Report on the Loss of the Mars Polar Lander and Deep Space 2 Missions

JPL Special Review Board

22 March 2000

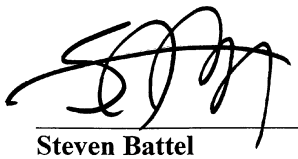
Jet Propulsion Laboratory
California Institute of Technology

JPL D-18709

REPORT ON THE LOSS OF MARS POLAR LANDER / DEEP SPACE 2
JPL SPECIAL REVIEW BOARD
— SIGNATURE PAGE —

Arden Albee

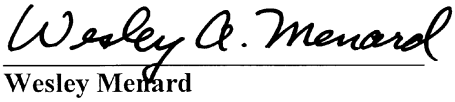
Charles Leising



Steven Battel

Duncan MacPherson

Richard Brace



Wesley Menard

Garry Burdick

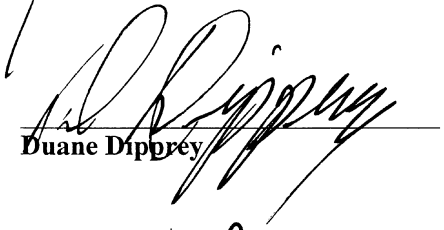
Richard Rose

Peter Burr

Robert Sackheim

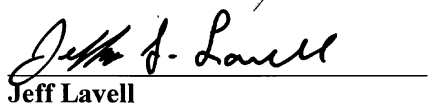
John Casani, *Chair*

Al Schallenmuller



Duane Dipprey

Charles Whetsel, Deputy Chair



Jeff Lavell

CONTENTS

List of Tables ..... *vii*

List of Figures ..... *vii*

Acronyms and Abbreviations ..... *viii*

EXECUTIVE SUMMARY ..... **xi**

1 INTRODUCTION **1**

1.1 Mars Surveyor Program **1**

1.2 Loss of the Mars Climate Orbiter Mission **1**

1.2.1 Investigation of the MCO Loss *1*

1.2.2 Post-MCO Corrective Actions for Mars Polar Lander *1*

1.3 Loss of Mars Polar Lander and Deep Space 2 Missions **2**

1.4 MPL Post-Landing Communication and Imaging Efforts **2**

1.5 Investigation of the MPL/DS2 Loss **3**

2 MISSION DESCRIPTIONS **4**

2.1 Mars Polar Lander **4**

2.2 Deep Space 2 ..... **4**

3 FINDINGS AND RECOMMENDATIONS **6**

3.1 Project Implementation **6**

3.1.1 MPL Findings *6*

3.1.2 Recommendations *7*

3.2 Review Process **8**

3.2.1 MPL Findings *8*

3.2.2 Recommendations *8*

3.3 Design Process **9**

3.3.1 MPL Findings *9*

3.3.2 DS2 Findings *10*

3.3.3 Recommendations *10*

3.4 Verification and Validation Process **10**

3.4.1 MPL Findings *10*

3.4.2 DS2 Findings *11*

3.4.3 Recommendations *11*

3.5 Other **12**

3.5.1 Findings *12*

3.5.2 Recommendation *12*

4 SPECIFIC RECOMMENDATIONS FOR THE MARS 2001 LANDER **13**

5 MPL SYSTEM-LEVEL ASSESSMENT 15

5.1 Project vs. Program Decisions 15

5.1.1 No Telemetry for Entry, Descent, and Landing 15

5.1.2 Launch Vehicle 15

5.2 Design Robustness 16

5.2.1 Findings and Assessment 16

5.2.2 Lessons Learned 17

5.3 System Verification and Validation 17

5.3.1 Findings and Assessment 19

5.3.2 Lessons Learned 19

6 SUMMARY OF POTENTIAL FAILURE MODES 20

6.1 Plausible Failure Modes 20

6.1.1 MPL 20

6.1.2 DS2 21

6.2 Failure Mode Assessments 21

6.2.1 Failure Modes Affecting the Lander and Both Probes 23

6.2.2 Failure Modes Affecting Only the Lander 24

6.2.3 Failure Modes Common to EDL Phases 29

7 MPL DISCIPLINE AREA ASSESSMENTS 31

7.1 MPL Environment and Landing Site 31

7.1.1 Delivery Corridor to Landing Site Errors (Due to Entry Flight Path, Cross-Track, or Center of Mass) 32

7.1.2 Heatshield Design or Physical Flaw 41

7.1.3 MPL Landing Site Unsurvivable 42

7.1.4 MPL Backshell/Parachute Recontacts or Drapes Over Lander After Touchdown 43

7.2 MPL Mechanical Systems 45

7.2.1 Lander/Aeroshell Fails to Separate from Cruise Stage 45

7.2.2 Center-of-Mass Migration Due to Mechanical Shifting 46

7.2.3 Parachute Fails to Deploy and Inflate 47

7.2.4 Heatshield Fails to Separate from Backshell 48

7.2.5 Legs Fail to Deploy 50

7.2.6 Lander Fails to Separate from Backshell 51

7.2.7 Propulsion Dynamics Interaction with Structure 53

7.2.8 Landed Solar Array Fails to Deploy 54

7.2.9 MGA Fails to Deploy 55

7.3 MPL Dynamics and Control 57

7.3.1 Radar Data Lockout 57

7.3.2 Radar–Terrain Interaction 58

7.3.3 Inertial Measurement Unit (IMU) Performance 59

7.3.4 Model Fidelity 60

7.3.5 Unstable Limit-Cycle Behavior During Terminal Descent 61

7.3.6 Fuel Slosh 62

7.3.7 Center-of-Mass Migration/Uncertainty 62

7.3.8 Adverse Flexible Body Interaction with Terminal Descent Controller 64

7.3.9 Zero Velocity Singularity *64*
7.3.10 Minimum Thrust Margin *65*
7.3.11 Radar–Heatshield Lockup *65*
7.4 MPL Communications/Command and Data Handling **67**
7.4.1 C&DH Reset During EDL *67*
7.4.2 EEPROM Errors After Landing *68*
7.4.3 CMIC Errors After Landing *69*
7.4.4 Power Controller Unit Fails *70*
7.4.5 Landed Orientation Prevents Communication *71*
7.4.6 Coaxial Transfer Switch Fails *73*
7.4.7 Failure to Establish UHF Link Between the Lander and Mars Global Surveyor *74*
7.4.8 Transponder Power Supply Fails *75*
7.4.9 Medium-Gain Antenna Gimbal Fails *76*
7.4.10 Command Detector Unit Fails *77*
7.4.11 Diplexer Fails *77*
7.4.12 Telemetry Modulation Unit Fails *78*
7.4.13 Solid-State Power Amplifier Fails *78*
7.4.14 Uplink/Downlink Card Fails *78*
7.5 MPL Propulsion and Thermal **81**
7.5.1 Introduction *81*
7.5.2 RCS Propulsion Component Fails Prior to Terminal Descent *82*
7.5.3 Larger Than Allowable Propellant Center-of-Mass Offset *82*
7.5.4 Larger Than Allowable Propellant Migration During "Zero G" Cruise Prior to Hypersonic Entry *86*
7.5.5 Larger Than Allowable Propellant Migration During Hypersonic Entry *88*
7.5.6 Augmented Propellant Migration During Parachute Operation *88*
7.5.7 Larger Than Allowable Center-of-Mass Shift During Powered Descent *89*
7.5.8 Inadequate Thermal Control of Propulsion Subsystem *90*
7.5.9 Propulsion Component Fails During Terminal Descent (Other Than Caused By Water Hammer Effects) *91*
7.5.10 Terminal Descent Propulsion Component Fails During Terminal Descent (Caused By Water Hammer Effects) *92*
7.5.11 Adverse Plume Interactions During Terminal Descent and Touchdown *94*
7.5.12 Other Issues *94*
7.5.13 Conclusions *95*
7.6 MPL Avionics **98**
7.7 MPL Flight Software/Sequencing **111**
7.7.1 Uplink Loss Timer Software Error *111*
7.7.2 Premature Descent Engine Shutdown *114*
8 SUMMARY OF POTENTIAL DS2 FAILURE MODES **124**
8.1 DS2 Failure Mode Assessments **126**
8.1.1 Failure Modes Affecting Both Probes *126*
8.1.2 Failure Modes Affecting a Single Probe *128*
9 DS2 DISCIPLINE AREA ASSESSMENTS **129**
9.1 DS2 Environment and Impact Site **129**

9.1.1 DS2 Environment and Delivery Corridor *129*
9.1.2 DS2 Landing Site Unsurvivable *129*
9.2 DS2 Mechanical Systems **131**
9.2.1 DS2 Premature Separation *131*
9.2.2 DS2 Fails to Separate from Cruise Stage Due to Failure of Cruise Stage Separation from Aeroshell/Lander *132*
9.2.3 DS2 Fails to Separate After Cruise Stage/Aeroshell Separation *133*
9.2.4 DS2 Aeroshell Failure/Fracture at Entry Max-G *133*
9.2.5 DS2 Structural Failure at Impact *134*
9.2.6 DS2 Telecom Subsystem Fails at Impact *136*
9.3 DS2 Avionics **138**
9.4 DS2 Communications **142**
9.4.1 UHF Link Fails *142*

TABLES

Table 5-1. Mars ’98 MPL System-Level Verification and Validation Program Activities 18
Table 6-1. Failure Assessment Criteria 20
Table 6-2. MPL Potential Failure Modes Classified by Plausibility 21
Table 7-1. Mechanisms for Propellant Center-of-Mass Offset 84

FIGURES

Figure 6-1. MPL Entry, Descent, and Landing (EDL) Sequence with Potential Failure Modes 22
Figure 7-1. Site Selection Ellipse — Based on LMA Scatter for 75° S, Rotated for 76° S Landing Site 35
Figure 7-2. TCM-4 Planning Ellipse — LaRC 3DOF Scatter, 11/23/99 37
Figure 7-3. Required Maneuver-Execution Errors, LaRC 6DOF 3/3/00 (Yellow [Light]), and TCM-4 Planning Ellipse, LaRC 3DOF 11/23/99 (Green [Dark]) 38
Figure 7-4. Required Maneuver Execution Errors, LaRC 6DOF 3/3/00 (Yellow [Light]), and Final Estimated Ellipse, LaRC 6DOF 3/3/00 (Green [Dark]) 39
Figure 7-5. Earth Geometry for the Nominal Landing Orientation and Site on Sol 0 72
Figure 7-6. Command-Blind Zones in Azimuth for MGA (125 bps) and LGA (7.8125 bps) 72
Figure 7-7. MPL Propulsion Subsystem Schematic 83
Figure 7-8. Touchdown Monitor Functional Flow Diagram 115
Figure 7-9. MPL System Mapping Requirements to Flight Software Requirements 120
Figure 8-1. DS2 Entry, Descent, and Impact (EDI) Sequence with Potential Failure Modes 125

APPENDICES

Appendix 1. *Bibliography* 144
Appendix 2. *Review Team Members* 153

Acronyms and Abbreviations

AACS	Attitude and Articulation Control Subsystem
ACD	adiabatic compression decomposition
ACS	Attitude Control System
ASIC	application-specific integrated circuit
ATLO	assembly, test, and launch operations
ATP	acceptance test procedure
AXAF	Advanced X-ray Astrophysics Facility (Chandra X-ray Observatory)
BER	bit-error rate
BIT	built-in test
bps	bits per second
BPSK	bi-phase shift key
BTTS	basic time transmission sequence
C	Celsius
C&DH	command and data handling
CARES	Ceramics Analysis and Reliability Evaluation of Structures
CCU	Charge Control Unit
CDR	Critical Design Review
CDU	Command Detector Unit
CE	Cincinnati Electronics
CFD	computer fluid dynamics
CMIC	C&DH Module Interface Card
CNES	Centre National d'Etudes Spatiales
CPU	central processing unit
CPV	common pressure vessel
CRC	cyclic redundancy check
CTE	coefficient of thermal expansion
DET	direct energy transfer
DGB	disk-gap-band (parachute)
DOF	degrees of freedom
DOY	day of year
DRAM	dynamic random-access memory
DS2	Deep Space 2
DSN	Deep Space Network
DST	Deep Space Transponder
DTE	direct to Earth
E_b/N_0	ratio of energy-per-bit to noise power spectral density
EDAC	error detection and correction
EDI	entry, descent, and impact (DS2)
EDL	entry, descent, and landing (MPL)
EDU	engineering development unit
EEPROM	electrically erasable programmable read-only memory
EMC	electromagnetic compatibility
EMI	electromagnetic interference
EPS	Electrical Power System
ESD	electrostatic discharge
FEM	finite-element model
FMEA	failure modes and effects analysis
FMECA	failure modes and effects criticality analysis (or assessment)
FPGA	field-programmable gate array
FSK	frequency shift key
FSW	flight software
FTA	fault-tree analysis
FTE	Find the Earth (sequence)

g	acceleration of gravity
G&C	guidance and control
G&H	(Manufacturer's name for release nut)
GOES	Geostationary Operational Environmental Satellite
GPMC	Governing Program Management Council
GPS	Global Positioning System
Gr/E	graphite epoxy
GSE	ground support equipment
GSFC	NASA Goddard Space Flight Center
HGA	high-gain antenna
HKPS	housekeeping power supply
IMU	Inertial Measurement Unit
I/O	input/output
IPV	independent pressure vessel
ISA	Incident/Surprise/Anomaly
IUS	Inertial Upper Stage
JPL	Jet Propulsion Laboratory
kohm	kilohm (1000 ohms)
ksi	kilo-pounds per square inch
LaRC	NASA Langley Research Center
lbf	pounds-force
LET	linear energy transfer
LGA	low-gain antenna
LMA	Lockheed Martin Astronautics
LPIU	Lander Pyro Initiation Unit
MAD	Motor Articulation Drive
MARDI	Mars Descent Imager
MARS	Martin Anomaly Reporting System (LMA P/FR system)
Mbit	megabit
MCO	Mars Climate Orbiter
MFB	multifunction bus
MGA	medium-gain antenna
MGS	Mars Global Surveyor
MIMU	Miniature Inertial Measurement Unit
MOC	Mars Orbiter Camera (MGS)
MOLA	Mars Orbiter Laser Altimeter (MGS)
MOSFET	metal-oxide semiconductor field-effect transistor
MPIAT	Mars Program Independent Assessment Team
MPL	Mars Polar Lander
MR	Mars Relay (MGS)
MSFC	NASA Marshall Space Flight Center
MSP	Mars Surveyor Program
MUX	multiplexer
MVACS	Mars Volatiles and Climate Surveyor (MPL)
N	newton
NASA	National Aeronautics and Space Administration
NSI	NASA Standard Initiator
P/FR	Problem/Failure Report
PAL	programmable array logic
PCU	Power Controller Unit
PDDU	Power Distribution and Drive Unit
PDR	Preliminary Design Review
PICA	phenolic impregnated carbon ablators
PIM	Pyrotechnic Initiator Module
PIU	Pyrotechnic Initiation Unit

POR	power-on reset
psi	pounds per square inch
PVDM	Propulsion Valve Drive Module
PWM	pulse-width modulation
R/T	receive/transmit
RAD	rocket-assisted descent (Mars Pathfinder)
RC	resistor–capacitor (time constant)
RC1, 2, 3	request command (Mars Relay subcarrier tone modes)
RCS	Reaction Control System
REM	Rocket (Reaction) Engine Module
RFA	Request for Action
rms	root mean square
RVA	redundancy verification analysis
S/N	serial number
SAM	site adjust maneuver
SCR	silicon controlled rectifier
SCT	spacecraft team
SDST	Small Deep Space Transponder
SEE	single-event effect
SEU	single-event upset
SFP	system fault protection
SMO	Systems Management Office
SRAM	static random-access memory
SRS	Software Requirements Specification
SSPA	solid-state power amplifier
STL	Spacecraft (System) Test Laboratory (LMA)
STS	Space Transportation System
T/R	transmit/receive
TAG	Technical Advisor Group (LMA)
TAG	two-axis gimbal
TC	telemetry command (Mars Relay subcarrier tone mode)
TCM	trajectory correction maneuver
TDL	tunable diode laser
TES	Thermal Emission Spectrometer (MGS)
TMU	Telemetry Modulation Unit
TPS	thermal protection system
ULDL	Uplink/Downlink (Card)
USO	Ultra-Stable Oscillator
VHDL	Very High Speed Integrated Circuit Hardware Description Language

EXECUTIVE SUMMARY

Mars Polar Lander (MPL) and the two Deep Space 2 (DS2) probes were launched using a single launch vehicle from Kennedy Space Center on 3 January 1999. Upon arrival at Mars, communications ended according to plan as the three spacecraft prepared to enter the Martian atmosphere. Communications were scheduled to resume after the lander and the probes were on the surface. Repeated efforts to contact all three continued for several weeks to no avail.

On 16 December 1999, in accordance with Jet Propulsion Laboratory (JPL) policy, the Laboratory Deputy Director appointed a Special Review Board (the Board) to examine the loss of MPL and DS2. The Board included members from JPL, industry, and academia, as follows:

Arden Albee — Caltech
Steven Battel — Battel Engineering
Richard Brace — JPL
Garry Burdick — JPL
Peter Burr — GSFC, ret
John Casani, *Chair* — JPL
Duane Dipprey — JPL, ret.
Jeffrey Lavell — NASA Independent Program Assessment Office
Charles Leising — JPL
Duncan MacPherson — JPL
Wesley Menard — JPL
Richard Rose —TRW, ret.
Robert Sackheim — MSFC
Al Schallenmuller — LMA, ret.
Charles Whetsel, *Deputy Chair* — JPL

Two consultants, Frank Locatell (JPL, ret.) and Parker Stafford (LMA, ret.), who had been closely associated with the MPL development process, were engaged to assist the Board in its investigation. Bruce Murray (Caltech) was assigned by NASA to keep the Administrator informed of the Board's activities and progress.

The Board was tasked to:

1) Determine the possible root causes for the loss of the two missions.
2) Identify actions needed to assure future success in similar Mars landings.

Given the total absence of telemetry data and no response to any of the attempted recovery actions, it was not expected that a probable cause, or causes, of failure could be determined.

In fact, the probable cause of the loss of MPL has been traced to premature shutdown of the descent engines, resulting from a vulnerability of the software to transient signals. Owing to the lack of data, other potential failure modes cannot positively be ruled out. Nonetheless, the Board judges there to be little doubt about the probable cause of loss of the mission.

In contrast, the Board has been unable to identify a probable cause of the loss of DS2. The loss of both probes can be accounted for by a number of possibilities. The Board identified four plausible failure modes.

With regard to task 1) above, discussions of all the potential failure modes that the Board identified are found in Sections 6 and 8 of this report for MPL and DS2, respectively. Each potential failure mode is briefly described and the plausibility of each assessed. The plausibility assessment is not intended to imply probability of occurrence. Each potential failure mode is assessed as plausible unless it is counterindicated by design and test or by operation during the mission.

With regard to task 2) above, the Board found several design weaknesses, any of which could have resulted in loss of the mission. The Board has findings and recommendations in specific areas related to the potential failure modes that are applicable to all missions in general. These are discussed in Section 3. The major areas are Project Implementation, Review Process, Design Process, and Verification and Validation Process.

Section 4 contains recommendations specific to the Mars ’01 Lander. Foremost among these is a recommendation to add telemetry coverage for the entry, descent, and landing (EDL) phase of the mission. The recommendations cover hardware, software, test, and analysis.

The DS2 mission was designed to validate 10 advanced, high risk, high-payoff technologies. As originally approved, the development plan included a system-level qualification test that was ultimately deleted. This represented an acknowledged risk to the program that was assessed and approved by JPL and NASA management on the basis of cost and schedule considerations and best use of available resources. The absence of a system-level, high-impact qualification test compromised the ground validation of the targeted technologies, and the loss of both probes precluded flight validation.

Both the MPL and DS2 projects made noteworthy efforts to reduce the cost of implementing flight projects in response to severe and unprecedented technical and fiscal constraints. Although the MPL and DS2 missions were lost, there are valuable lessons to be learned from both, which this report attempts to set forth.

One lesson that should *not* be learned is to reject out of hand all the management and implementation approaches used by these projects to operate within constraints that, in hindsight, were not realistic. A more appropriate point of departure would be to evaluate the approaches, and improve, modify, or augment them in response to implementing the Recommendations contained herein.

1 INTRODUCTION

1.1 Mars Surveyor Program

NASA's Mars Surveyor Program (MSP) began in 1994 with plans to send spacecraft to Mars every 26 months. Mars Global Surveyor (MGS), a global mapping mission, was launched in 1996 and is currently orbiting Mars. Mars Surveyor '98 consisted of Mars Climate Orbiter (MCO) and Mars Polar Lander (MPL). Lockheed Martin Astronautics (LMA) was the prime contractor for Mars Surveyor '98. The Jet Propulsion Laboratory (JPL), California Institute of Technology, manages the Mars Surveyor Program for NASA's Office of Space Science.

MPL was developed under very tight funding constraints. The combined development cost of MPL and MCO, including the cost of the two launch vehicles, was approximately the same as the development cost of the Mars Pathfinder mission, including the cost of its single launch vehicle. The MPL project accepted the challenge to develop effective implementation methodologies consistent with programmatic requirements.

1.2 Loss of the Mars Climate Orbiter Mission

MCO was launched on 11 December 1998 for arrival at Mars on 23 September 1999. MCO was designed to operate in a polar orbit for up to five years to study the weather and serve as a telecommunications relay link for MPL and other missions. Five minutes into Mars Orbit Insertion, MCO was occulted by Mars and contact was never reestablished.

1.2.1 Investigation of the MCO Loss

To investigate the loss, JPL appointed an internal JPL team (the MCO Peer Review Team) and a Special Review Board. The team and the Special Review Board determined that the mission loss occurred when the spacecraft entered the Martian atmosphere. The report of the Special Review Board on the loss of MCO (document JPL D-18441, 11 November 1999) included findings and recommendations in 13 areas. Some of the recommendations in 12 of those areas were identified as relevant to MPL as well as MCO.

1.2.2 Post-MCO Corrective Actions for Mars Polar Lander

In the wake of the loss of the MCO mission, measures were taken by the Laboratory, both within and external to the MPL project, to incorporate findings from the various review boards as they related to the success of the MPL mission.

One of the activities involved the creation of an MPL Mission Safety and Success Team (MSST), comprising over 50 senior JPL technical experts. This team was responsible for the creation of a fault-tree analysis for EDL, including safe transition into landed operations, and for assessment of the mitigation of each identified failure mode based on review of development design packages, the test program, and expert interviews with members of the MPL development and operations teams.

While the probable cause of the loss of MPL (premature trigger of touchdown sensor) was identified as a potential failure mode by this fault-tree analysis prior to EDL, the description of the software design and testing provided at that time by LMA did not leave any concerns in the mind of the MSST.

Ultimately, it was discovered that the software did not behave in the manner intended (see Section 7.7.2). The MSST final report was published as JPL IOM 3130-CWW-001, dated 1 December 1999.

Another activity undertaken by JPL was the creation of a "Red Team," which was charged with tracking all work items underway between the loss of MCO and MPL EDL, as well as reviewing and assessing the completeness of closure for all recommendations relating to MPL following the MCO failure, and reviewing the work of the MSST. The Red Team's final report was presented on 23 November 1999.

1.3 Loss of Mars Polar Lander and Deep Space 2 Missions

MPL, with the two DS2 probes, was launched on 3 January 1999 for arrival at Mars on 3 December 1999. All three were mounted to a shared cruise stage, which provided Earth communications, power, and propulsion support services for the trip to Mars. All were targeted to a sector at approximately 76° S, 195° W on the edge of the Martian south polar layered terrain. The length of the planned MPL mission after landing was 90 days; the DS2 mission was two days. The probes were to be released from the cruise stage after lander–cruise stage separation, plummeting to the surface to impact about 60 kilometers from the MPL landing site.

MPL approached Mars on 3 December 1999, in apparent good health. A final trajectory-correction maneuver, TCM-5, was executed 6.5 hours before entry. At 12:02 p.m. PST, the spacecraft slewed to entry attitude. At this attitude, the antenna pointed off-Earth, and the signal was lost as expected. Lander touchdown was expected to occur at 12:14 p.m. PST, with a 45-minute data transmission to Earth scheduled to begin 24 minutes later. It was expected that the first data from the DS2 probes would be received on 4 December at 7:25 p.m. PST, about 7 hours after MPL touchdown. However, no communications from MPL or the probes were received.

1.4 MPL Post-Landing Communication and Imaging Efforts

Attempts to communicate with MPL continued until mid-January without success. On 17 January 2000, the flight team announced that the effort to recover the spacecraft had concluded. However, in late January and the first two weeks of February, mission managers sent more commands to MPL. These attempts to contact the lander were based on a report from Stanford University that a faint signal had been detected during processing of data recorded earlier. These data were collected during communications attempts on 18 December and 4 January when Stanford was using its 45-meter antenna to try to pick up the lander's UHF signal. Radio telescopes in the United Kingdom, the Netherlands, Italy, and at Stanford continued to listen for a possible signal, with negative results. Subsequent analysis of the data has determined that the signal was generated from within the Stanford University receiver itself and was not from MPL.

High-resolution (1.5 meters per pixel) photography of the MPL landing site area began on 16 December 1999 and continued through January 2000 using the Mars Orbiter Camera (MOC) on board MGS, in hopes of imaging the lander or parachute. Data from the Mars Orbiter Laser Altimeter (MOLA) and the Thermal Emission Spectrometer (TES) aboard MGS were evaluated to better characterize the MPL and DS2 landing sites. The MOC scans covered more than 300 square kilometers of south polar terrain, including the vast majority of the expected landing area. A 1.5-meters-per-pixel view is the highest spatial resolution achievable by MOC. At this resolution, the lander would be perhaps one or two pixels in size. The white parachute, if lying flat, would measure about 6 meters, covering perhaps three or four pixels in a MOC image. Locating the lander or the

parachute would require distinguishing a few pixels among nearly 150 million pixels in a MOC image. In spite of the efforts of three independent organizations, no conclusive evidence for the presence of the lander or parachute was seen in detailed analyses of the images.

1.5 Investigation of the MPL/DS2 Loss

The JPL Special Review Board and its consultants identified a number of failure scenarios, which for convenience were organized by mission phase. The failure scenarios for MPL are presented in Section 6 and those for DS2 are presented in Section 8.

The Board organized itself into seven Review Teams, in the areas of Environment and Landing Site, Mechanical Systems, Dynamics and Control, Communications/Command and Data Handling, Propulsion and Thermal, Avionics, and Flight Software/Sequencing. Each Review Team provided an assessment in their respective areas related to the design and test practices relevant to the hypothesized failures. The Review Teams' Findings, Process Assessments, and Lessons Learned are presented in Section 7 for MPL and Section 9 for DS2.

The Review Teams conducted their investigations through meetings and teleconferences with Mars Surveyor '98 personnel from LMA and JPL, and DS2 project personnel, throughout January and February 2000. Plenary sessions of the Board were held through the first part of March, during which the Board determined its Findings and Recommendations (see Sections 3 and 4) and the system-level Findings, Assessments, and Lessons Learned (see Section 5).

Note — This report reflects units of measure as used by the MPL and DS2 projects.

2 MISSION DESCRIPTIONS

2.1 Mars Polar Lander

MPL and MCO were part of the JPL Mars ’98 Development Project, which turned over responsibility for operations to the Mars Surveyor Operations Project (MSOP) at launch. As a part of MSOP, LMA performed spacecraft operation functions from their facility in Denver, Colorado, for MCO and MPL, as they have been doing for MGS and Stardust. Science data were to be delivered to the experiment Principal Investigators (PIs) at their home institutions, with the PIs able to send commands to their instruments on a daily basis.

MPL was launched on 3 January 1999 from Cape Canaveral Air Station on a Delta II–7425 launch vehicle with two liquid-fuel stages plus four solid-fuel boosters, and a third-stage Thiokol Star 48B solid-fuel booster. After an 11-month cruise, the spacecraft arrived at Mars on 3 December 1999, targeted for a landing zone near the edge of the south polar layered terrain. The lander was encased in an aerodynamic entry body consisting of a forward heatshield and a backshell (aft heatshield), which separated from the cruise stage about 5 minutes before atmospheric entry. The subsequent EDL sequence — with parachute deployment, heatshield jettison, lander leg deployments, Radar ground acquisition, separation of backshell with parachute from the lander, and powered descent to the surface — lasted about 5.5 minutes.

MPL was designed to study volatiles and climate history during its 90-day mission. The lander carried three science investigations: the Mars Volatiles and Climate Surveyor (MVACS), the Mars Descent Imager (MARDI), and a Russian-provided Lidar instrument. A small microphone, provided by The Planetary Society, was also on board. MVACS was an integrated instrument package designed to study the surface environment, weather, and geology at the landing site. The package included a surface stereo imager on a 1.5-meter mast; a 2-meter, jointed robotic arm with a digging scoop, camera, and temperature probe; a meteorology package; and a thermal and evolved gas analyzer to heat soil samples and determine concentrations of volatiles. MARDI was scheduled to take pictures during the lander’s descent to the surface, beginning with heatshield jettison at about 8 kilometers altitude. The Lidar instrument’s purpose was to characterize ice and dust hazes in the lower part of the atmosphere.

MPL was designed to send its data to MCO for relay to Earth, a plan eliminated by the loss of MCO on 23 September 1999. However, the lander had the ability for direct-to-Earth communication using its X-band radio and medium-gain antenna (MGA) at 12,600 bits per second (bps) using the Deep Space Network’s 70-meter antennas, or at 2100 bps using the DSN 34-meter antennas. It could also relay data through MGS at 128,000 bps.

2.2 Deep Space 2

The DS2 project was part of NASA’s New Millennium Program, whose purpose is to flight-test new technologies and demonstrate innovative approaches for future missions. DS2’s challenge was to demonstrate that miniaturized components could be delivered to the surface of another planet and conduct science experiments. The mission consisted of two “microprobes” (generally referred to as “probes” in this report), each encased in its own aeroshell attached to the MPL spacecraft cruise stage.

About 5 minutes before MPL entered the upper atmosphere, the lander entry body and cruise stage were to have separated. This separation was to have initiated mechanical pyro devices that separated

the DS2 aeroshells about 18 seconds later. The aeroshells were designed to fall to the surface, shattering on impact and releasing their probes. The probes would then penetrate the surface by as much as a meter, first separating into two parts at impact — an aft-body (which would stay at the surface) and a penetrator (which would come to rest below the surface) — connected with a flexible cable. The probes were expected to strike the surface with an impact velocity of about 200 meters per second. The aft-body was designed to withstand a peak rigid body shock of about 60,000 g's; the penetrator, a shock of about 30,000 g's. The aft-body could operate in temperatures from 0 to –80 degrees C; the penetrator could operate in temperatures as low as –120 degrees C.

Micro-instruments in the penetrator were designed to perform sample collection with a miniature drill, move about 100 milligrams of soil into a cup, heat the sample, and attempt to detect water vapor using a tunable diode laser assembly. Also encased in the penetrator were a power micro-electronics unit, an advanced micro-controller, and sensors to measure soil conductivity. Data from the penetrator were to be transmitted via the flexible connecting cable to a micro-telecommunications system in the aft-body and then transmitted to MGS. The data were to be buffered in the MGS camera's memory and then transmitted to Earth. The nominal DS2 mission was two days; low-temperature lithium batteries mounted in the aft-body were to provide power resources for about one to three days for each probe.

3 FINDINGS AND RECOMMENDATIONS

3.1 Project Implementation

3.1.1 MPL Findings

From the beginning, the MPL project was under considerable funding and schedule pressure. The project team was asked to deliver a lander to the surface of Mars for approximately one-half the cost of Mars Pathfinder, which had been done for significantly less than earlier planetary missions. In addition, the complexity and technical challenges for MPL were at least as great, if not greater. The important consequences of this technical and financial situation fell chiefly into two categories — project staffing and key technical decisions.

3.1.1.1 Project Staffing

In order to meet the challenges, the Laboratory decided to manage the project with a small JPL team and to rely heavily on LMA's management and engineering structure. Consequently, there was essentially no JPL line management involvement or visibility into the project. This was a departure from previous project management approaches at the Laboratory, but was accepted as necessary in order to proceed within the cost constraint.

LMA first- and second-level technical managers provided day-to-day technical oversight of the project. The JPL project team, consisting of approximately 10 technical and management people, provided higher-level oversight and was supplemented with part-time consultants and JPL discipline experts selected by the project. The result was minimal involvement by JPL technical experts.

LMA used excessive overtime in order to complete the work on schedule and within the available workforce. Records show that much of the development staff worked 60 hours per week, and a few worked 80 hours per week, for extended periods of time. Another consequence of the tight funding constraint was that many key technical areas were staffed by a single individual. Although none of these individuals were lost to the project during its development, the effect of inadequate peer interaction was, in retrospect, a major problem. It is the Board's assessment that these conditions led to a breakdown in inter-group communications, and there was insufficient time to reflect on what may be the unintended consequences of day-to-day decisions. In short, there was insufficient time and workforce available to provide the levels of checks and balances normally found in JPL projects.

3.1.1.2 Key Technical Decisions

The Mars '98 project made key decisions early in the formulation phase, as required in any cost-constrained project. However, some of these key decisions ultimately required more development effort than originally foreseen. In the opinion of the Board, this occurred partly as a result of insufficient systems engineering during the formulation phase.

The project also adopted a number of operating mandates in order to cope with the severely tight funding and schedule constraints. These mandates were:

- Use off-the-shelf hardware components and inherited designs to the maximum extent possible.
- Use analysis and modeling as an acceptable lower-cost approach to system test and validation.
- Limit changes to those required to correct known problems; resist changes that do not manifestly contribute to mission success.

On the whole, this philosophy was sound, with design and trade choices based on a reasonable balance between technology, cost, and schedule. However, even in a highly cost-constrained environment, great care must be taken in the cost–risk tradeoff. In retrospect, the Board found that a few choices (as enumerated below) resulted in unanticipated design complexity or other unanticipated consequences.

1. The decision to use pulse-mode control for the descent engines avoided the cost and cost risk of developing and qualifying a throttle valve in exchange for a somewhat more difficult terminal descent guidance system algorithm. This introduced other risks in the propulsion, mechanical, and control areas. Although the risks in the mechanical and thruster areas were dealt with satisfactorily, the risks in the dynamics and control area were not completely retired and should have been more fully addressed through analysis and test.

2. The lander configuration required at least two canted engines in each of three locations for stability and control. The project elected to use four smaller off-the-shelf engines at each location.

3. The decision to use analysis and modeling instead of testing, when possible, was an effective cost-reduction strategy; however, there were some cases where the project depended on models not thoroughly validated. Examples are:
   — Radar–terrain interaction
   — Dynamical control effects of pulse-mode propulsion

4. The decision not to have EDL telemetry was a defensible project decision, but an indefensible programmatic one. (See Section 5.1.1.)

5. The decision to forgo downlink through the omni antenna made the X-band downlink dependent upon the MGA being pointed accurately at Earth. This reduced the ability to get health and safety engineering data in an anomalous landed configuration.

3.1.2 Recommendations

R1) For highly cost- and schedule-constrained projects, it is mandatory that sufficient systems engineering and technical expertise and the use of the institution's processes and infrastructure be applied early in the formulation phase to ensure sound decision making in baseline design selection and risk identification.

R2) Do not permit important activities to be implemented by a single individual without appropriate peer interaction; peers working together are the first and best line of defense against errors. Require adequate engineering staffing to ensure that no one individual is single string; that is, make sure that projects are staffed in such a way as to provide appropriate checks and balances.

R3) Establish standards for JPL technical involvement and line management oversight for all ongoing and future projects. The standard should be clearly delineated and the Governing Program Management Council (GPMC) should review all projects for compliance before authorization to proceed.

R4) Revise institutional policies and procedures as necessary to preclude personnel working excessive overtime (paid or unpaid); e.g., greater than 60 hours per week for more than eight weeks without senior line management approval. Criteria should be expanded to include technical performance and hardware safety in addition to employee well-being.

R5) Similarly, projects must limit use of excess contractor overtime unless approved by senior contractor management and the JPL project manager.

3.2 Review Process

3.2.1 MPL Findings

The project did not have a documented review plan, but did hold many reviews, both formal and informal. Subsystem Preliminary and Critical Design Reviews (PDRs and CDRs) were conducted in a manner that reduced the level of formality and streamlined the review process, while still attempting to involve the appropriate depth and breadth of technical oversight. This approach made it possible for the project to conduct the appropriate number of reviews, which for the most part were thorough and well documented. Concerns and requests for actions were generated at these reviews. Project management had a mission assurance person track all review actions and see that written closures were obtained and closure approved at the usual levels.

Most of the subsystem PDRs and CDRs included in-depth "table-top" or "shirt-sleeve" penetration by technical experts, but some did not. True peer reviews that focused on specific problems or critical functions were conducted in some areas. The hinge deployment damper MGS-heritage review, the G&H release nut issue, and the Deployments Independent Review are a few examples. Technical experts from JPL and elsewhere participated in these reviews.

In the case of the Propulsion Subsystem, the thermal control design interfaces were not mature enough to evaluate at the CDR. A delta review should have been held but was not. Such a review could have discovered the problems experienced in flight.

The subsystem PDRs and CDRs themselves were adequate in identifying most of the technical issues contained in this report. Although all actions and recommendations were closed out formally prior to launch, these closures were usually approved by the project based on LMA closures without any independent technical support (by reviewers or otherwise). There was no substantive technical assessment of the closures in many areas; the JPL technical support was minimal, and LMA did not have their closures reviewed by Board members or non-project LMA personnel.

The Board has reviewed the closure of some action items related to the potential failures, and found that while the appropriate concerns were raised in the reviews, the actions taken by the project did not adequately address the concerns in all cases. This limitation on technical penetration of the action items and their closure is not typical of JPL projects and was probably an unintended consequence of project funding limitations.

Rather than following the typical process of choosing board chairpersons with technical expertise in functional areas from outside the project, the Flight System Manager was the chairperson of all the subsystem reviews. This approach may have contributed to the limited technical penetration on some of the action item closures.

3.2.2 Recommendations

R6) Projects should follow the institutional requirements to develop a documented review plan during project formulation. This project review plan should address how formal and informal reviews will be used to ensure adequate assessment of all project designs.

R7) The institutional review process should require that the response of projects to concerns and requests for actions raised at the review be fed back to the initiator. This will allow the initiator to assess whether the response by the project actually and adequately responds to the original concern. This is not meant to imply that the initiator can veto or override a project decision, but it does provide the opportunity and the responsibility of raising technical concerns through the appropriate management channels.

R8) Require non-project technical discipline persons to chair subsystem PDRs and CDRs.

R9) If, in the assessment of the review board, the objectives of a design review are not met, the review board should indicate in its recommendations whether a delta review, or other follow-up action, is warranted.

R10) Program-level decisions and requirements must be recognized as such, and accounted for in the requirements and system design of each of the program's constituent projects.

3.3 Design Process

3.3.1 MPL Findings

The systems engineering resources were insufficient to meet the needs of the project. For example, full evaluation of system interaction between propulsion, thermal, and control was incomplete. Fault-tree analysis was treated inconsistently. The thermal and software system design activities lagged behind the design of other subsystems requiring these inputs. In some cases, consideration of potential failure modes was not adequately assessed.

Precision navigation requirements were incompatible with spacecraft design, which could have been, but were not, adequately accounted for in mission operations. Specifically, the small forces generated by the spacecraft could not be modeled to the accuracy required by the navigation plan.

Certain MPL mission phases and sequences provide coverage only for parameter dispersions that conservatively represent stochastic dispersions, but unnecessarily fail to acceptably handle anomalously large parameter dispersions created by unmodeled errors or other non-stochastic sources. A notable example is EDL Sequence Implementation; i.e., the sequence design was not tolerant to anomalous conditions, and there was no functional backup to key go–no go event triggers.

Many of the technical concerns discussed in Sections 7 and 9 stem from the use of design practices not well suited to this mission. Specific examples of design weaknesses were found in the following areas:

- Propulsion system thermal control
- Control of propellant migration
- Processor tolerance to resets during critical events
- Control system stability margin verification
- Software object initialization

As a result, the system exhibited several areas of vulnerability, all of which compromised the robustness of the system design.

3.3.2 DS2 Findings

The system design for the probes did not permit functional testing after aeroshell integration; therefore, verification of probe status after each of the following critical mission phases was precluded:

- Final assembly
- System-level environmental tests
- Cruise stage integration
- Launch vehicle integration
- Launch environment
- Pre cruise stage separation

This design approach may be appropriate for a validated design that is deployed in quantity, but it is inappropriate for a technology demonstration mission.

3.3.3 Recommendations

R11) Establish a standard for appropriate levels of systems engineering throughout the formulation and implementation phases of projects.

R12) Ensure compatibility between navigation plan and spacecraft design through appropriate navigation engineering presence during the formulation and implementation phases.

R13) System design should ensure continuation of critical activities or sequences in the presence of anomalous conditions.

R14) Review contractor engineering practices and determine whether they are in conformance with accepted JPL principles.

R15) Establish, track, and verify design margins throughout development and operation.

R16) Provide electrical test access for pre-launch and in-flight verification purposes for all spacecraft.

R17) Require JPL and contractor line management to be accountable for the quality of the product design and conformance to institutional standards.

3.4 Verification and Validation Process

3.4.1 MPL Findings

In general, the verification and validation process for MPL was well planned and executed except as noted in Section 5.3. Most verification and validation deficiencies were in the final three EDL phases — parachute, terminal descent, and touchdown. This is not surprising since these are the most difficult areas to test or otherwise validate from a system perspective. In particular, many of the findings are related to the propulsion system, which employed analysis as a substitute for test in the verification and validation of total system performance. Therefore, the end-to-end validation of the system through simulation and other analyses was potentially compromised in some areas when the tests employed to develop or validate the constituent models were not of an adequate fidelity level to ensure system robustness.

The flight software was not subjected to complete fault-injection testing. Problems with post-landing fault-response algorithms (see Section 7.7) were uncovered in the course of the investigation.

The touchdown sensing software was not tested with the lander in the flight configuration. Because of this, the software error was not discovered during the verification and validation program (see Section 7.7.2).

The propulsion/thermal design was inadequately characterized in system thermal–vacuum test due to insufficient instrumentation, an error in the thermal model, and poor communication between the propulsion and thermal groups. Consequently, major errors in the propulsion thermal design went undetected until after launch. One error had to do with the catalyst bed heaters, and was handled satisfactorily prior to entry. Another led to the concern over uneven propellant drain from the tanks during descent (see Section 7.5.8).

3.4.2 DS2 Findings

Due to lack of a suitable air gun, a complete system-level impact test of the probe with aeroshell was not conducted. This prevented full characterization of the dynamic interaction between the aeroshell and the probe. The Board believes that there was a risk of structural failure due to the dynamic interaction between the aeroshell and the probe.

There was no impact test of an electrically powered, complete system. Such a test was planned but was deleted midway through the project, based on schedule considerations and a determination that the test article could be put to better use in a non-destructive test. This issue was fully aired at the project Risk Assessment Review in June 1998. The decision to delete the test was concurred in by senior JPL and NASA Headquarters management.

The antenna was analyzed but not tested in the 6-torr Mars environment. The failure to test the antenna in a simulated Martian environment may have overlooked the possibility that the RF subsystem link margin might be compromised due to ionization breakdown at the antenna.

The flight battery lot was not subjected to impact tests. Testing was performed on eight cells from a predecessor flight-like lot, with one structural but non-catastrophic failure. Therefore, the statistical certainty of the battery impact test program is considered inadequate to ensure flight battery impact survival.

3.4.3 Recommendations

R18) The Laboratory needs to reinforce the system-level test principle of “test as you fly, and fly as you test.” Departures from this principle must be carefully assessed and, if they are determined to be necessary, alternate measures, such as independent validation, should be incorporated. Such items must be reflected in the project risk management plan, communicated to senior management for concurrence, and reported at reviews.

R19) Assemble at least one flight-quality probe and subject it to a powered-on, system-level qualification test program.

R20) The structural/dynamic interactions between the aeroshell and the probe at impact should be characterized completely to reduce risk for future missions of this type, either by sufficient analysis or

a test. Since testing may involve development of a suitable air gun, a cost–benefit trade should be revisited in light of possible future mission uses.

R21) System software testing must include stress testing and fault injection in a suitable simulation environment to determine the limits of capability and search for hidden flaws.

3.5 Other

3.5.1 Findings

Findings related to more detailed design and process issues are contained in Sections 5, 7, and 9. These sections also include relevant Process Assessments and Lessons Learned.

3.5.2 Recommendation

R22) Each of the Lessons Learned contained in Sections 5, 7, and 9 require follow-up action. Most of them should be incorporated into appropriate institutional management or engineering practices. Each should be included in a Corrective Action Notice (this is not meant to imply necessarily one Corrective Action Notice for each Lesson Learned) to ensure tracking and proper closure.

4 SPECIFIC RECOMMENDATIONS FOR THE MARS 2001 LANDER

The recommendations in this section represent the Board's consensus on actions that could be taken to enhance the probability of success of the Mars '01 Lander. They are specific to the existing '01 configuration and would not necessarily apply to different lander designs. The recommendations derive from findings that could have led to problems for MPL. If the Mars '01 project chooses to respond to these recommendations, it well may be that alternate implementations could adequately address the concerns on which these recommendations are based.

The Board does not intend to convey that strict implementation of these recommendations will guarantee success for the '01 mission. Therefore, the Mars '01 project should continue its systematic search for additional actions that could be taken to enhance the probability of mission success.

The recommendations for the Mars '01 Lander are:

- Communications
  - Add EDL communications.
  - Add low-gain transmit antenna.
  - Perform an ionization breakdown test of the medium-gain and UHF antennas in a landed 6-torr environment.
  - Conduct an end-to-end UHF verification test between the lander and both the '01 and MGS orbiter configurations.

- Propulsion and Thermal
  - Ensure that tank outlet and line temperatures are maintained well above the freezing point of hydrazine.
  - Ensure acceptable operating temperatures for the thruster inlet manifolds and catalyst beds.
  - Ensure that propellant valve temperatures are monitored during flight.
  - Limit propellant migration between tanks to acceptable levels during all mission phases.
  - Perform a high-fidelity, closed-loop dynamic propulsion test with at least three live engines and flight-like plumbing support structure.
  - Evaluate the water hammer effect on the thrusters, structures, and controls due to 100-percent duty cycle thrusters.
  - Conduct plume–soil interaction analysis or test.

- Software
  - Ensure compliance with existing flight software review and test procedures.
  - Fix known software problems — e.g., landing leg touchdown false indication; singularity at zero descent velocity (gravity turn orientation); Radar data lockout; parachute deployment trigger algorithm (count up as well as count down); parachute separation algorithm (whether parachute or thrusters provide more deceleration); ground-detection algorithm (possible false detection of heatshield).
  - Fix and validate post-landing fault-recovery algorithm and sequences.

- Structures and Mechanisms
  - Validate center-of-mass properties of lander.
  - Stiffen support structure for propulsion feed lines.
  - Perform heatshield ATLO system first-motion separation test.

- Controls
  - Ensure through analysis, simulation, and testing that the control system has adequate authority and stability margins.

- Operations
  - Resolve small-forces discrepancies.
  - Improve TCM-5 flexibility for improved landing site control.

- Miscellaneous
  - Modify Radar to reduce sensitivity to slopes.
  - Review key triggers in EDL sequence to improve robustness.
  - Perform an analysis to determine that the probability of the parachute draping over the lander is acceptably low.

5 MPL System-Level Assessment

Observations or assessments relating to more than one area, or relating to the system development as a whole, are discussed in this section. Observations, assessments, and Lessons Learned relating to specific technical discipline areas are detailed in Section 7.

5.1 Project vs. Program Decisions

5.1.1 No Telemetry for Entry, Descent, and Landing

The project understood from the outset that in order to manage within the established cost constraints, clear project decision-making criteria would need to be established and rigorously followed. One of the criteria was that no resources would be expended on efforts that did not directly contribute to landing safely on the surface of Mars. On that basis, the project decided not to provide EDL telemetry. Senior Headquarters and Laboratory management concurred in this decision.

5.1.1.1 Findings and Assessment

The omission of EDL telemetry was justifiable from a project perspective. However, the loss of MPL without yielding any clues as to the cause of the loss jeopardized the potential for success of future Mars landers. Therefore, the decision was not justifiable in the context of MPL as one element of the ongoing Mars exploration program.

5.1.1.2 Lessons Learned

The requirements and goals established for each individual project within a program should not be permitted to disadvantage future projects without careful consideration by the program authority. Program requirements not clearly delineated at the project outset must be funded or established requirements on the project must be descoped accordingly.

5.1.2 Launch Vehicle

A program-level decision was made early in the project to fly on a launch vehicle that could provide a 565-kilogram injection capability to Mars. In comparison, the launch vehicle capability for Mars Pathfinder was 950 kilograms.

5.1.2.1 Findings and Assessment

At PDR, the resulting MPL mass margin was only 15 percent for the chosen launch vehicle, with significant mass liens yet to retire. Given the state of maturity at that point, a prudent mass margin should have been at least 25 percent.

The program–project decision to proceed beyond PDR with 15-percent mass margin and significant liens put the development effort in an unquantified state of risk, principally diverting engineering and management attention to intensive mass reduction and mass management activities at the expense of risk reduction activities.

5.1.2.2 Lessons Learned

Program decisions affecting project resources should be revisited if needed in the course of project development to assess whether evolving circumstances, including the engineering and science instrument developments, are forcing the project into an unacceptable risk posture.

5.2 Design Robustness

Three recurring themes encountered by the Board in the course of this investigation can be grouped under the heading of Design Robustness. These three themes are discussed below:

- System Fault Analysis — gaining an early understanding of the most significant risks to mission success.
- Fault Tolerance — the ability of the system to press on in the presence of off-nominal circumstances.
- Margin Characterization — gaining an understanding of how much room for error exists between the in-spec performance level and the levels at which the system fails to function.

5.2.1 Findings and Assessment

5.2.1.1 System Fault Analysis

Most of the design and review work associated with any project is focused on how the system is expected to work under nominal or moderately off-nominal conditions. It is also very important to consider how the system fails, or what conditions beyond the design cases can cause the system to not meet expected performance.

The best possible method to ensure that failures cannot occur in a given mission is to methodically identify all known failure modes and take the appropriate steps to prevent them. Such steps might include design changes, testing to gain confidence that such failures are unlikely, or operational procedures to avoid such failure modes.

Interface FMECAs and RVAs were performed for the engineering elements. A fault-tree analysis (FTA) was conducted by the project before launch for specific mechanisms and deployment systems where redundancy was not practical. No system-level FTA was formally conducted or documented.

The greatest value of system-level FTAs is to identify, from a top-down perspective, critical areas where redundancy (physical or functional) or additional fault protection is warranted. The NASA Administrator recently refocused attention on this method via his request for all projects to perform this type of analysis during the project's early stages (refer to "NASA Health and Safety Topic #11" of 20 January 2000).

An FTA can be performed earlier than, and is complementary to, analyses such as a system-level FMECA, which was performed for MPL. The use of deductive, top-down analyses such as FTA provides a valuable insight into the system, which can sometimes be lost in the details when using an inductive, bottom-up technique such as FMECA.

5.2.1.2 Fault Tolerance

The use of single-string operation during the relatively short EDL sequence can be justified based on simplicity and the associated advantages. However, there are examples where a single fault or off-nominal condition could cause the loss of the mission. In some cases, modest modifications would have enabled the system to degrade gracefully and continue on in the presence of such faults. The absence of functionally redundant sequence triggers to fail-safe against hardware or software failures for each sub-phase of EDL is one such example. Most EDL sub-phases have only one transition criterion, the absence of which prevents continuation of the EDL sequence.

The touchdown sensor check was enabled as soon as the Radar was powered off, enabling engine shutdown at 40 meters altitude. A more robust logic strategy would have enhanced the probability of survival in the presence of a premature touchdown sensor signal.

Similarly, it appears that there are some conditions under which the lander might have been able to physically land with a failure in one of the 12 terminal descent engines. The software implementation of the pulse-width control algorithm, based on the average required thrust duration ±10 milliseconds, made this more difficult, if not impossible.

A flaw in the Radar data acceptance algorithm would have forced the system to attempt to land without Radar data in the event of some invalid miscompares between the Radar measured velocity and the velocity propagated/integrated from the pre-entry state. It is extremely unlikely that MPL could land successfully without the use of Radar data.

The absence of a low-gain transmit antenna is another example of a lack of robustness in the design. Although the UHF system provides some measure of increased robustness in this area, other operational limitations make it less useful than a direct-to-Earth wide-beam link.

5.2.1.3 Margin Characterization

There were several effects that could contribute to erosion of the terminal descent control system margins. Items such as propulsion system dynamics (impulse variations due to water hammer or thermal effects), propellant center-of-mass migration, the lack of a high-fidelity fuel slosh model, and nonlinear pulse-width modulation effects, are all examples of effects that could contribute to the erosion of margins. The true margins of the system were not fully characterized in the presence of these effects.

There were also several effects that eroded propulsion system thermal margins (see Section 7.5.8).

5.2.2 Lessons Learned

A system-level FTA or a similar method should be employed to uncover fundamental failure modes and strategies for mitigation as an element of the systems engineering process. As the design evolves, the FTA should be updated and the results summarized at each major project review.

Project systems engineering personnel should be responsible for conducting FTAs, rather than personnel external to the project, since they are the most knowledgeable in the design of the mission elements. Advantage should be taken of the Systems Management Office (SMO), which has been given responsibility for facilitating these analyses.

Projects that adopt a single-string operational approach for critical events should do so with special attention to functional redundancy and algorithmic robustness.

When using simulations for system-level verification, validated (e.g., supported by test) models must be used, and sufficient parametric variations in the simulations must be performed to ensure that adequate margins exist.

5.3 System Verification and Validation

The Board conducted an assessment of the system-level verification and validation program for MPL. The purpose of this assessment is to judge the adequacy of the pre-launch development program, with

emphasis on functions related to EDL. This assessment does not include post-launch analysis and testing.

Table 5-1 lists all the functions that would comprise a prudent system-level verification and validation program related to EDL by mission phase. The column labeled *Qual. Method* indicates how each function was verified, i.e., by Test, Similarity (Simil.), or Analysis (Anal.). The *Adequacy Assessment* column provides a top-level evaluation of the verification and validation activity. "Yes" indicates that the validation was acceptable in all respects. Normally a project would expect to launch with all rows "Yes." "No" represents deficiencies in the verification and validation of the function. These assessments are not necessarily related to the MPL potential failure modes. The rightmost column contains references to the sections of the report that include a more complete assessment of the verification and validation approach.

The method of verification and validation for any given program is dependent on the degree of inheritance of the system hardware and its intended application in the specific mission. Depending on the circumstances, qualification by analysis may be entirely sufficient. The *Adequacy Assessment* rating provides a judgment of whether the verification and validation method used was both adequate for this program and implemented effectively. For example, the rating for the Touchdown Sensing System Qualification is rated "No," since the validation of the function was inadequate to reveal the system response to a spurious touchdown indication at leg deployment.

Table 5-1. Mars '98 MPL System-Level Verification and Validation Program Activities

EDL Mission Phase	Function	Qual. Method	Adequacy Assessment	Reference
Launch	Random Vibration	Test	Yes	Note 1
	Sine Vibration	None	Yes	Note 1
	Acoustic	Test	Yes	Note 1
	Launch Vehicle Matchmate	Test	Yes	Note 2
Cruise	DSN Compatibility	Test	Yes	Note 3
	Star Camera Stray Light/ Field-of-View	Anal.	No	7.3.3
	Mass Properties Control	Anal.	No	7.5.3, 7.5.4
	Thermal Vacuum (Propulsion Thermal Control)	Test	No	7.5.8
Pre-Entry	Cruise Stage Separation	Test	Yes	7.2.1, 7.6
	Power Profile	Test	Yes	7.6
	Connector Separation	Test	Yes	7.2.1
	DS2 Probe Separation	Test	Yes	9.2.3
Hypersonic	Heatshield Qualification	Simil.	Yes	7.1.2
	Aerothermal Performance	Anal.	Yes	7.1.2
	Aerodynamic Performance	Anal.	Yes	7.1.2
	Center-of-Mass Control	Anal.	Yes	7.5.5
Parachute	Parachute Qualification	Simil.	Yes	7.2.3
	Aerodynamics	Anal.	Yes	7.2.3
	Center-of-Mass Control	Anal.	No	7.5.6
	Deployment Dynamics (Snatch)	Test	Yes	7.2.3
	Separation Nut Qualification	Test	Yes	7.2.4, 7.2.6
	Heatshield Separation	Anal.	No	7.2.4, 7.6

EDL Mission Phase	Function	Qual. Method	Adequacy Assessment	Reference
Parachute (cont'd.)	Leg Deployment Qualification	Test	Yes	7.2.5, 7.6
	Radar Performance	Test	Yes	7.6
	Radar False Data Rejection	Test	No	7.3.1, 7.3.11
	Propulsion Pyro Devices	Test	Yes	7.5.2, 7.6
	Backshell Separation	Test	Yes	7.2.6
Terminal Descent	Terminal Descent Thruster Qualification	Test	Yes	7.5.9, 7.5.10
	Center-of-Mass Control	Anal.	No	7.5.6, 7.5.7
	Propulsion Thermal Control	Anal.	No	7.5.8
	Propulsion Water Hammer	Test	Yes	7.5.10
	Plume Interaction	None	No	7.5.11
	Control Stability	Anal.	No	7.3.4 through 7.3.8, 7.3.10
	Radar Doppler–Terrain Interaction	Test	No	7.3.2
Touchdown	Leg Qualification	Test	Yes	7.2.5
	Lander Drop Qualification	Test	Yes	7.2.5
	Touchdown Stability	Anal.	Yes	7.2.5, 7.1.3
	Touchdown Sensing System	Test	No	7.7.2
Post-Landing	Solar Panel Deployment	Test	Yes	7.2.8
	MVACS Deployment	Test	N.A.	Note 4
	Antenna Deployment	Test	Yes	7.2.9
	Thermal–Pressure	Test	Yes	7.6
	Ionization Breakdown	Anal.	No	7.6
	UHF Link	Test	Yes	7.4.7
	X-Band Landed Fault Protection	Test	No	7.7.1

Note 1 – Although a sine vibration test has been used in the past to dynamically qualify spacecraft systems, today it is generally agreed that random vibration and acoustic tests provide a more representative dynamic environment.

Note 2 – Quasi-static separation tests were performed at LMA using the flight cruise stage and the launch vehicle system adapter. Fit checks at the separation plane were conducted both with and without push-off springs installed. Pyro firing of the separation band was not conducted because the separation band, its pyrotechnics, and the firing system are part of the launch vehicle system.

Note 3 – DSN compatibility was successfully conducted using the Compatibility Test Trailer.

Note 4 – MVACS deployments were not assessed by the Board. While these might have interfered with the deployment of the MGA, this would not explain the absence of subsequent UHF contacts.

5.3.1 Findings and Assessment

The findings and assessment for the functions rated as non-adequate are discussed in Section 3.4.1 or in the cited reference in Table 5-1.

5.3.2 Lessons Learned

Lessons learned for the verification and validation program are incorporated in the recommendations in Section 3.4.3 and the Lessons Learned in Sections 7 and 9.

6 SUMMARY OF POTENTIAL FAILURE MODES

This section provides synopses of the potential failure modes considered and assessed by the Board. Subsection 6.1 identifies the plausible failure modes for MPL and DS2. Each potential failure mode is briefly summarized in subsections 6.2 (MPL) and 8.1 (DS2). The plausibility of each failure mode is assessed as:

Plausible — meaning that the failure mode cannot be excluded based on the design/test evaluation or available data.

Plausible but Unsupported — meaning that, while the failure mode cannot be ruled out, it is counterindicated by the data reviewed in the course of this investigation.

Implausible — meaning that the failure mode cannot reasonably be hypothesized.

The plausibility assessment is not intended to imply probability of occurrence. Rather, it is a subjective attempt to connect the postulated failure modes with the robustness of their relevant design and test efforts and evidence of operability.

Table 6-1 depicts the methodology the Board used to assess each identified failure mode. The information used to make these determinations was collected through interviews and reviews of project documentation.

Table 6-1. Failure Assessment Criteria

Verification	Design/Test "Robust" Assessment	Design/Test "Fragile" Assessment
Function Verified During Cruise	*Implausible*	*Plausible But Unsupported*
Function Not Verified During Cruise	*Plausible But Unsupported*	*Plausible*

6.1 Plausible Failure Modes

6.1.1 MPL

The following failure modes were assessed as plausible by the Board:

- Premature shutdown of descent engines. (See Section 6.2.2, *FLAG E*)
- Surface conditions exceed landing design capabilities. (See Section 6.2.1, *FLAG A*)
- Loss of control due to dynamic effects. (See Section 6.2.2, *FLAG C*)
- Landing site not survivable. (See Section 6.2.2, *FLAG F*)
- Backshell/parachute contacts lander. (See Section 6.2.2, *FLAG G*)
- Loss of control due to center-of-mass offset. (See Section 6.2.2, *FLAG D*)
- Heatshield fails due to micrometeoroid impact. (See Section 6.2.2, *FLAG B*)

The Board found compelling evidence that premature shutdown of the descent engines was the cause of the loss of MPL (see Section 6.2.2, *FLAG E*). It is important to note that there are no corroborating flight data to support this finding, so other failure modes cannot be ruled out.

6.1.2 DS2

Unlike the case with MPL, there was no one failure mode that was identified as being most probable. However**,** there were four failure modes that were determined to be plausible and they are listed below. Refer to Section 8 for a more detailed treatment of the DS2 failure modes.

- Both probes bounce on impact due to unanticipated surface effects. (See Section 8.1.1, *FLAG 1*)
- Both probes suffer electronic or battery failure at impact (See Section 8.1.1, *FLAG 2*)
- Probes fail due to ionization breakdown in Mars atmosphere. (See Section 8.1.1, *FLAG 3*)
- Probe lands on its side, interfering with antenna performance. (See Section 8.1.2, *FLAG 4*)

6.2 Failure Mode Assessments

This subsection summarizes the potential failure modes considered by the Board. Subsection 6.2.1 deals with failure modes affecting the lander and both DS2 probes; subsection 6.2.2 addresses failure modes affecting only the lander during EDL. The MPL failure mode descriptions in subsection 6.2.2 are shown by EDL phase: Entry, Parachute Phase, Terminal Descent, and Touchdown. Failure modes that could have occurred Post-Landing are also shown. Subsection 6.2.3 summarizes failure modes that were considered to be common across EDL phases. Failure modes specific to DS2 are presented in a separate part of the report (Section 8), with technical details in Section 9.

Section 7 of the report is organized by technical discipline, with the MPL failure modes described in greater detail. (Section 7 also addresses failure modes that affect both MPL and DS2.) In the summaries in subsections 6.2.1 through 6.2.3, the appropriate references to Section 7 are included in the assessment for each failure mode. (If the failure mode was considered implausible, there may be no such reference.)

Table 6-2 lists potential MPL failure modes by mission phase, classified by category of plausibility.

Table 6-2. MPL Potential Failure Modes Classified by Plausibility

Mission Phase	Number of Potential Failure Modes in Each Category			Total
	Plausible	Plausible but Unsupported	Implausible	
Common to Lander/Probes	1	1	1	3
Entry	1	1	—	2
Parachute	—	6	—	6
Terminal Descent	3	5	1	9
Touchdown	1	1	—	2
Post-Landing	1	5	—	6
Common to EDL Phases	—	5	—	5
Total	7	24	2	33

Figure 6-1 depicts the MPL EDL sequence and shows potential failure modes.

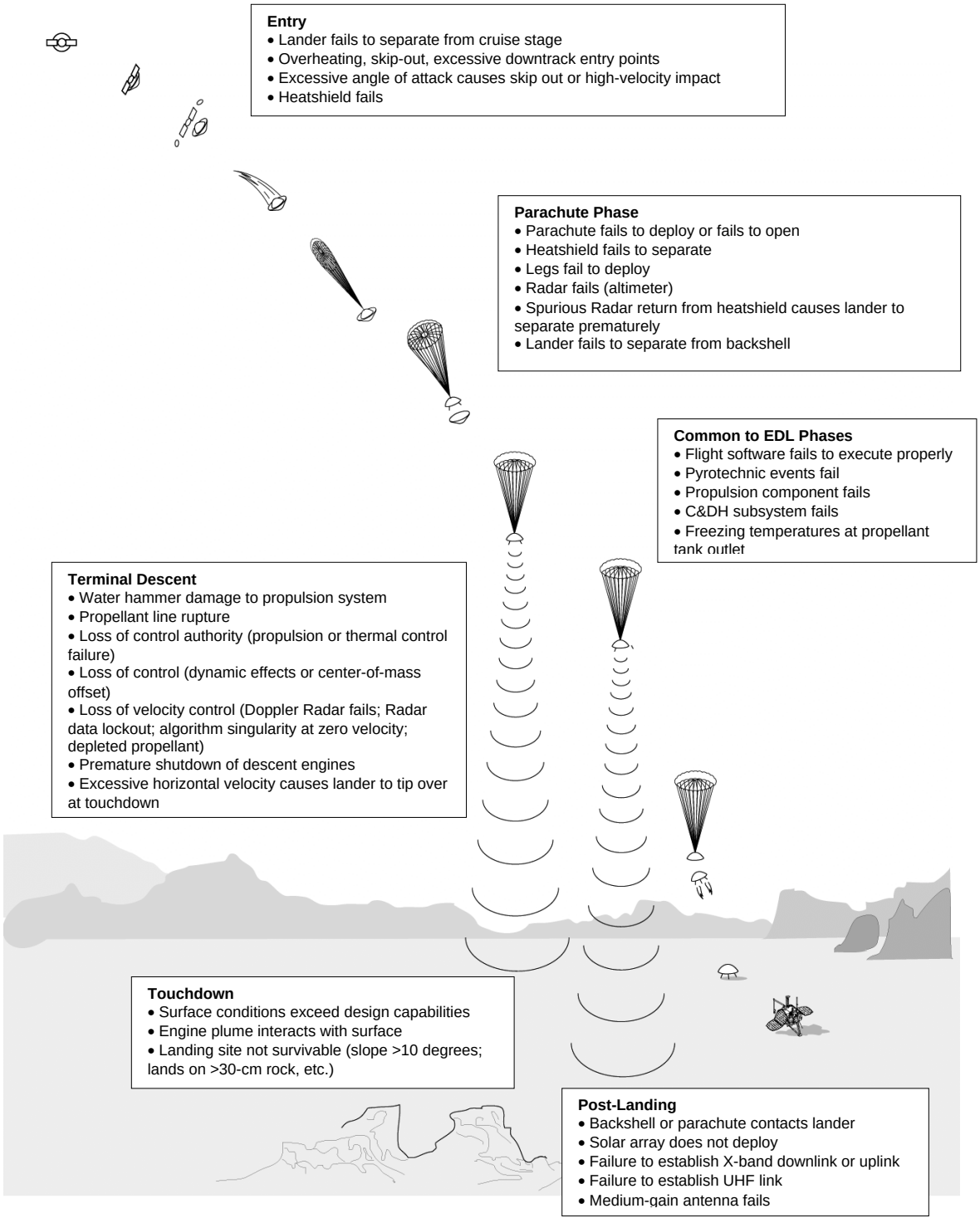


Figure 6-1. MPL Entry, Descent, and Landing (EDL) Sequence with Potential Failure Modes

6.2.1 Failure Modes Affecting the Lander and Both Probes

Failure Mode	Assessment
Lander/aeroshell fails to separate from the cruise stage due to any one of a number of causes.	PLAUSIBLE BUT UNSUPPORTED. This failure mode would necessarily preclude separation of the DS2 probes from the cruise stage. Consequently, this failure mode and all of its sub-modes have been intensely reviewed, as discussed in Section 7.2.1. While impossible to rule out, it is not considered likely. A review of the pyro firing design and distribution showed that all circuits were tested and properly functional prior to launch. The flight software that controls the firing of the pyros was extensively tested at the unit level, during integration test, and in many tests in the System Test Laboratory. The performance of the software was as expected.
Incorrect aerodynamic models and/or Mars atmosphere databases, leading to overheating, skip-out, or excessive downtrack entry points.	IMPLAUSIBLE. The same models and databases were used successfully for the Viking and Mars Pathfinder designs. Some updates to the Mars atmosphere database were made based on MGS data, and the modeling approach has been independently verified by NASA Langley Research Center (LaRC).
FLAG A Lander and both probes encounter conditions at the surface that exceed design capabilities.	PLAUSIBLE. Local slopes and surface roughness at each of the three touchdown sites could have exceeded design capabilities for successful landing. Large-scale (on the scale of a few tens of meters) slopes greater than a few degrees are absent, except for part of a crater, which may encompass about 5 to 10 percent of the landing dispersion ellipse. However, lander-scale slopes could have been excessive for all three vehicles, even in the absence of large-scale slopes. The dispersion of the three impact points is large compared to the crater size, so independent local slopes would be required to account for the failures. See Sections 7.1.3 and 9.1.2. A soft surface layer overlaying a harder substrate might have caused the lander to come to rest at an anomalously large azimuthal orientation (see Sections 7.1.3 and 7.4.5). This condition also might have caused the probes to bounce and land in an attitude such that communication was not possible. See Section 9.1.2.

6.2.2 Failure Modes Affecting Only the Lander

ENTRY	
Failure Mode	**Assessment**
Skip out or high-velocity impact due to excessive angle of attack caused by: —Center-of-mass offset due to propellant migration —Center-of-mass offset due to mechanical shifting —Asymmetric ablation	PLAUSIBLE BUT UNSUPPORTED. There is a potential of propellant migration during "zero g" cruise that can cause significant offsets between the center of mass and the center of pressure of the aeroshell during hypersonic entry. This would change the angle of attack of the aeroshell and cause large displacements in the landing location. The Propulsion Subsystem design does not prohibit the migration from occurring. See the discussion on Propellant Migration Prior to Hypersonic Entry in Section 7.5.3 and 7.5.4. All other sources of excessive angle of attack are unsupported. See Section 7.2.2. See also the discussion with respect to attitude control concerns in Section 7.3.7.1.
FLAG B Heatshield fails due to: —Manufacturing defect —Micrometeoroid impact —Inadequate design margins	PLAUSIBLE. The design, fabrication, test, and handling history of the heatshield were examined by the Board. The high degree of heritage to the successful Mars Pathfinder design, fabrication, test, and flight results led the Board to the assessment that the failure of an undamaged heatshield is implausible. The most credible source of heatshield failure is burnthrough as a result of a cavity created by impact of a relatively large micrometeoroid; the associated modeling is uncertain, but has low probability with conservative assumptions. See Section 7.1.2.

PARACHUTE PHASE	
Failure Mode	**Assessment**
Parachute fails: —Failure to initiate parachute deployment —Pyro/mortar failure —Chute fails to open	PLAUSIBLE BUT UNSUPPORTED. High reliability, test verification, and Mars Pathfinder similarity of the pyro/mortar deployment system make its failure unlikely. The chute is a pure heritage item from Pathfinder. Although there was not an extensive qualification program as part of the Pathfinder design phase, the Pathfinder chute did, in fact, work, thus providing at least one successful occurrence. The deployment conditions are different from Pathfinder, but are less severe. A review of the pyro firing design and distribution showed that all circuits were tested and properly functional prior to launch. See Section 7.2.3 and Section 7.6, paragraph 3.f.
Heatshield fails to separate.	PLAUSIBLE BUT UNSUPPORTED. A failure of the heatshield to separate could prevent lander separation. A review of the pyro firing design and distribution showed that all circuits were tested and properly functional prior to launch. See Section 7.2.4.
Legs fail to deploy.	PLAUSIBLE BUT UNSUPPORTED. A failure of one or more legs to deploy could cause significant damage to the lander at touchdown. Design and test verification of leg deployment was adequate. See Section 7.2.5.
Radar fails: altimeter.	PLAUSIBLE BUT UNSUPPORTED. The landing Radar altimeter electronics are verified as part of the built-in test (BIT) function. Based on the BIT performed prior to entry, it is known that the altimeter electronics were working up to and including the output of the power amplifier. The T/R MUX and the antenna itself could not be tested due to RF operational restrictions within the heatshield, but were tested and verified to be properly functional prior to launch. See Section 7.6, paragraph 4.b.
Lander separates from backshell prematurely due to spurious Radar return (altimeter mode) from heatshield.	PLAUSIBLE BUT UNSUPPORTED. If the Radar detected the separated forward aeroshell during descent, it might interpret this as ground detection, initiating early parachute separation and loss of mission due to propellant depletion and loss of control before touchdown. See Section 7.3.11.

PARACHUTE PHASE (continued)	
Failure Mode	**Assessment**
Lander fails to separate from backshell.	PLAUSIBLE BUT UNSUPPORTED. This robust design has generous separation margin, and thorough analysis and quasi-static test verification. A review of the pyro firing design and distribution showed that all circuits were tested and properly functional prior to launch. See Section 7.2.6.

TERMINAL DESCENT	
Failure Mode	**Assessment**
Water hammer damage to propulsion system.	PLAUSIBLE BUT UNSUPPORTED. During powered descent, the 12 60-lbf descent thrusters operate in a pulse mode. This generates large pressure waves (water hammer) and expansion waves in the liquid feed system and thrusters that can shake loose contamination, damage valve seats and catalyst beds, and excite structural resonances. See Section 7.5.10.
Propellant line rupture due to water hammer interaction with structure.	PLAUSIBLE BUT UNSUPPORTED. The failure mode here is excessive deflections of propellant lines that produce bending stresses in lines and fittings high enough to cause rupture. Large water hammer loads arising late in the program made the existing support system design marginally acceptable. Although the propellant line support system strength margins were generous, the system was overly compliant. The test-correlated finite-element model (FEM) analysis of the system was conservative. Yielding of the 321 annealed stainless steel at weld joints was predicted to occur at two locations. This material is ductile and has good fatigue properties. A thorough fatigue analysis based on fatigue test specimens showed positive margins on the requirement of four lifetimes. The test-correlated FEM and fatigue analyses verification of the system were acceptable. See Section 7.2.7.
Loss of control authority due to propulsion component or thermal control failure.	PLAUSIBLE BUT UNSUPPORTED. Failure of any one of the propulsion components used during descent would probably have resulted in loss of lander control. However, if the water hammer environment is ignored, the environmental and lifetime requirements on these components are fairly benign. See Sections 7.5.8 and 7.5.9. Line temperatures downstream of the tank were measured to be 4.6 degrees C. The actual temperature could be lower upstream, leading to the potential of freezing and partial blockage in the tank outlets or lines.
FLAG C Loss of control due to dynamic effects.	PLAUSIBLE. Control margins are incorporated to provide robustness against modeling simplification. The complexity of the MPL terminal descent dynamics requires considerable modeling, all of which unavoidably includes modeling uncertainties and simplifications. While no single model simplification is of concern by itself, the total combined effects of all model simplifications could produce unacceptable erosion of control margins. See Sections 7.3.4, 7.3.5, and 7.3.6.
FLAG D Loss of control due to center-of-mass offset.	PLAUSIBLE. Thruster imbalance and center-of-mass uncertainty were verified primarily by analysis and, in addition, control authority margins were relatively low. Center-of-mass shift caused by fuel migration is uncertain and could significantly contribute to total loss or further erosion of control authority margins. See the discussion with respect to attitude control concerns in Section 7.3.7.2, and see the discussion with respect to propellant migration concerns in Sections 7.5.3 through 7.5.7.

TERMINAL DESCENT (continued)	
Failure Mode	**Assessment**
Loss of velocity control: —Radar fails: Doppler —Radar data lockout —Algorithm singularity at zero velocity	PLAUSIBLE BUT UNSUPPORTED. The Radar is well designed and has good heritage. Radar data lockout is unlikely. The components involved, particularly the IMU, were sufficiently checked out during the cruise phase and in investigations conducted prior to EDL. Significant out-of-specification performance of the IMU would be required. The zero velocity problem was well known, and there are no known mechanisms for the vertical velocity to reach conditions where this problem can occur. The Doppler processor electronics are not tested as part of the Radar BIT function. Therefore, although thoroughly tested and verified before launch, the Doppler electronics' functionality could not be tested as part of cruise pre-EDL checkout. The BIT function did demonstrate that the altimeter electronics were operating correctly prior to EDL. See Sections 7.6, Paragraph 4.b (Radar Failure), 7.3.1 (Radar Data Lockout), and 7.3.9 (Zero Velocity Singularity).
Lander tips over due to excessive horizontal velocity at touchdown.	PLAUSIBLE BUT UNSUPPORTED. The Radar system design is sensitive to large-scale slopes, resulting in a bias in the horizontal velocity estimate that is in error by 0.2 meter per second for each degree of slope. The resulting horizontal velocity reduces the lander's tolerance to slopes at touchdown, which could result in lander tip-over. However, this is unlikely to be a factor in the lander loss. Most of the landing footprint does not have significant large-scale slopes, so the error does not come into play. The large crater that could be in a small part of the lander footprint appears to have such large slopes that the lander would not survive touchdown with or without the error. See Section 7.3.2.
Loss of velocity control caused by depleted propellant.	IMPLAUSIBLE. Analysis of the delta-V capability indicates that there was more than adequate margin for a safe landing.
FLAG E Premature shutdown of descent engines. MOST PROBABLE CAUSE OF LOSS OF MISSION	PLAUSIBLE. A magnetic sensor is provided in each of the three landing legs to sense touchdown when the lander contacts the surface, initiating the shutdown of the descent engines. Data from MPL engineering development unit deployment tests, MPL flight unit deployment tests, and Mars 2001 deployment tests showed that a spurious touchdown indication occurs in the Hall Effect touchdown sensor during landing leg deployment (while the lander is connected to the parachute). The software logic accepts this transient signal as a valid touchdown event if it persists for two consecutive readings of the sensor. The tests showed that most of the transient signals at leg deployment are indeed long enough to be accepted as valid events, therefore, it is almost a certainty that at least one of the three would have generated a spurious touchdown indication that the software accepted as valid. The software — intended to ignore touchdown indications prior to the enabling of the touchdown sensing logic — was not properly implemented, and the spurious touchdown indication was retained. The touchdown sensing logic is enabled at 40 meters altitude, and the software would have issued a descent engine thrust termination at this time in response to a (spurious) touchdown indication. At 40 meters altitude, the lander has a velocity of approximately 13 meters per second, which, in the absence of thrust, is accelerated by Mars gravity to a surface impact velocity of approximately 22 meters per second (the nominal touchdown velocity is 2.4 meters per second). At this impact velocity, the lander could not have survived. See Section 7.7.2.

TOUCHDOWN	
Failure Mode	**Assessment**
FLAG F Landing site not survivable: —Lander-scale slope greater than 10 degrees —Deep, low-density upper layer —Lands on a rock >30 centimeters tall —Surface interaction on landing results in undesired azimuth orientation	PLAUSIBLE. Large-scale (a few tens of meters) slopes greater than a few degrees occur only in part of a crater, which overlays 5 to 10 percent of the landing ellipse. In this region, lander-scale slopes can be greater than 10 degrees, so it is impossible to rule out the potential that the lander came to rest on a surface that was beyond its design specifications. The presence of rocks cannot be ruled out, but is deemed unlikely based on interpretations of the available remote-sensing data. See Section 7.1.3. The ability for the lander to communicate directly with Earth and generate adequate power is determined by the azimuth orientation at landing, which could be adversely affected by a deep, low-density surface upper layer. See Sections 7.1.3, 7.4.5, and 7.5.4.
Surface interaction: —Engine plume excavation; ground effects —No engine cutoff at touchdown —Plume ground effects	PLAUSIBLE BUT UNSUPPORTED. Adverse plume effects could arise from interaction of adjacent thruster plumes during descent and interaction between the plumes and ground just before landing. The former could lead to backflow, contamination, localized heating, and reduction in control authority. The latter could again reduce control authority, adversely alter the landing site, and generate large dust clouds. See Section 7.5.6.

POST-LANDING	
Failure Mode	**Assessment**
FLAG G Backshell contacts lander and/or parachute drapes over lander.	PLAUSIBLE. This failure mode could cause structural damage to the lander or its mechanisms, and could also preclude the ability to generate power if the lander was impacted by the backshell or draped by the parachute. Simulations conducted after EDL indicate a probability of approximately 1 percent that the backshell/parachute system touched down close enough to the lander to potentially recontact it on the surface. This analysis is rather sensitive to assumptions about the direction and magnitude of the winds at the landing site at the time of touchdown (absence of winds increases the probability of draping). See Section 7.1.4.
Lander solar array does not deploy.	PLAUSIBLE BUT UNSUPPORTED. Depending on failure to deploy or partial deployment, this would impact the ability to recharge the batteries. A secondary effect would be to preclude the MGA from articulating through its full range. This would prevent a direct-to-Earth X-band downlink (see Section 7.4.9). The mechanical system design was robust and there was an adequate test verification process. A review of the pyro firing design and distribution showed that all circuits were tested and were properly functional prior to launch (see Section 7.2.8).
Failure to establish X-band downlink.	PLAUSIBLE BUT UNSUPPORTED. The Red Flag PF/R against the Cassini spare transponder (Side A on MPL) was for an open via on the power converter board. If a similar problem occurred during EDL or touchdown, the result would be loss of X-band downlink. This would not explain the loss of the X-band uplink or UHF link (see Section 7.4.8). The solid-state power amplifier (SSPA) used on the lander was of the same design as the ones on the cruise stage. Other than a problem associated with a 1 to 2 dB drop in RF output power associated with this design, there is no evidence in the test program of a problem resulting in total loss of RF output. The SSPA could not be turned on in flight. The failure of the SSPA would not explain the loss of X-band uplink or UHF (see Section 7.4.13). Failure modes of the Diplexer and Telemetry Modulation Unit were reviewed and found to be implausible (see Sections 7.4.11 and 7.4.12).

POST-LANDING (continued)	
Failure Mode	**Assessment**
Failure to establish X-band uplink.	PLAUSIBLE BUT UNSUPPORTED. If an open via (same power converter board as above) were to occur on the receiver power lines, the result would most likely be to trip component-level fault protection, which was enabled during EDL, and swap to the backup Deep Space Transponder (DST). If power to the Command Detector Unit (CDU) was lost, the component-level fault protection would not swap to the backup unit, which could result in the loss of uplink command capability. The CDU itself was reviewed and was used during flight; its failure is considered implausible (see Section 7.4.10). The RF Coaxial Transfer Switch and Uplink/Downlink Card were evaluated and the failure of these elements is considered implausible (see Sections 7.4.6 and 7.4.14). Any of the above would explain the loss of X-band uplink, but not the loss of X-band downlink or UHF.
Failure to establish UHF link	PLAUSIBLE BUT UNSUPPORTED. The UHF link was tested primarily for use with MCO. The testing with MGS, because of the phasing of the two missions, was done with a test set and was piecemeal rather than an overall end-to-end test. The pieces all appear to be accounted for, and the recent tests with Stanford and MGS were successful. The UHF transceiver was not turned on in flight. The link margin between the MGS transmitted beacon signal is approximately 10 dB. If the path loss were of that magnitude for any reason, the lander would not respond with a transmitted signal. See Section 7.4.7.
Loss of signal due to: —MGA fails to unlatch —Gimbal failures prevent deployment of MGA	PLAUSIBLE BUT UNSUPPORTED. The MGA latch and gimbal system designs have adequate margins and the test verification process was complete. The same gimbal system was successfully actuated on the MCO solar array during flight. A review of the pyro firing design and distribution showed that all circuits were tested and properly functional prior to launch. See Section 7.2.9.

6.2.3 Failure Modes Common to EDL Phases

Failure Mode	Assessment
Flight software fails to execute properly.	PLAUSIBLE BUT UNSUPPORTED. The flight software can produce incorrect actions because of errors in logic, incorrect database values, and incorrect equations or missing statements. The incorrect actions may cause faults in other subsystems that depend on the software for their proper functionality. For example, EDL functions depend on the software for triggers to open gates for certain events such as parachute deployment, aeroshell separation, backshell and parachute separation, and descent engine touchdown enable. If the software does not operate properly, the gates may be missed or signaled at the improper time, and the planned events that depend on those gates to open will not happen at the correct time or condition. The software gates were tested extensively in the System Test Laboratory and the errors that were discovered were corrected and regression tested. The flight software logic errors may also cause errors in fault-protection logic, which may prevent a switch from a failed component to a backup component. An example of this kind of error was found in the uplink loss routine (see Section 7.7 for further discussion). The logic would have caused the loss of command uplink capability if the receive chain failure occurred during EDL. However, Sequence C, which starts to execute a few days after the landing, does provide a switch to the backup uplink string. While this failure could cause a temporary problem, there would be a recovery when Sequence C started.
Pyrotechnic events fail.	PLAUSIBLE BUT UNSUPPORTED. The Pyro Initiation Unit (PIU) was subjected to a detailed schematic-level review. Its design and redundancy approach is fundamentally sound and the test program was determined to be acceptable. Rework of the PIU electronics did occur late in the program to correct cracked diodes in several locations and to remove a programmable array logic (PAL) device. The box-level retest program and subsequent system-level test activity were adequate to verify performance and reliability. As part of the system-level test, all pyro lines were verified to be operational with acceptable pulse amplitude and energy. The non-operation of all other pyro lines was also verified as part of the test. Given its redundancy and proper operation prior to EDL, a failure of the PIU is considered unlikely. See Section 7.6.
Propulsion component fails (other than due to water hammer).	PLAUSIBLE BUT UNSUPPORTED. A failure in any of the propulsion components used during EDL would have resulted in loss of spacecraft control. All components, down to and including valve heaters, had to work. However, a failure is considered unlikely. Adequate design margins had been demonstrated and the environmental and lifetime requirements on these components was fairly benign (other than that due to water hammer environment, which is discussed in another failure mode). Prior to loss of telemetry, it was confirmed that pressurization had successfully occurred, the regulator had locked up at the expected pressure, and the valve heaters had been activated. See Section 7.5.9.
Command and Data Handling Subsystem fails: —Processor reset —Hardware component	PLAUSIBLE BUT UNSUPPORTED. A processor reset or a hardware failure in the C&DH could preclude the proper execution of the EDL sequence. Failure modes exist that could cause a flight processor reset; however, none occurred in flight prior to the start of EDL. The component-level environmental test program was a good program and no problems with the C&DH hardware occurred in flight. See Sections 7.4.1, 7.4.2, 7.4.3 and 7.4.4.

Failure Mode	Assessment
Freezing temperatures at tank outlet.	PLAUSIBLE BUT UNSUPPORTED. Line temperatures dropped from 13 degrees C to 4.6 degrees C (3 degrees C above freezing) during the TCM-5 slews and burn. The measurement was made on one of the two tank outlet feed lines approximately 6 inches downstream of the tank outlet in the vicinity of a support boss that had a temperature believed to be as low as –20 degrees C. There was no sensor on the feed line of the second tank. The support boss was conductively coupled to the tank near the tank outlet, and neither the tanks nor lines had heaters or insulation in the immediate area. The concern is that propellant temperatures in the tank near the attachment point could have been even colder and that there may have been some local freezing or "slushing." The outlets contain perforation plates. Partial freezing of the propellant upstream of the outlets could lead to a large flow imbalance between the two tanks. This would result in center-of-mass offset developing during powered descent. If combined with the potential center-of-mass offsets that could have occurred during "zero g" cruise (see Section 7.5.4) and/or the center-of-mass offset that could be developing due to potential mismatches in flow resistance across the normally closed pyro valves (see Section 7.5.7), control authority could have been jeopardized. Inadequate testing was done to validate the tank and line thermal models given the very low margins observed.