures had this charge) and a 130-percent booster charge (where one bomb test

using the OEA initiator did not eject an initiator). Other characteristics of the pressure-time history were found to be significantly different when NSIs were used in bomb tests. For example, the sympathetic firing of the second initiator occurred after peak pressure had been reached. However, it is not clear how these differences affect the likelihood of initiator expulsion.

In summary, the test history of these pyro valves on the Cluster program is:

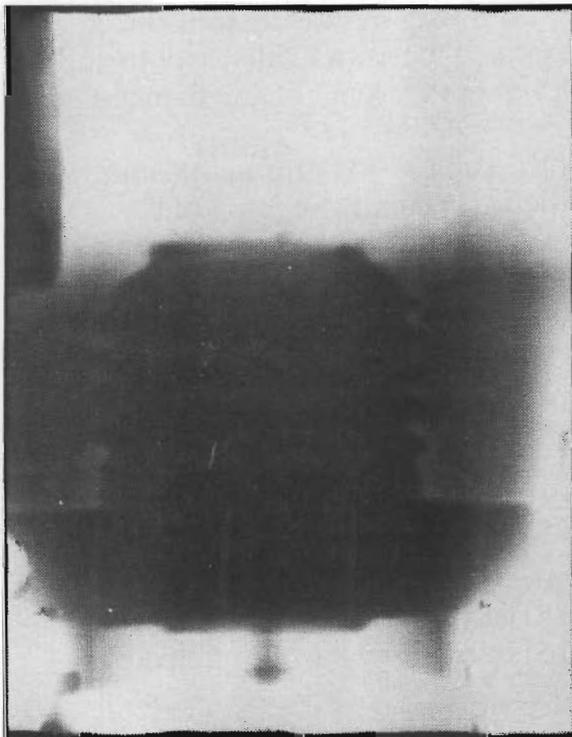
- (1) Three qualification units were tested with up to 130-percent booster charge without expelling the OEA 4704 initiators when the initiators were fired simultaneously.
- (2) Three units experienced (or would have if not restrained) ejection of the electrically initiated OEA 4704 initiator using 100-percent booster charge when one initiator was allowed to fire sympathetically.
- (3) Two simulated valves were tested using 130-percent booster charges and sympathetic ignition of one OEA 4704 initiator. Only one unit experienced ejection of the electrically initiated initiator; the other had no ejection.
- (4) Two simulated valves were tested using 130-percent booster charges and sympathetic ignition of one NSI. Neither test exhibited ejection of a NSI.

When the statistical sampling involved in these tests is considered, it is impossible to draw firm conclusions as to the existence of a causal relationship of initiator type or firing mode to the occurrence of these failures.

II. Mars Observer Pyro Valve Evaluation

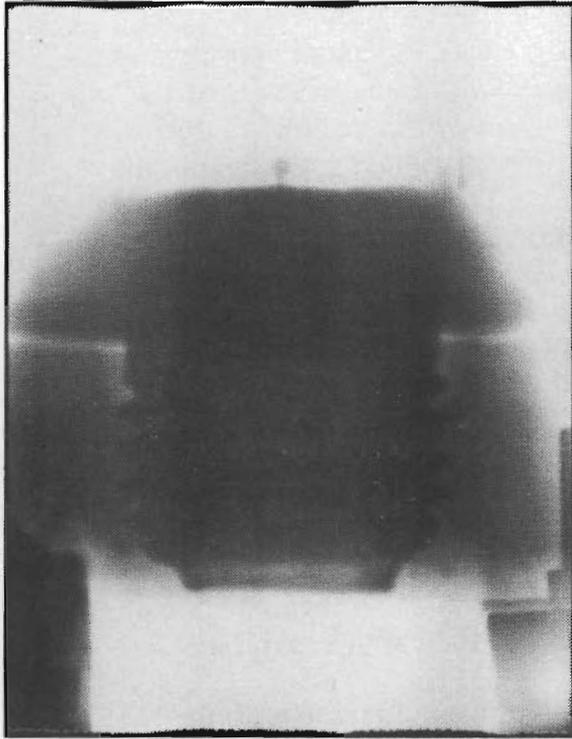
X-rays of the two Mars Observer pyro valves fired during pyro shock testing were received from Astro. These photographs are reproduced in Figure P-5. They do not resolve the titanium threads very well, but there are low-density regions around the NSI threads that indicate damage to the titanium threads. Damage was fairly evident around the booster plug threads of serial number 003. Although reading of these X-rays is somewhat subjective, Lynn Lowry of the JPL Materials Laboratory thought that thread erosion was fairly clear in these photographs.

Further examination of these two valves is to include: (1) removal of all initiators and recording the torque required to loosen them, (2) visual inspection and photography of the threads on the NSIs and in the valve bodies, and (3) removal of the booster plug following similar inspection procedures. These data have not yet been received from Astro, although it has been reported that the torques required to remove the initiators were in all cases close to installation torques. This indicates that the tensile preload of the threads had not reduced significantly, which could be consistent with such damage as that shown in Figures P-1 and P-2.

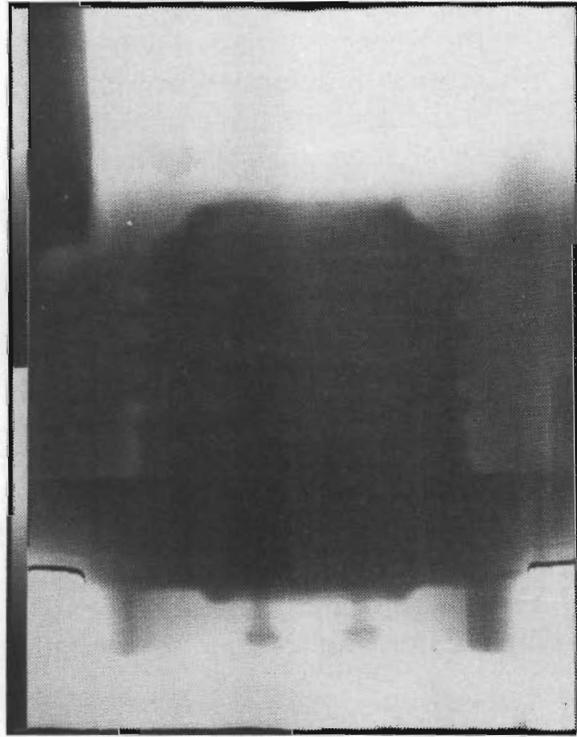


SN003

LEFT

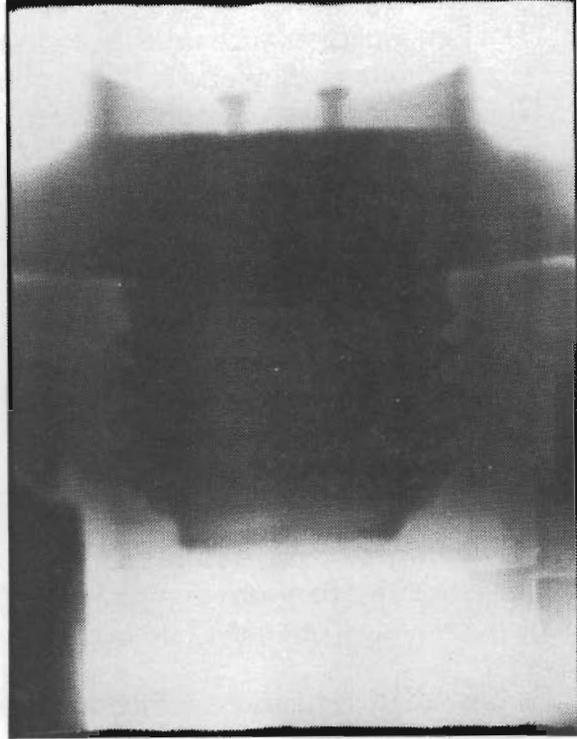


RIGHT



SN001

LEFT



RIGHT

Figure P-5. X-rays of pyro valves fired in Mars Observer pyro shock tests.

The test history of the Mars Observer pyro valves can be summarized as follows:

- (1) Ten lot acceptance units were tested using 80- to 120-percent booster charges without ejection of a NSI. No sympathetic NSI ignitions were tested.
- (2) Two units were fired with sympathetic ignition of the second NSI during pyro shock testing without ejection of a NSI. However, x-rays indicate that the titanium threads were damaged.
- (3) Pyro shock test data indicate that an additional two pyro valves were fired, but Astro cannot confirm the existence, much less the condition, of these valves.

As in the case of the Cluster test history, it is not possible to draw firm conclusions as to the feasibility of this failure mechanism based wholly upon pass/fail criteria for this small statistical sample.

Additionally, a preliminary review by R. Bamford of the stress analysis of the initiator threads indicates that the structural margin of these threads may be fairly low. Thread damage or temperatures above those assumed could lead to failure of the titanium threads. Bamford is proceeding with a more detailed stress analysis using detailed drawings, obtained late in this investigation, of the valve and initiator.

Follow-on investigations which have been initiated in conjunction with the NASA Review Board include:

- (1) Destructive examination of the Mars Observer lot acceptance test valves by careful sectioning (e.g., with a diamond saw). The cut plane passes through the centerline of both NSIs. Although some of these valves were fired with two initiators simultaneously while others were fired with a pressure transducer in the second position, it will be valuable to examine them for evidence of thread erosion or deformation and to determine whether the extent of any damage correlates with test conditions.
- (2) Destructive analysis (as in item 1 above) of the valves fired during upcoming pyro shock testing. These valves will experience sympathetic firing of the second NSI.

These analyses are required to be more definitive, but the required analyses have not been completed. As of this writing, four of the lot acceptance test units have been x-rayed and all showed some degree of thread damage. One test unit was sectioned and subjected to thorough analysis. It was concluded that thread damage on that unit was primarily due to chemical attack by the combustion products. Chlorine and fluorine compounds in the NSI charges were the primary reactive agents. With the available data, it is clear that even though no NSI expulsion was documented in Mars Observer lot acceptance or pyro shock firings, such a failure is a credible cause of the Mars Observer loss-of-signal anomaly. For such a failure to occur, it is necessary (1) that PV-5 eject an initiator, and (2) that the sympathetically fired initiator be the one ejected.

APPENDIX Q

STRUCTURAL ANALYSIS OF THE MARS OBSERVER TWTA CATHODE HEATER SUPPORT TUBE

I. Introduction

This Appendix addresses an updated evaluation of the structural integrity of the Mars Observer Traveling Wave Tube Amplifier (TWTA) cathode support tube. This is a continuation of the study described in an earlier report.¹ Additional information was gathered from a TWTA meeting held at Hughes EDD on October 11, 1993,² allowing more accurate analysis to be conducted. JPL has performed an analysis of the structure, and the results are reported herein.

II. Information Gleaned from the Mars Observer TWTA Meeting

It was learned from the TWTA meeting³ that the cathode support tube was seam welded with a lap joint formed from 0.5-mil-thick Mo/Re 50/50 sheet material. The attachment of the support tube to the Kovar cathode base mounting ring is accomplished by having the tube rest inside the inner diameter of the mount ring and spot welding the tube to the mount near the end of the tube (see Figure Q-1). Twelve spot welds, 0.25-mil diameter each, are equally spaced around the circumference of the tube. It was mentioned at the meeting that test specimens as well as actual cathode assemblies were pull tested; however, test data were not yet available. The spot welds were located by raised dimples in the support tube, indicating that the fit of the tube in its socket was not exceedingly snug.

The radial distance between the cathode and the surrounding focus electrode (see Figure Q-2) is 5 ± 0.1 mil. The focus electrode could conceivably limit the lateral deflection of the cathode. However, 5 mil is a large displacement for the cathode, and breakage may occur before contact. It was mentioned in the meeting that small amounts of permanent deflection (~1 mil) of the cathode would not prevent the TWTA from functioning, but would cause some beam defocus and loss of performance efficiency.

It was estimated that the Kovar cathode mount would reach a temperature of 200–300 °C, 5 min after the TWTA was turned off. The cathode and support tube would have a temperature very close to the temperature of the mount. It was reported that the cathode heaters had been cycle tested at Lincoln Laboratories, but those records are not yet available.

¹ A. Kissil, *Evaluation of Mars Observer TWTA Cathode Support Tube Pyro-Shock Analysis*, JPL Interoffice Memorandum 3541-93-214, Jet Propulsion Laboratory, Pasadena, California, October 8, 1993.

² Hughes FAX MAM-93-424, *Mars Observer TWTA Meeting on October 11, 1993*, M. A. Matsuoka of Hughes EDD to Jet Propulsion Laboratory, Pasadena, California, October 8, 1993.

³ *Ibid.*

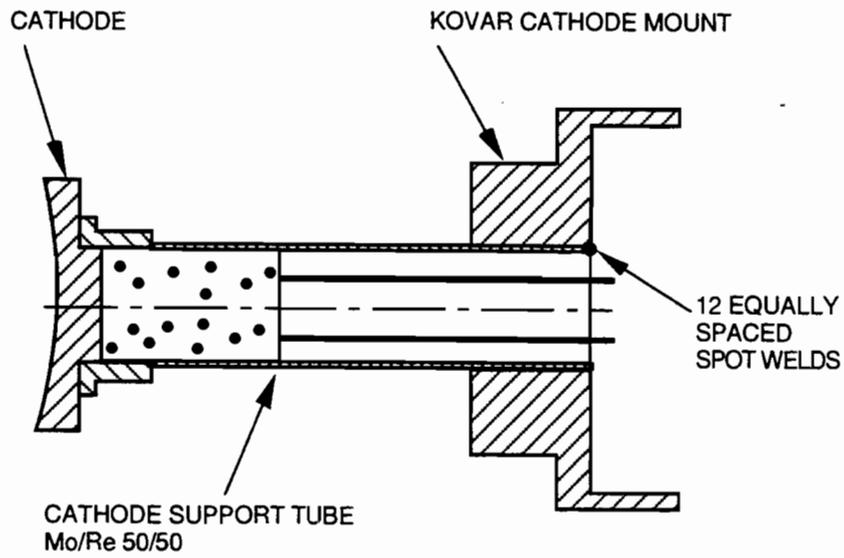


Figure Q-1. Mars Observer TWT cathode and support structure.

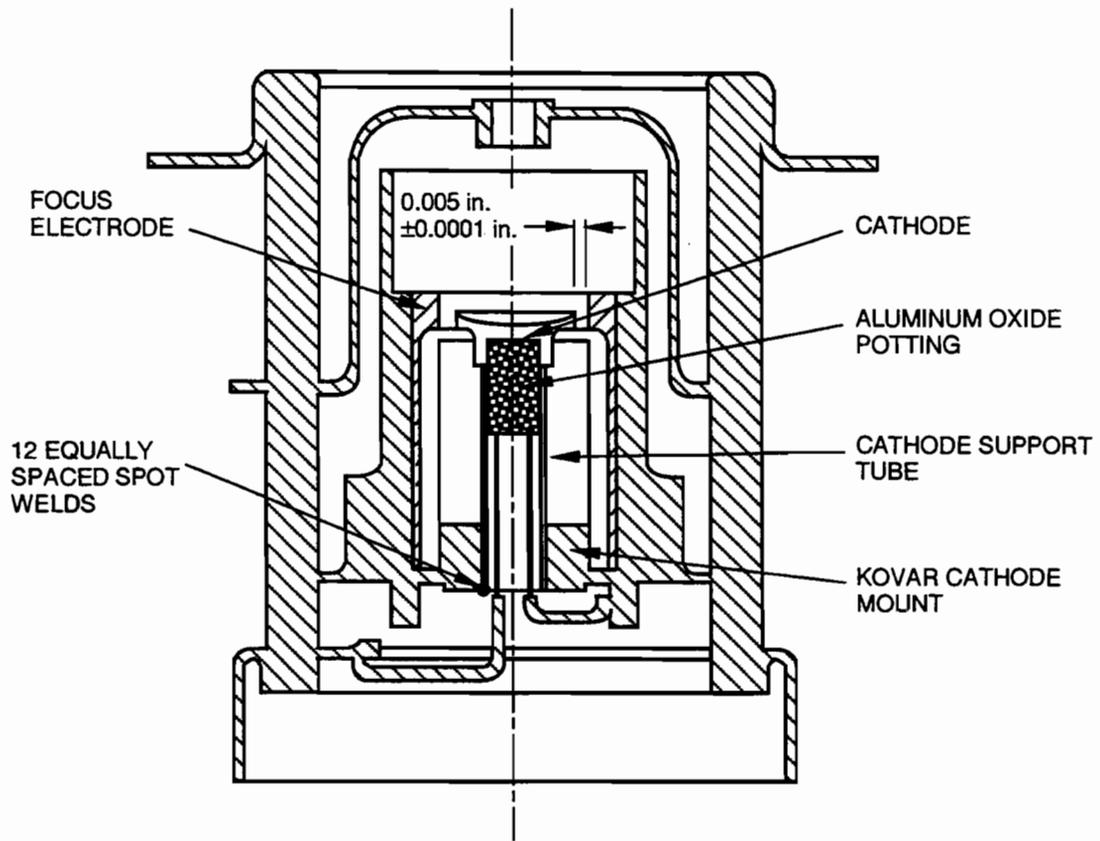


Figure Q-2. Mars Observer TWT cathode mounting configuration.

Pyro shock testing had previously been performed on a similar TWTA, namely the 3618-7 DSCS III. The test had been performed cold, i.e., power off and at room temperature, using a drop hammer.

III. Analysis of the Cathode Support Tube

An analysis was performed of the TWTA cathode support tube to find its capability in terms of quasi-static acceleration of the cathode (g-level). An ultimate tensile stress of 180 ksi was used for the support tube material, which is an approximation of the properties of 400 °C. For acceleration along the axis of the cathode, the ultimate capability was found to be approximately 665 g's. This calculation is based on the load being carried evenly by 12 perfect spot welds. Although sinusoidal distributions are assumed for the normal and shear stresses around the spot welds, additional stress concentration is not used.

For acceleration in the direction lateral to the cathode axis, the maximum stress in the tube was found to occur near the end. The capability of the tube depends on the orientation of the seam with respect to the direction of acceleration. For the case where the seam is at the location of maximum stress, a stress concentration factor of 4 is used. The lateral ultimate capability was found to be in the range of 71–137 g's, depending on the seam orientation. In this calculation, it is assumed that the spot welds contribute as much as 35–70 percent to the overall bending strength, with the remainder carried by line contact with the supporting cylinder. It should be noted that the tube may buckle before the ultimate tensile stress is achieved, and post-buckling analysis or test would be necessary to determine if subsequent breakage would occur.

The detailed calculations of the results reported herein can be found in an earlier report.⁴

IV. Summary and Conclusions

Following the TWTA meeting on October 11, 1993, an analysis was performed to examine the structural capability of the cathode support tube. It was determined that the cathode support had an axial capability of 665 g's and a lateral capability of 71–137 g's. If the Mars Observer in-flight pyro shock environment is higher than these capabilities, structural failures of the TWTA cathode support tube can occur.

⁴ A. Kissil and R. Bamford, *MO TWTA Cathode Support Tube Strength Calculations*, JPL Interoffice Memorandum 3541-93-225, Jet Propulsion Laboratory, Pasadena, California, October 21, 1993.

APPENDIX R

AACS SIMULATIONS

I. RWA Overspeed Scenario (S7) Details

Skew Wheel Spin-up: The skew wheel spins up in deploy mode causing about a 1-deg/s spacecraft angular velocity. REDMAN is disabled in deploy mode and also for wheel speeds in excess of 6000 rpm. The switch out of deploy mode turns off this wheel. The spacecraft should recover within 20 min of Go ANS, with no lasting harmful effects. HGA downlink would have been seen, but 16 min late (see Figure R-1).

X-wheel spin-up: Simulations show that the motion resulting from nominal control about the Y- and Z-axes with the X-wheel stuck at 9000 rpm would allow approximately one 2-min period every 4.5 min when the LGA is within 80 deg of the Earth Line. An X-axis scale factor error of 1360 PPM causes the 2-deg Sun-Monitor-Ephemeris limit to be exceeded at about 36 min from the start of pressurization. This will put the spacecraft in Contingency Mode and switch to LGA uplink and downlink (see Figure R-2).

Y-wheel spin-up: Simulations show that with a Y-wheel spin-up, the X- and Z-axis control algorithms remaining are able to keep the Y-axis pointed at the Earth within about 3 deg (see Figure R-3).

Z-wheel spin-up: Nominal desaturation triggered, followed by emergency desaturation 15 min later. Simulations show that the motion resulting from nominal control about the X- and Y-axes with the Z-wheel stuck at 9000 rpm would allow approximately one 40-s or greater period every 4 minutes when the LGA is within 80 deg of the Earth Line. A Z-axis scale factor error of 2500 PPM causes the 2-deg Sun-Monitor-Ephemeris limit to be exceeded about 22 min from the start of pressurization. This will put the spacecraft in Contingency Mode and switch to LGA uplink and downlink (see Figure R-4).

R-2

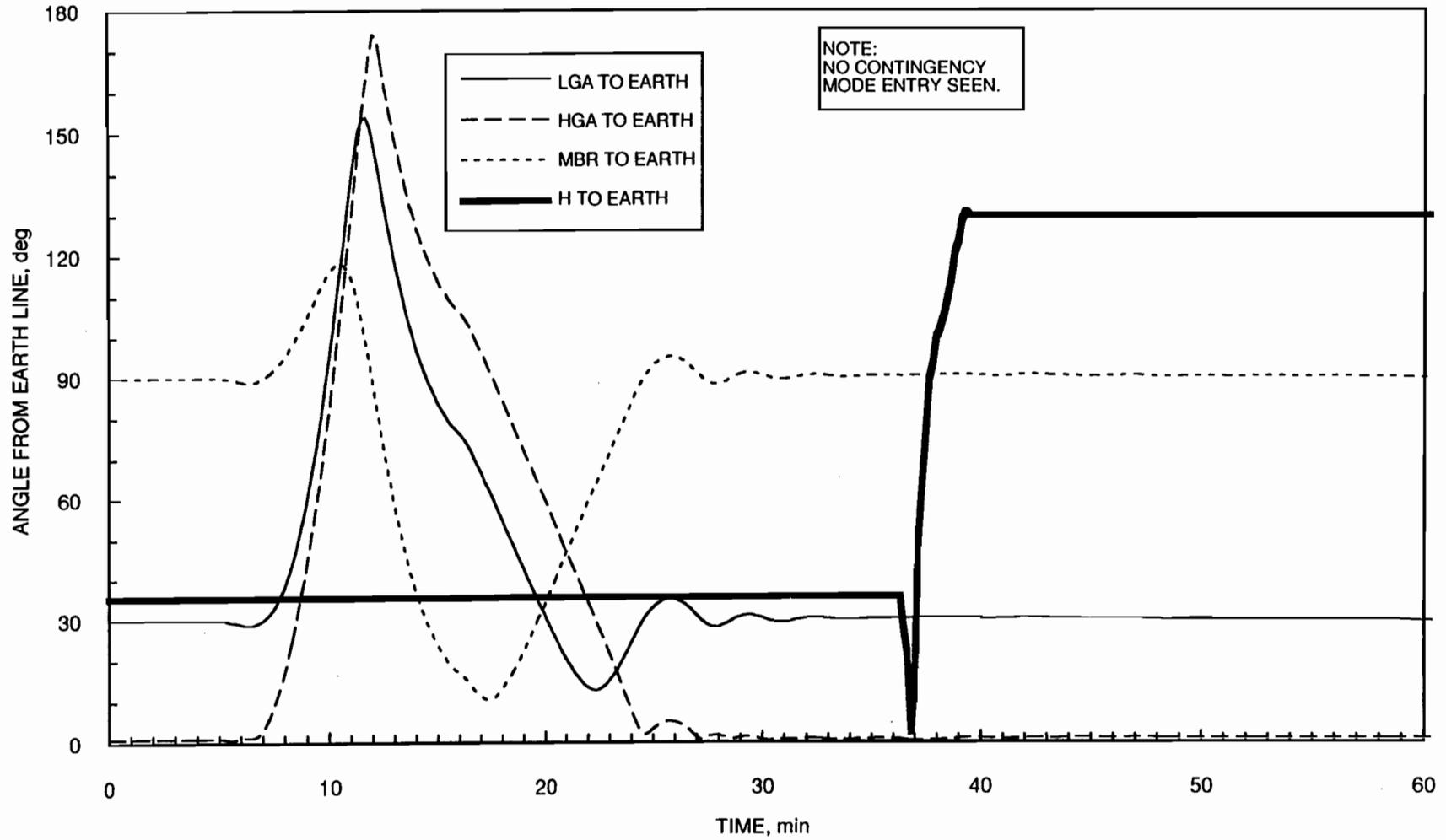


Figure R-1. RWA S uncontrolled spin-up to 9000 rpm.

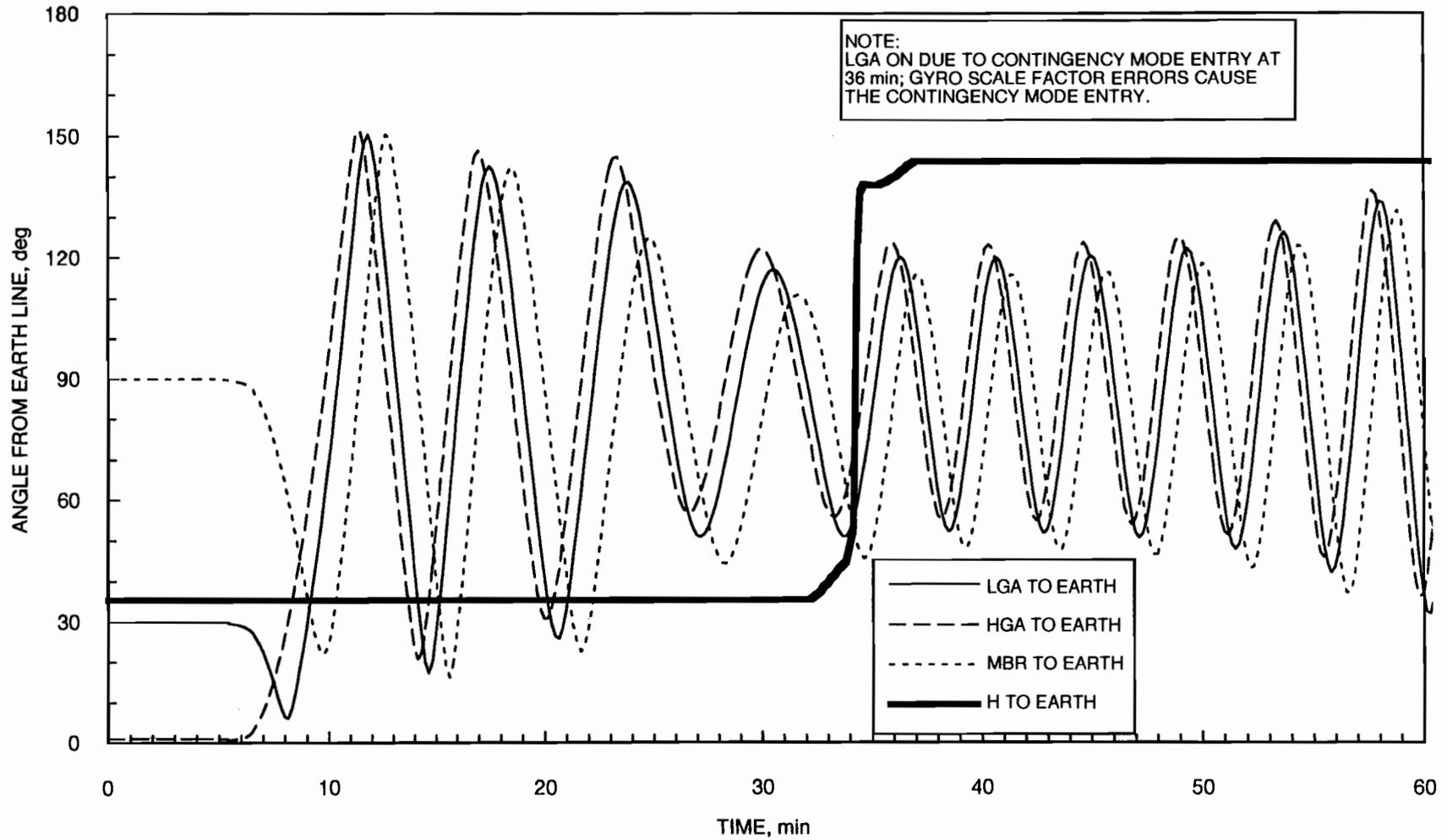


Figure R-2. RWA X uncontrolled spin-up to 9000 rpm.

R-4

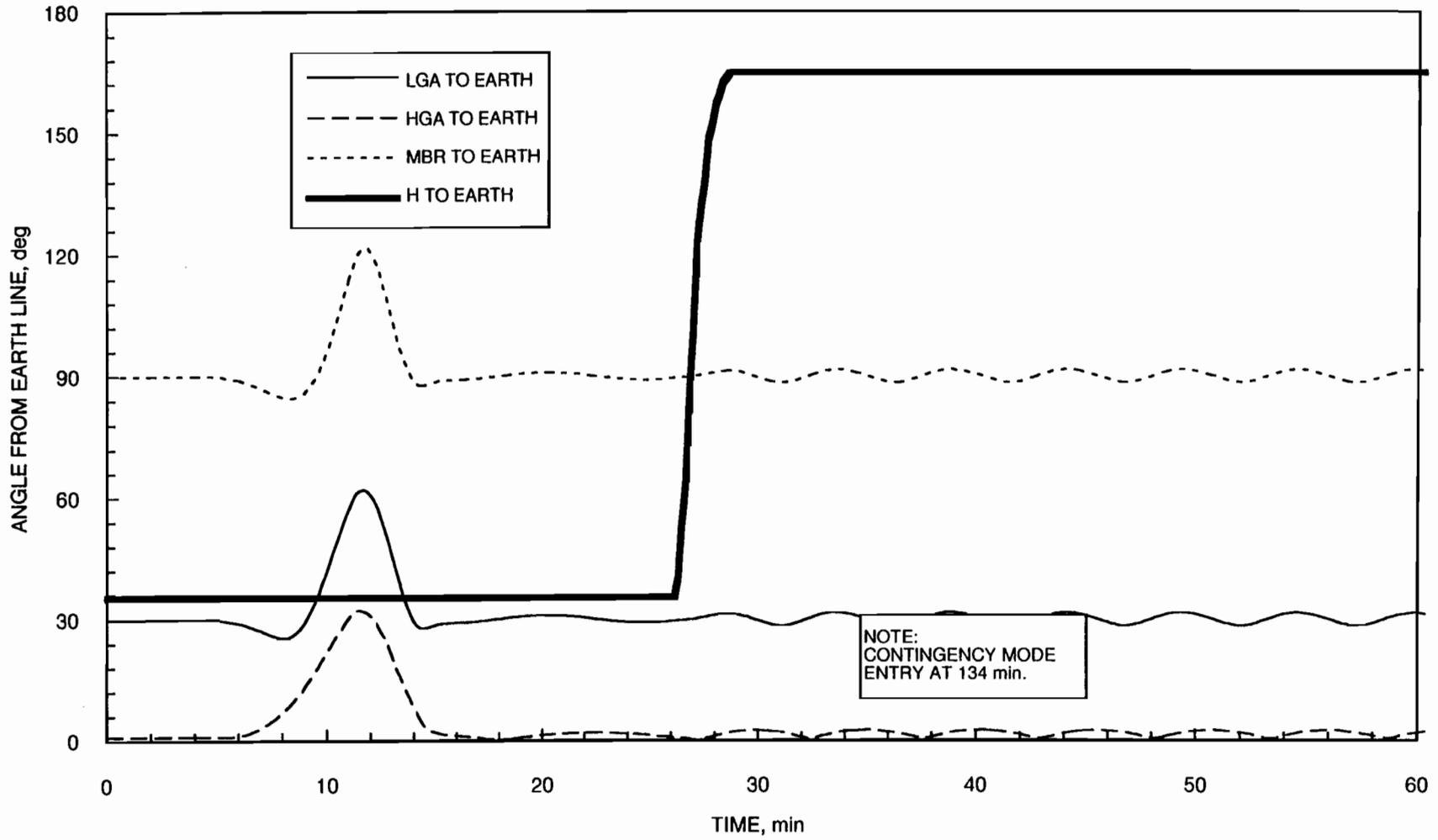


Figure R-3. RWA Y uncontrolled spin-up to 9000 rpm.

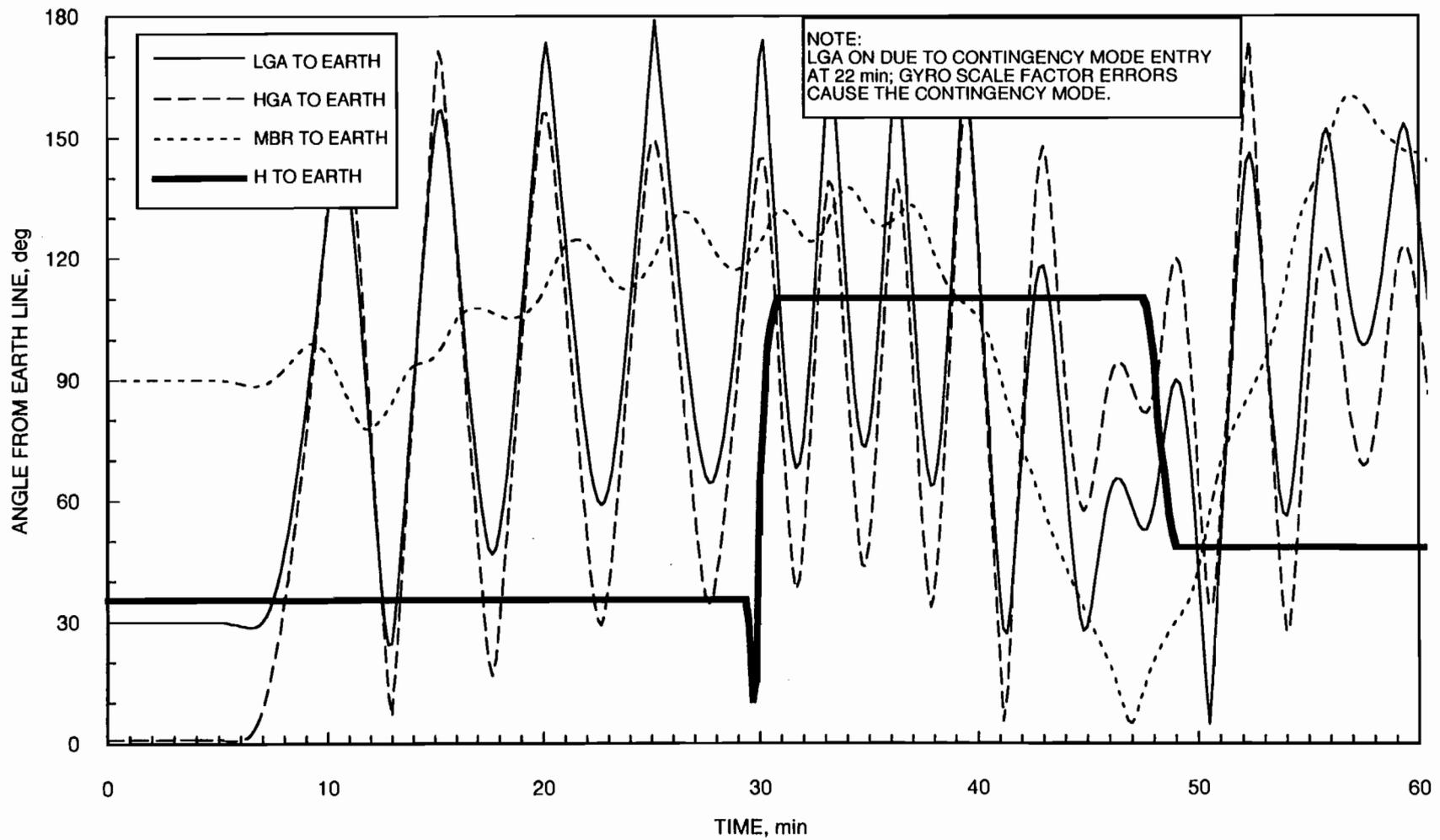


Figure R-4. RWA Z uncontrolled spin-up to 9000 rpm.

II. IMU Motor Short Scenario (S5) Details

When all the gyros spin down and give full-scale readings (of unknown sign), the control algorithm will apply torques to the RWAs in an attempt to reduce the spacecraft angular velocity. Eight different cases are possible: all combinations of spinning each wheel with either sign. Four of these were investigated on VTL in an attempt to understand the resulting dynamics. The first 160 min of each were simulated, and excerpts from the resulting antenna-to-Earth line time histories are shown in Figures R-5 through R-8. Although these simulations do not extend to the 309-min mark when RPA Beam-on commands could have been received, it is clear that the attitude dynamics have settled into a repetitive pattern as the spacecraft spins and nutates.

For uplink, notice that the angle to the Earth line crosses 90 deg every 110 to 140 s, so the chance of a 40-s duration RPA Beam-on command being received entirely by one LGA or the other is between 64 and 72 percent.

For downlink, notice that if the RPA beam is on, there are 1- to 2-min periods approximately every 4 to 5 min when the LGA to Earth line is less than 80 deg and the signal should be detected.

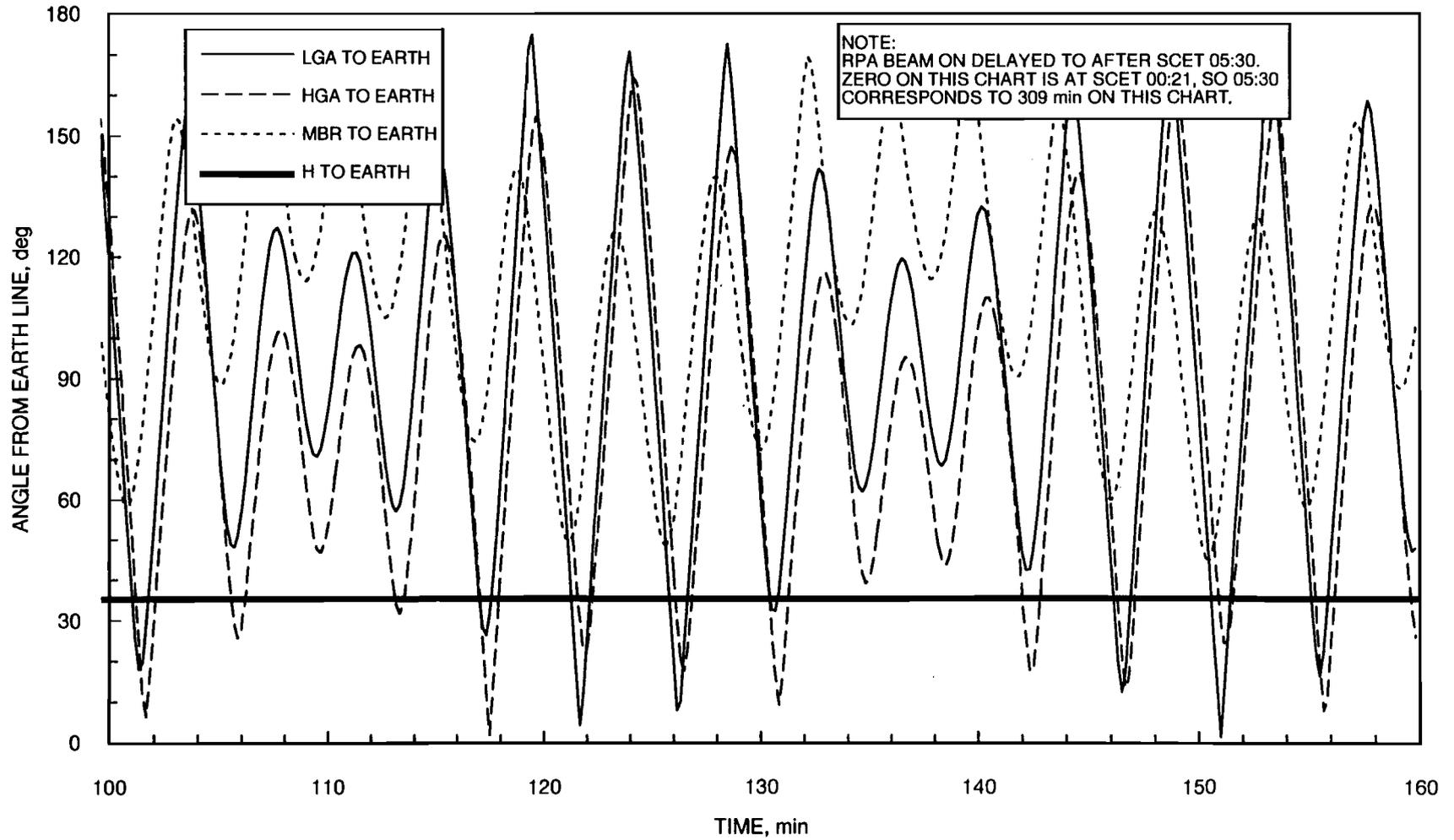


Figure R-5. IMU spin motor short, RWAs at +6500, -6500, -6500 rpm (X, Y, Z, respectively).

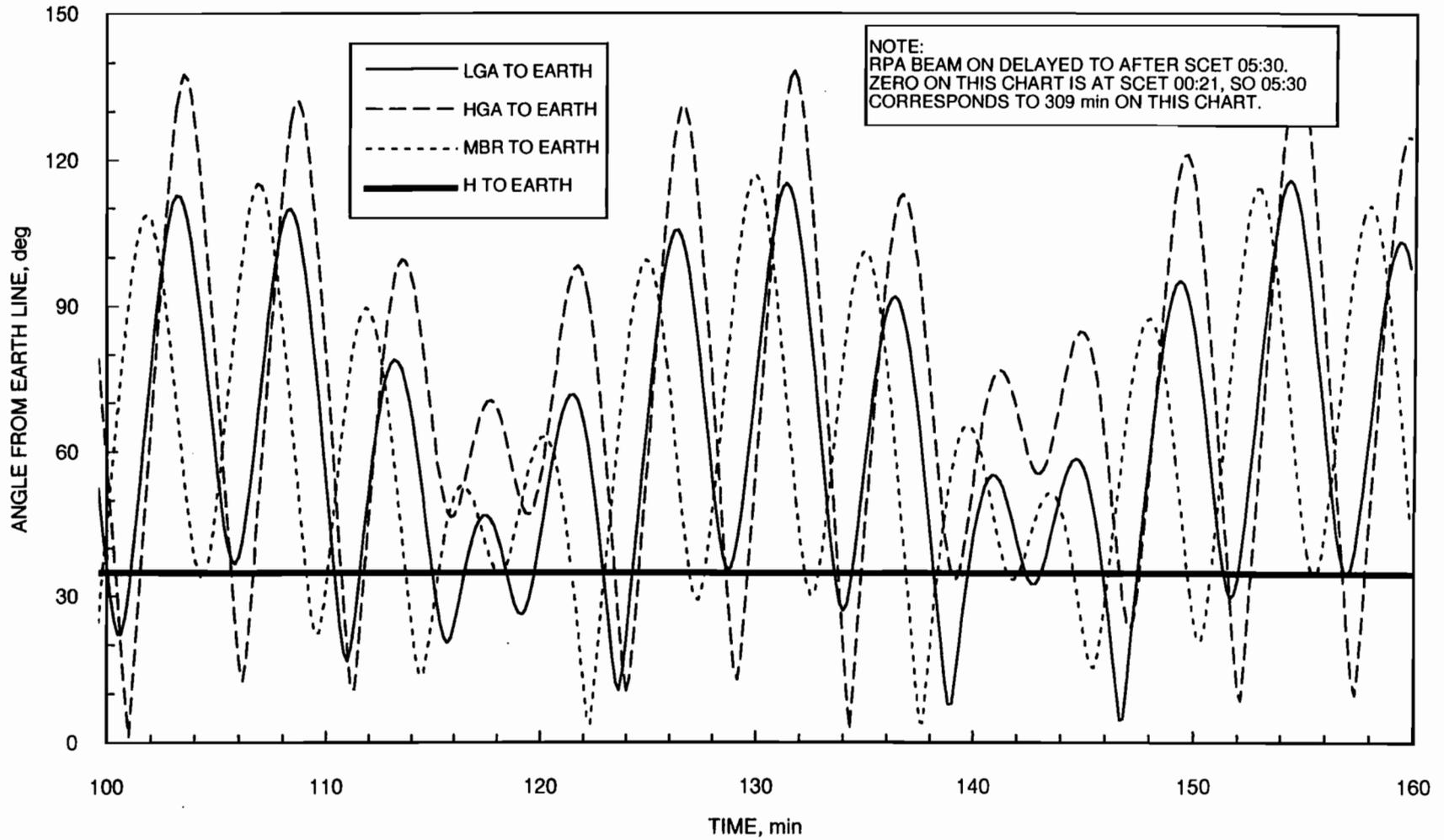


Figure R-6. IMU spin motor short, RWAs at +6500, -6500, +6500 rpm (X, Y, Z, respectively).

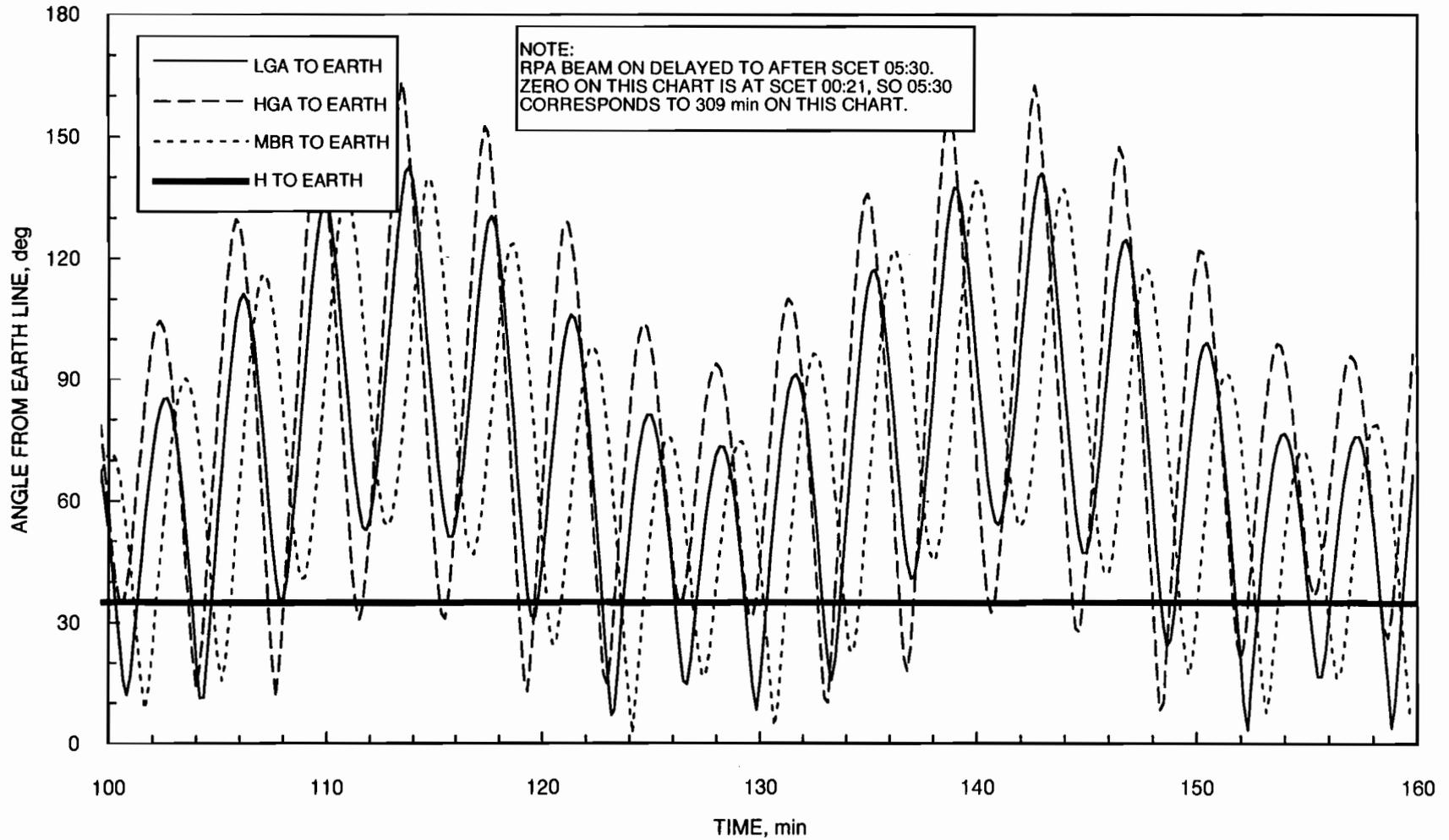


Figure R-7. IMU spin motor short, RWAs at -6500 , -6500 , $+6500$ rpm (X, Y, Z, respectively).

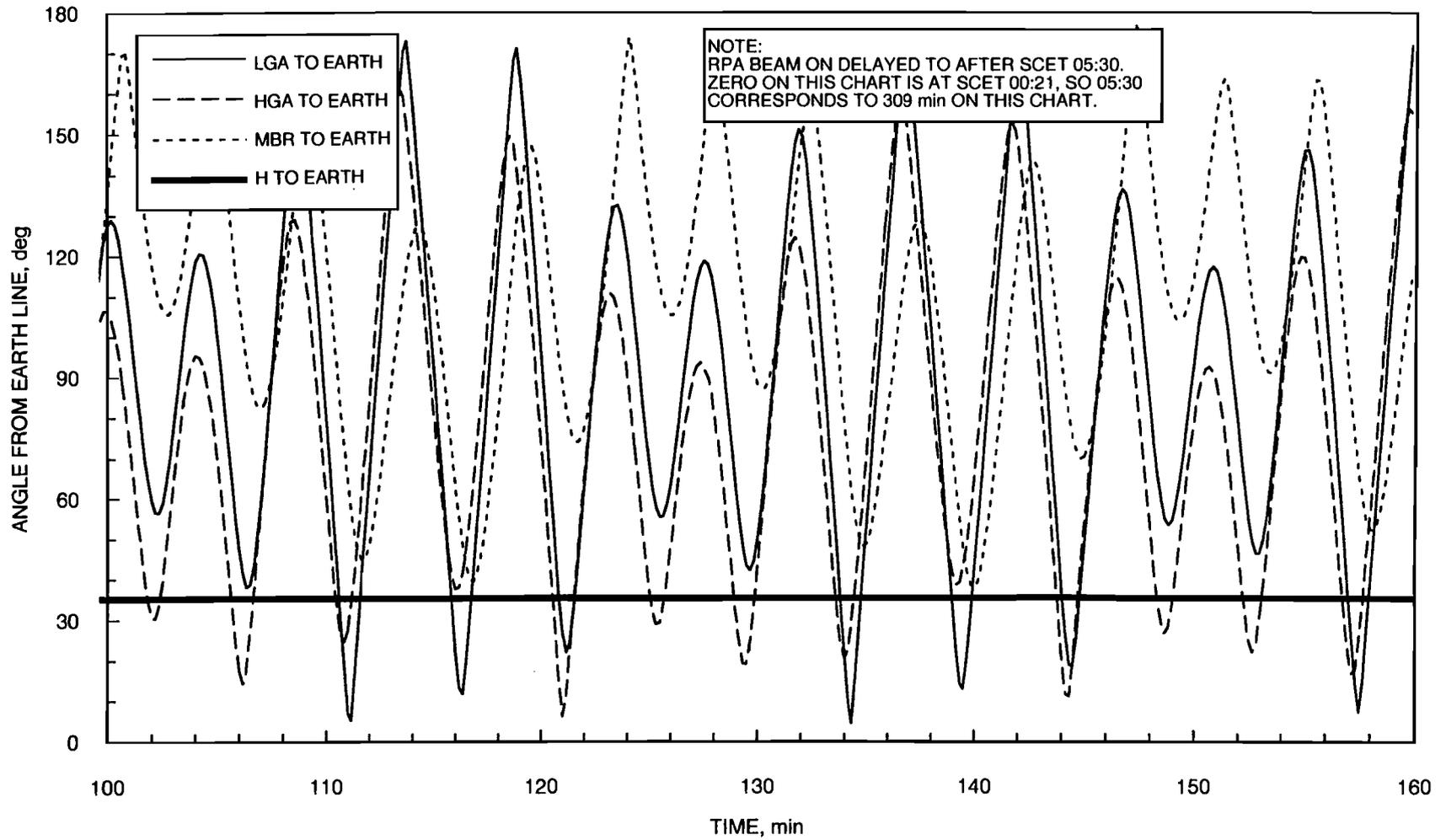


Figure R-8. IMU spin motor short, RWAs at -6500, -6500, -6500 rpm (X, Y, Z, respectively).

APPENDIX S

THE UNITRODE JANTXV2N3421 IN THE MARS OBSERVER RXO

I. Origin of Concern Over the Unitrode JANTXV2N3421 in the Mars Observer RXO

The Mars Observer RXO was supplied to Astro by FEI and the same or similar versions have been used by Astro in many spacecraft. Astro also frequently uses a function called Thermal Control Electronics (TCE) supplied by FEI. This function was not used in Mars Observer because Mars Observer does not use louvers.

In approximately May 1993 there was a failure of TCE SN 336. The TCE was returned to FEI for repair and it was determined by FEI that failure had occurred as the result of an open emitter in a Unitrode JANTXV2N3421 transistor. FEI noted that after removal from the TCE, the transistor no longer exhibited the open emitter condition. The TCE and the transistor were returned to Astro. No failure analysis of the transistor was done at that time.

On approximately July 1, 1993, there was a failure of RXO SN 204 in NOAA-I while on the launch pad at Vandenberg. Analysis traced the failure to be caused by an open emitter in a Unitrode JANTXV2N3421 transistor.

Within a week after the RXO failure, an intensive failure analysis activity was initiated by both GSFC and Astro. It was found that both the TCE and RXO transistor failures had come from lot date code 8350 and that transistors from that same lot had been used in FEI hardware supplied to Astro for use on several TIROS and DMSP spacecraft, as well as LANDSAT 6, GGS, and Mars Observer. Shortly thereafter, Hughes and Aerospace started additional investigations because FEI hardware with transistors from this same lot was being used on MILSTAR. At the time of the NOAA-I failure only three spacecraft had been launched with FEI hardware containing transistors from the 8350 lot. They were TIROS H, DMSP S12, and Mars Observer.

In approximately August 1993 another TCE failure was found by Astro. Analysis again traced the failure to be caused by a Unitrode JANTXV2N3421 from lot date code 8350. The defective transistor was again found to exhibit an intermittently open emitter as did the original failure.

From the work done by Astro, GSFC, Hughes and Aerospace there seems to be unanimity that the Unitrode JANTXV2N3421 transistors in lot date code 8350 were manufactured with an out-of-control welding process and that the parts were not suitable for use in critical spacecraft applications. The transistors from the suspect lot have by now been purged from critical applications in hardware that is still on the ground. That was clearly not an option available to Mars Observer.

II. Description of the Unitrode JANTXV2N3421

The JANTXV2N3421 is capable of a collector current of 3 A_{dc} and is designed to allow a relatively large power dissipation in a TO-5 can, although in the RXO applications none of these capabilities are challenged. The device uses a planar npn silicon chip which is eutectically attached to a Mo disc which is Ag brazed to a TO-5 Kovar header to make the collector connection. External base and emitter wires have glass to metal seals allowing them to pass through the header and act as posts for internal connections. The emitter and base are connected from the chip to their respective posts by 8-mil Al wire. The connections at the chip are made by *ultrasonically bonding* the Al wire to Al metallization patterns on the chip. The connections at the posts are made by *tweezer welding* the Al wire to the Au plated Kovar posts. A silicone encapsulant is then used to cover the chip, and packaging is completed by welding a Ni can to the Kovar header to form a hermetic enclosure.

III. Internal Wire Connections

The first internal connection is made by ultrasonically bonding an 8-mil Al wire to the chip. Wire is then spooled out beyond the location of the appropriate post and is cut. This step is performed for both the emitter and the base, and the device is passed on to another station for tweezer welding.

The tweezer welding device has opposed electrodes which are preloaded in the closed position. An operator causes the tweezer to open and maneuvers it so as to position the Al wire and the post between the halves of the tweezer. The tweezer is then closed, resulting in deformation of the Al wire and allowing electrical discharge between the tweezer elements through the wire/post and creates a weld. A final step is for the operator to manually break away the wire pig-tail that extends beyond the weld at the post.

The quality of a tweezer weld can be affected by the angle and amount of contact between a wire and post, which is very dependent on operator positioning of the tweezer. Small amounts of contamination can cause considerable variation of electrical resistance during welding and may result in welding only in very localized areas with large amounts of the deformed area unwelded. Tweezer welding in general is a difficult process to control and an out-of-control process can be somewhat masked by either accidentally or intentionally breaking off the pig-tail toward the post rather than away from it.¹

IV. Failure Mode and Mechanism

The mode of failure experienced in spacecraft hardware has consistently been an open or intermittently open transistor emitter. In each case the cause of the open or intermittence has been further traced to a tweezer weld at the emitter post.

¹ Private communication with George Harman of the National Institute of Standards and Technology, September 1993.

The laboratory work done by Astro and others clearly shows that transistor lot date code 8350 had a very wide dispersion in weld quality, as reflected by the results of pull tests. Some welds have proven to be quite strong and others have been quite weak. Unfortunately there is no nondestructive way to determine which transistors have welds in which category.

The wire bonds in the transistors from the suspect lot have a wide dispersion in their pull strength when destructively tested and may even be bimodally distributed. It is presumed that in use, those bonds which are physically the weakest at the outset will be prone to fail first. Failure of even a weak bond, however, must be induced by some mechanism.

One straightforward failure mechanism is related to mechanical perturbances that are of either thermal or mechanical origin. A structural analysis of the Unitrode JANTXV2N3421 transistor emitter wire has been performed considering both thermal distortion and shock response loading.² An MSC/Nastran finite-element model was constructed of one wire between the silicon die and Kovar post. Typical wire geometry was obtained by optical microscope. All major components were included (Kovar post, glass seal, Kovar header, molybdenum disk and silicon die). Only the wire and post were modeled elastically, however, all were capable of thermal expansion and assumed stress free at room temperature. The analysis results indicated that a wire-to-post bond force of 8–20 grams will be developed over a 100°C temperature change depending on the amount of prior strain hardening. An assumed shock level of 2000 g's, however, will produce only 0.2 grams of wire-to-post bond force due to the low mass of the wire. The amount of force required to fail welds has been stated to be highly variable and for a very bad weld, the force to cause failure could be infinitesimal (<<0.2 grams).

The weld joint can ultimately fail due to fatigue, which can be induced through either thermal cycling the transistor, or by self heating, which will occur through power on/off cycles. Either of these actions will cause stress in the wire and if done enough times will produce a fatigue failure. Fatigue failure can be modeled³ but in this case there was inadequate data available regarding the material properties to allow calculation.

A second possible failure mechanism is related to degradation which occurs as a function of time. It is well known that when a couple is formed between Au and Al, intermetallics will form and the intermetallics will occupy a volume that is larger than would have been required by the two individual materials involved. Also, Kirkendall voids will occur because of the relative rates at which the two metals diffuse into one another. Elzbietha Kolawa of JPL has calculated that over a period of 10 years (roughly the time since 8350) that an Au/Al couple at room temperature would have formed an

² P. Rapacz, *Unitrode JANTXV2N3421 Transistor Analysis*, JPL Interoffice Memorandum 3542-93-298, Jet Propulsion Laboratory, October 8, 1993.

³ S. Sutharshana, *Calculating the Probability of Transistor Weld Joint Failure During MOI*, JPL Interoffice Memorandum, Jet Propulsion Laboratory, Pasadena, California, October 21, 1993.

intermetallic layer slightly more than 0.26 μm thick. The intermetallic formation would potentially create substantial additional weakening of any bond that was initially weak from manufacturing. It is considered highly credible that tweezer welding may have produced a very weak weld containing a complex set of initial conditions within the weld joint materials and that subsequent intermetallic formation and/or some other mechanism may have been active in causing the weld to deteriorate with time. One such process which can lead to spontaneous bond failure has been proposed by E. Cuddihy of JPL.⁴

V. Use of the JANTXV2N3421 in the RXO

There are two JANTXV2N3421 transistors in each redundant half of the RXO (see Chapter V.D of this report for a complete description of the RXO). In each redundant half, one transistor is used in the power supply circuitry and the other transistor is used in the outer oven controller. Failure of either or both of the transistors used for outer oven control would not result in a failure that would be either sudden or catastrophic. Therefore, these transistors are declared not to be related to the Mars Observer anomaly. Failure of a transistor in the power supply circuitry results in loss of the RXO output on the side which corresponds to the failed transistor.

VI. Probability of Failure of a JANTXV2N3421 in the RXO

In Figure S-1, the RXO is depicted as 4 transistors with Q_1 and Q'_1 representing the ones in the power supplies and Q_2 and Q'_2 being the ones in the outer oven controllers. Therefore with respect to the Mars Observer anomaly, the failure states of Q_2 and Q'_2 are of no concern.

From telemetry data it is known that the power supply on the backup side was not failed at the start of the pressurization sequence or any prior time (this is not the same as saying that one knows that there was 5.12 MHz at the output of the backup side). It is also known that the RXO had been operating on the primary side since launch and therefore its power supply transistor had to be working and it is very likely that the oven controller transistor was also working. The failure state table in Figure S-1 is based on this information.

From data provided by Astro,⁵ there are several alternatives for selecting the fraction of bonds that are believed to be defective. The number used in Figure S-1, 2%, is based on the number of observed failures excluding screening rejects. From Figure S-1 it is seen that the probability of having one transistor failing during flight is $B = 0.04$. Since it is known that both critical transistors were working at the start of the pressurization sequence, the probability of failure of one transistor is still 0.04. The

⁴ *Modeling Tweezer Welds*, JPL Interoffice Memorandum EFC-514-C-89-93, Jet Propulsion Laboratory, Pasadena, California, October 26, 1993.

⁵ D. Bennett and K. Lackey, *Transistor Failure—JANTXV2N3421 Findings and Recommendations*, Martin Marietta Astro Space Interoffice Memorandum, July 22, 1993.

probability of both critical transistors failing is therefore $B^2 = 0.0016$. Hence, the probability that one of the critical transistors will be working⁶ through the pressurization sequence is $(1 - B^2) = 0.9984$.⁷

In Chapter VII.R and in Table 8-1 of this report, it is shown by analysis that failure of a single critical transistor in the RXO does not result in a scenario that matches the observables for the Mars Observer anomaly.

VII. Other Commentary

It is interesting to note that the Unitrode JANTXV2N3421 received approval in February 1984 to be used in the RXO for DMSP(S11-S14) because a 2N5154 was not available as a military grade device. In January 1986, the device was approved for use on TIROS based on heritage. In December 1987, it was approved for use on Mars Observer because of heritage use on TIROS and DMSP. In July 1993, it appears that only three spacecraft including Mars Observer had been launched.⁸ How much testing all of the other spacecraft had undergone while awaiting launch is unknown, but idle time in storage does not generate much of a heritage upon which future decisions should be based.

Acknowledgments

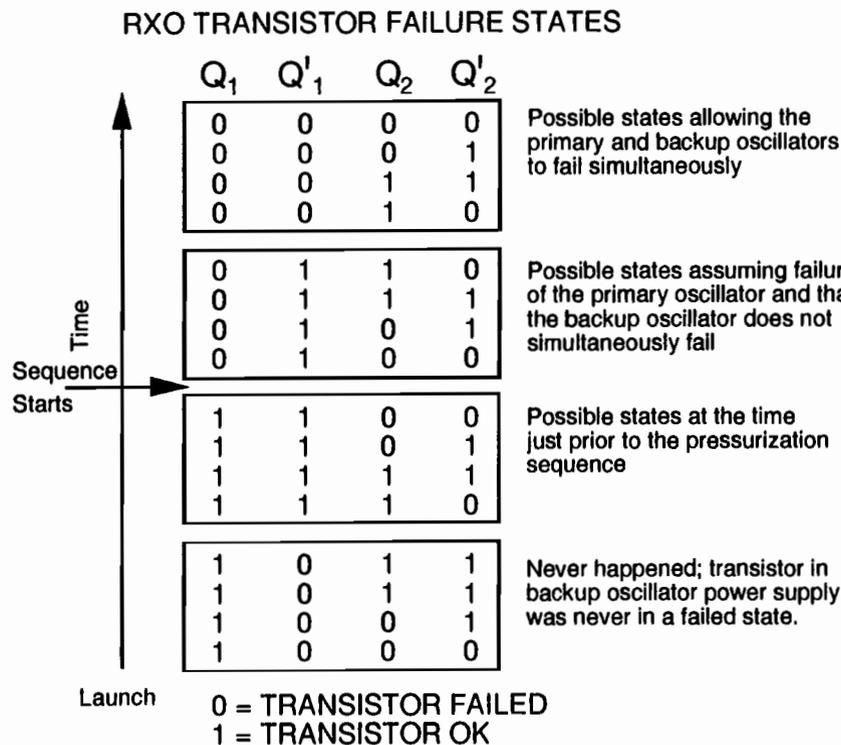
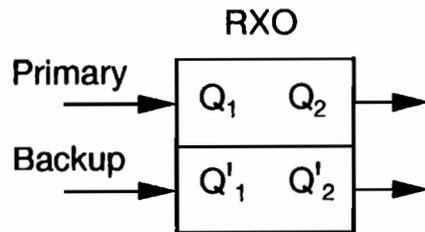
In preparation of this Appendix, the author has drawn extensively upon information obtained from the individuals and documents listed below and gratefully acknowledges the help which was derived from that body of work and those individuals. Attribution, however, has not been given on an item-by-item basis throughout this Appendix.

- (1) *GSFC Failure Analysis Report Serial No. 31929*, Goddard Spaceflight Center, Greenbelt, Maryland
- (2) D. Bennett and Ken Lackey, *Transistor Failure—JANTXV2N3421 Findings and Recommendations*, Martin Marietta Astro Space IOM, July 22, 1993
- (3) Tom Hoskinson, Don Schmunk, Gary Stupian, and Mel Cohen of The Aerospace Corporation
- (4) David Bennett of Astro
- (5) Chez DiGregorio of Hughes Aircraft Corporation

⁶ Ibid. Their calculation was made using an incorrect assumption that all of the RXO transistors are critical. A different value of $P = 0.09$ was also used. Using that value of P and performing the calculation correctly produces an answer of 0.9705.

⁷ This assumes that failure is not causally related to the pressurization sequence. If, for example, it is shown that firing of the pyro valves produces a very large shock pulse at a critical transistor, then a very weak bond might be caused to fail.

⁸ See Footnote 5.



P = Fraction of defective bonds

$1-P$ = Fraction of good bonds

$G = (1-P)^2$ = Probability of a part (2 bonds) being good

$B = 1-(1-P)^2$ = Probability of a part (2 bonds) being bad (at least one bad bond)

or

$B = 2P - P^2 \approx 2P$

Therefore, if from the Astro data one selects $P = 0.02$, then the probability of 1 transistor failing during flight is $B = 0.04$.

P	B	Represents
.02	.04	Unitrode (8350)
.002	.004	Poor Quality
.0002	.0004	Average Quality
.00002	.00004	Good Quality

Figure S-1. Probability of failure of a JANTXV2N3421 in the RXO.

APPENDIX T
PRESSURIZATION SEQUENCE

OWLT = 18:58
 (@ 233/100 18:57.624
 234/0100 18:58.357
 234/0900 18:59.085
 234/1100 18:59.809
 PAGE 38

 ** MARS **
 ** OBSERVER **

SEQUENCE OF EVENTS: YEAR-DAY OF YEAR --> 1993-234
 S/C = 094 INPUT FILE NAME --> t01.u.epef.4
 SEQ = T01 OUTPUT FILE NAME --> t01.u.4.1.soe

GENERATED ON DAY OF YEAR = 225
 August 13, 1993 17:41:09 UTC

ITEM NO	GROUND TIME DDD HH:MM:SS	T	ACTION	EVENT DESCRIPTION	DSN	COMMAND (*-RTC)	S/C EVENT TIME	TLM FMT
567	234 00:29:52	E		START DIGITAL TAPE RECORDER CONTROL BLOCK			234 00:10:54	
568	234 00:30:04	E		RECORD ---> ENGINEERING DATA FORMATTER (EDF1) DATA DIGITAL TAPE RECORDER 1 TRACK 1 - 2 KBPS		STDTRC	234 00:11:06	
				----- C-0016 DTR1_PWR_ON C-0015 DTR1_MTR_STP C-0017 DTR1_TAP_DIR C-0046 XSU_TLM_WORD C-0051 DTR1MODE C-0055 DTR1_CLK C-0066 DTR1_TRK C-0101 DTR1TAPE_SPD 0 0 RED: 0 0 IPS C-0501 DTR1_CURRENT 0 0 RED: 0 0 MAMPS -----				
569	234 00:34:59	E		ALL DSS: 5-MIN WARNING -- BIT RATE CHANGE	15			
570	234 00:34:59	E		ALL DSS: 5-MIN WARNING -- TLM OFF	15			
571	234 00:39:59	E		START PROPULSION SYSTEM PRESSURIZATION BLOCK "A"			234 00:21:01	
572	234 00:39:59	E		TURN OFF -> TRANSPONDER EXCITER TURN OFF -> RADIO FREQUENCY POWER AMPLIFIER BEAM		STRPAF	234 00:21:01	
				----- L-0008 MOT1_EXCITER L-0015 MOT2_EXCITER L-0601 MOT1EXC_RF_O 12 14 RED: 10 0 DBM L-0605 MOT2EXC_RF_O 12 14 RED: 10 0 DBM L-0023 TWT1_BEAM_ON L-0028 TWT2_BEAM_ON L-0504 RPA2HELX_CUR 0 0 RED: 0 0 MAMPS L-0505 RPA1_INP_BUS 0 0 RED: 0 0 AMPS L-0507 RPA2HELX_CUR 0 0 RED: 0 0 MAMPS L-0508 RPA2_INP_BUS 0 0 RED: 0 0 AMPS -----				
573	234 00:39:59	E		START PROPULSION SYSTEM PRESSURIZATION BLOCK "B"			234 00:21:01	
574	234 00:39:59	E					234 00:21:01	N/A_N/A_ENG
				S/C X-BAND TELEMETRY STATUS BIT RATE : 0 BPS TLM MOD INDEX : 44.8 CODING : CD SUBCARRIER : LOW TLM FMT : N/A_N/A_ENG				

PRP7PR-5^m5^s
 (OWLT = 18:58.35)

T-2

 ** MARS **
 ** OBSERVER **

SEQUENCE OF EVENTS: YEAR-DAY OF YEAR --> 1993-234
 S/C = 094 INPUT FILE NAME --> t01.u.epcf.4
 SEQ = T01.U.4.1 OUTPUT FILE NAME --> t01.u.4.1.soe

GENERATED ON DAY OF YEAR = 225 PAGE 39
 August 13, 1993 17:41:09 UTC

ITEM NO	GROUND TIME DDD HH:MM:SS	T B	ACTION	EVENT DESCRIPTION	DSN	COMMAND (*=RTC)	S/C EVENT TIME	TLM FMT
575	234 00:39:59	E		ISSUE S/C X-BAND TELEMETRY STATUS KEYWORD	15			
576	234 00:39:59	E		ALL DSS: BIT RATE CHANGE 0CD	15			
577	234 00:39:59	E		ALL DSS: WARNING -- TLM OFF	15			
578	234 00:40:01	E		S/C TRANSMITTER STATUS CHANGE RF PWR AMP : 2 EXCITER : 2 CARRIER : X-BAND POWER : OFF			234 00:21:03	
579	234 00:40:01	E		DSS-15: LOS - S/C TRANSMITTER TURNED OFF	15			
580	234 00:40:01	E		ISSUE S/C TRANSMITTER STATUS KEYWORD	15			
581	234 00:40:04	E		TURN OFF -> RADIO FREQUENCY POWER AMPLIFIER 1 FILAMENT L-0024 TWT1_FILA_ON L-0505 RPA1_INP_BUS 0 0 RED: 0 0 AMPS		TCR1FF	234 00:21:06	
582	234 00:40:04	E		TURN OFF -> RADIO FREQUENCY POWER AMPLIFIER 2 FILAMENT L-0029 TWT2_FILA_ON L-0508 RPA2_INP_BUS 0 0 RED: 0 0 AMPS		TCR2FF	234 00:21:06	
583	234 00:44:03	E		TURN ON --> SKEW REACTION WHEEL ASSEMBLY A-0504 SRWA_MTR_CUR 0 4.5 RED: 0 0 AMPS		ACRWSN	234 00:25:05	
584	234 00:44:04	E		SET -----> ATTITUDE/ARTICULATION CONTROL SUBSYS CONTROL STATE > SOLAR ARRAY/HIGH GAIN ANTENNA DEPLOY (SPIN UP REACTION WHEEL ASSY TO 200 RPM) F-0003 ATTSTATE F-2412 ***** F-2414 ***** F-2416 ***** F-2418 *****		SAGDPL	234 00:25:06	

T-3

 ** MARS **
 ** OBSERVER **

SEQUENCE OF EVENTS: YEAR-DAY OF YEAR --> 1993-234
 S/C = 094 INPUT FILE NAME --> t01.u.epef.4
 SEQ = T01 OUTPUT FILE NAME --> t01.u.4.1.soe

GENERATED ON DAY OF YEAR = 225 PAGE 40
 August 13, 1993 17:41:09 UTC

ITEM NO	GROUND TIME DDD HH:MM:SS	T	B	ACTION	EVENT DESCRIPTION	DSN	COMMAND (*-RTC)	S/C EVENT TIME	TLM FMT
585	234 00:44:54	E			ENABLE ---> EARLY CRUISE PYRO BUS A ----- P-1007 ECR PYRA_ENA -----		PYECAE	234 00:25:56	
586	234 00:44:54	E			ENABLE ---> EARLY CRUISE PYRO BUS B ----- P-1008 ECR PYRB_ENA -----		PYECBE	234 00:25:56	
587	234 00:44:55	E			ARM -----> EARLY CRUISE PYRO BUS A ----- P-1005 E/M PYRA_ARM -----		PYECAA	234 00:25:57	
588	234 00:44:55	E			ARM -----> EARLY CRUISE PYRO BUS B ----- P-1006 E/M PYRB_ARM -----		PYECBA	234 00:25:57	
589	234 00:45:04	E			FIRE -----> PYRO 7 VALVE PRIMARY SQUIB OPENS HI-PRESSURE GASEOUS HELIUM LINE OPENS HI-PRESSURE GASEOUS HELIUM LINE <i>to regulator and NTO tank</i>		PRP7PR	234 00:26:06	
590	234 00:49:25	E			ALL DSS: 5-MIN WARNING -- BIT RATE CHANGE	15			
591	234 00:50:04	E			FIRE -----> PYRO 5 VALVE PRIMARY SQUIB OPENS HI <i>Low</i> PRESSURE GASEOUS HELIUM LINE --> MONO-METHL HYDRAZINE TANK		PRP5PR	234 00:31:06	
592	234 00:50:11	E			ENTER -----> SUN-ACQUISITION/CONING ATTITUDE CONTROL STATE (STAR-FIX UPDATING ORIENTATION) ----- F-0003 ATTSTATE F-2412 ===== F-2414 ===== F-2416 ===== F-2418 =====		SAGSSI	234 00:31:13	
593	234 00:50:14	E			DISARM ---> EARLY CRUISE PYRO BUS A ----- P-1005 E/M PYRA_ARM -----		PYECAD	234 00:31:16	

T-4

5 m

added from a different script

 ** MARS **
 ** OBSERVER **

SEQUENCE OF EVENTS: YEAR-DAY OF YEAR --> 1993-234
 S/C = 094 INPUT FILE NAME --> t01.u.epef.4
 SEQ = T01 OUTPUT FILE NAME --> t01.u.4.1.sce

GENERATED ON DAY OF YEAR = 225 PAGE 41
 August 13, 1993 17:41:09 UTC

ITEM NO	GROUND TIME DDD HH:MM:SS	T B	ACTION	EVENT DESCRIPTION	DSN	COMMAND (* = RTC)	S/C EVENT TIME	TLM FMT
594	234 00:50:14	E		DISARM ---> EARLY CRUISE PYRO BUS B ----- P-1006 E/M PYRB_ARM -----		PYECBD	234 00:31:16	
595	234 00:50:15	E		DISABLE --> EARLY CRUISE PYRO BUS A ----- P-1007 ECR PYRA_ENA -----		PYECAX	234 00:31:17	
596	234 00:50:15	E		DISABLE --> EARLY CRUISE PYRO BUS B ----- P-1008 ECR PYRB_ENA -----		PYECBX	234 00:31:17	
597	234 00:50:16	E		SET -----> ATTITUDE/ARTICULATION CONTROL SUBSYS CONTROL STATE > ARRAY NORMAL SPIN ----- F-0003 ATTSTATE F-2412 ----- F-2414 ----- F-2416 ----- F-2418 ----- -----		SAGANS	234 00:31:18	
598	234 00:50:17	E		TURN ON --> TRANSPONDER EXCITER TURN ON --> RADIO FREQUENCY POWER AMPLIFIER BEAM ----- L-0008 MOT1_EXCITER L-0015 MOT2_EXCITER L-0601 MOT1EXC_RF_O 12 14 RED: 10 0 DBM L-0605 MOT2EXC_RF_O 12 14 RED: 10 0 DBM L-0023 TWT1_BEAM_ON L-0028 TWT2_BEAM_ON L-0504 RPA2HELX_CUR 0 0 RED: 0 0 MAMPS L-0505 RPA1_INP_BUS 0 0 RED: 0 0 AMPS L-0507 RPA2HELX_CUR 0 0 RED: 0 0 MAMPS L-0508 RPA2_INP_BUS 0 0 RED: 0 0 AMPS L-0024 TWT1_FILA_ON L-0029 TWT2_FILA_ON -----		STRPAN	234 00:31:19	

T-5

 ** MARS **
 ** OBSERVER **

SEQUENCE OF EVENTS: YEAR-DAY OF YEAR --> 1993-234
 S/C = 094 INPUT FILE NAME --> t01.u.epef.4
 SEQ = T01 OUTPUT FILE NAME --> t01.u.4.1.soe

GENERATED ON DAY OF YEAR = 225
 August 13, 1993 17:41:09 UTC

PAGE 42
*X should be
 00:35:27*

ITEM NO	GROUND TIME DDD HH:MM:SS	T B	ACTION	EVENT DESCRIPTION	DSN	COMMAND (* = RTC)	S/C EVENT TIME	TLM FMT
599	234 00:54:21	E		S/C TRANSMITTER STATUS CHANGE RF PWR AMP : 2 EXCITER : 2 CARRIER : X-BAND POWER : ON			234 00:35:23	
600	234 00:54:21	E		ISSUE S/C TRANSMITTER STATUS KEYWORD	15			
601	234 00:54:21	E		DSS-15: AOS - S/C TRANSMITTER TURNED ON	15			
602	234 00:54:22	E	TRK D15	DSS-15: ACQUIRE X-BAND D/L CHAN-16 RCVR BW=W12HZ TRK MODE=2-WAY	15			
603	234 00:54:25	E		S/C X-BAND TELEMETRY STATUS BIT RATE : 2000 BPS TLM MOD INDEX : 44.8 CODING : CD SUBCARRIER : LOW TLM FMT : N/A_N/A_ENG			234 00:35:27	N/A_N/A_ENG
604	234 00:54:25	E		ISSUE S/C X-BAND TELEMETRY STATUS KEYWORD	15			
605	234 00:54:25	E		ALL DSS: BIT RATE CHANGE 2000CD	15			
606	234 01:00:16	E		TURN OFF --> SKEW REACTION WHEEL ASSEMBLY ----- A-0504 SRWA_MTR_CUR 0 4.5 RED: 0 0 AMPS -----		ACRWSF	234 00:41:18	
607	234 01:00:17	E		TURN ON --> X Y & Z REACTION WHEELS ----- A-0504 SRWA_MTR_CUR 0 4.5 RED: 0 0 AMPS A-0505 XRWA_MTR_CUR 0 4.5 RED: 0 0 AMPS A-0506 YRWA_MTR_CUR 0 4.5 RED: 0 0 AMPS A-0507 ZRWA_MTR_CUR 0 4.5 RED: 0 0 AMPS -----		SRUXYZ	234 00:41:19	
608	234 01:00:18	E		END PROPULSION SYSTEM PRESSURIZATION BLOCK "A"			234 00:41:20	
609	234 01:09:59	E		START PROPULSION SYSTEM PRESSURIZATION BLOCK "C"			234 00:51:01	
610	234 01:30:00	E	TRK D45	BEGIN PRE-CALIBRATION PERIOD FOR DSS-45	45			
611	234 01:30:00	E		ISSUE S/C ANTENNA STATUS KEYWORD	45			
612	234 01:30:00	E		ISSUE S/C RECEIVER STATUS KEYWORD	45			

*should be
 00:54:25*

*PRP7PR
 + 9^m17^s
 (PRP5PR + 4^m17^s)*

T-6

APPENDIX U

MARS BALLOON RELAY BEACON DETECTION CAPABILITY

The Mars Observer spacecraft carries communication equipment to support data relay from a Mars Balloon mission planned for later this decade. That equipment includes a beacon on Mars Observer to initiate data transmission from the balloon near the Martian surface. It was proposed to command turn-on of the beacon transmitter and attempt detection of the signal at Earth. The results of this endeavor could possibly help resolve the credibility of some hypotheses about the loss of the X-band signal.

The Mars Balloon Relay (MBR) beacon transmits at 437.1 MHz with a power of 1.3 W. It utilizes a helical antenna pointed in the nadir direction, which provides a gain of +2.0 dBic with a broad toroidal-shaped pattern. The resulting EIRP is about +33.1 dBm, which would produce a received carrier flux at Earth of about 128 Jansky·Hz at Mars distance in late September 1993. That flux value is sufficient to allow real-time signal detection if sophisticated processing techniques are used.

An attempt to listen for the MBR beacon will require a carefully devised command strategy to assure activation of the MBR transmitter aboard Mars Observer. The command strategy must accommodate prevailing orbit uncertainties for Earth antenna pointing and transmitter frequency tuning. Command messages transmitted must also be compatible with the expected spacecraft state to ensure command decoding upon receipt.

At Earth, a receiving strategy involving three sites has been proposed. The sites are geographically diverse with different instrumentation employed at each. The three sites are: Jodrell Bank Radio Observatory, England; Goldstone Deep Space Communications Complex, California; and Stanford University, California. Key receiving parameters associated with each site are summarized in Table U-1.

Table U-1. MBR receiving station characteristics.

	Jodrell Bank	Goldstone	Stanford
Antenna diameter, m	76	70	46
Efficiency at 437.1 MHz	55%	40%	48%
System temperature, K	100	100	137
Search bandwidth, Hz	0.2	0.3	0.1-0.01
Signal-to-Noise ratio, dB	7.6	3.8	4.3-14.2

Complicating a search for the MBR is the potential of radio frequency interference (RFI) from terrestrial sources and uncertainty in drift rates for the MBR beacon oscillator. RFI can be discriminated by examining *frequency rate versus frequency* profiles for consistency with the dynamics of the Mars Observer orbit. Where RFI uncertainties

cannot be simply resolved, the receiving antenna may be articulated off-point momentarily to check if the signal is radiating from the direction of Mars. MBR oscillator drift uncertainties are simply accommodated by establishing search bandwidths consistent with the combination of the drift and orbit uncertainties.

Conservative estimates indicate the MBR beacon signal may be detected with probability greater than 90 percent if it is indeed present. An attempt in September 1993 had negative results, because the MBR transmitter was not properly commanded on at that time. Subsequent attempts to listen for the MBR must reassess detection probability for the solar system geometry prevailing at that time.