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

JPL Special Review Board

22 March 2000

JPL
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

Arden Albee

Steven Battel

Richard P Brace

Richard Brace

Garry M. Burdick

Garry Burdick

Peter Burr

Peter Burr

John Casani

John Casani, *Chair*

Duane Dipprey

Jeff J. Lavell

Jeff Lavell

Charles J Leising

Charles Leising

Duncan MacPherson

Wesley A. Menard

Wesley Menard

Richard Rose

Robert L. Sackheim

Robert Sackheim

Al Schallenmuller

Al Schallenmuller

Charles Whetsel, Deputy Chair

CONTENTS

TABLES

FIGURES

APPENDICES

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.

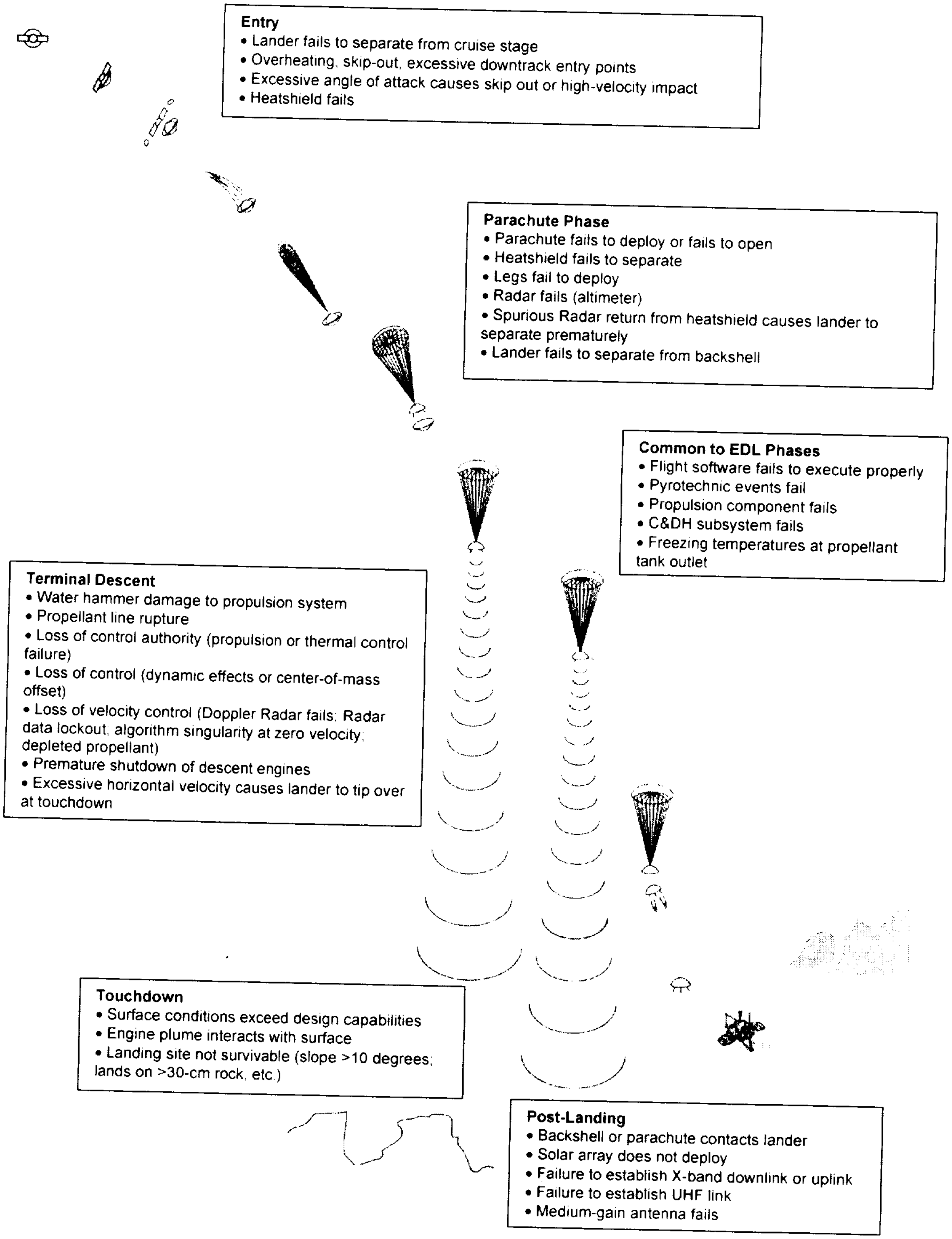
Section 7 of the report is organized by technical discipline, with the MPL failure modes described in greater detail. (Section 7 also addresses failure modes that affect both MPL and DS2.) In the summaries in subsections 6.2.1 through 6.2.3, the appropriate references to Section 7 are included in the 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.



Entry
- Lander fails to separate from cruise stage
- Overheating, skip-out, excessive downtrack entry points
- Excessive angle of attack causes skip out or high-velocity impact
- Heatshield fails

Parachute Phase
- Parachute fails to deploy or fails to open
- Heatshield fails to separate
- Legs fail to deploy
- Radar fails (altimeter)
- Spurious Radar return from heatshield causes lander to separate prematurely
- Lander fails to separate from backshell

Common to EDL Phases
- Flight software fails to execute properly
- Pyrotechnic events fail
- Propulsion component fails
- C&DH subsystem fails
- Freezing temperatures at propellant tank outlet

Terminal Descent
- Water hammer damage to propulsion system
- Propellant line rupture
- Loss of control authority (propulsion or thermal control failure)
- Loss of control (dynamic effects or center-of-mass offset)
- Loss of velocity control (Doppler Radar fails; Radar data lockout, algorithm singularity at zero velocity; depleted propellant)
- Premature shutdown of descent engines
- Excessive horizontal velocity causes lander to tip over at touchdown

Touchdown
- Surface conditions exceed design capabilities
- Engine plume interacts with surface
- Landing site not survivable (slope >10 degrees; lands on >30-cm rock, etc.)

Post-Landing
- Backshell or parachute contacts lander
- Solar array does not deploy
- Failure to establish X-band downlink or uplink
- Failure to establish UHF link
- Medium-gain antenna fails

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.

7 MPL Discipline Area Assessments

The major thrust of this investigation was centered on Review Teams of the Board conducting detailed reviews and interviews in specific technical discipline areas. Each Review Team focused on a list of postulated failure modes and attempted to ascertain whether or not the failure was plausible, based on precautions taken during the design phase, tests, or verifications conducted during system validation, and/or in-flight performance that validated that the functionality in question was available at the last time telemetry was available from the lander.

7.1 MPL Environment and Landing Site

INTRODUCTION

As part of the JPL Special Review Board MPL/DS2 failure investigation, a multidisciplinary Review Team was formed to examine environmental effects that might have led to the loss of MPL or DS2. Two groups were formed: one focused on the surface properties and interactions with any of the three spacecraft; the second addressed issues relating to aerodynamic entry and descent.

The first group reviewed the information that had been obtained prior to landing regarding the nature of the terrain in the targeted landing site. In addition, the MGS science teams provided new observations of the landing area and analyses in the following areas:

1. *Large-scale slopes (scale of hundreds of meters).* The presence of large-scale slopes greater than 10 degrees would introduce Radar–terrain interactions that affect the horizontal–velocity control during terminal descent. The laser altimeter (MOLA) on MGS provided maps of topography and point-to-point slopes. Most of the area is smooth; however, the area does include a large depression marked by slopes, the majority of which are less than 5 degrees. Approximately 1 percent of the area has large-scale slopes greater than 10 degrees.
2. *Medium-scale slopes (scale of tens of meters).* The spread of the returned optical pulse was used to map the roughness of the surface at the scale of the laser footprint. Over the majority of the landing zone, the pulse spread correlates well with the larger scale slopes, which is contrary to the norm for most of Mars. This indicates that the pulse spread is most likely due to the regional slope and that the surface at this scale is smoother than the norm for most of Mars.
3. *Small-scale slopes (scale of meters).* The camera (MOC) on MGS obtained high-resolution images of the landing zone. MOC provided stereophotogrammetric and photoclinometric (shape from shading) analysis for both medium- and small-scale slopes, calibrated by reference to a MOLA profile across the edge of the depression. Most of the landing zone appears to be quite smooth. In the most rugged region (a small portion of the landing zone) along the profile crossing the edge of the depressions, no more than 12 percent of the surface has slopes of more than 10 degrees at scales of 10 to 40 meters per pixel. In addition, approximately 4 percent of the surface has slopes of more than 15 degrees. The percentage of the landing ellipse that could present small-scale hazards is small — only a few percent.
4. *Surface properties.* Thermal emission data from TES and from previous missions indicate that most of the landing zone has a layer of a low thermal inertia/low-density material that is at least a few centimeters thick. Both these data and the accepted geologic model for this terrain indicate that rocks greater than 30 centimeters should not be a problem (that is, within the available lander clearance height).
5. *Subsurface conditions/models.* The presence of a hard subsurface of frozen permafrost is predicted by typical models of this terrain. The depth of this material could be anywhere below a few

centimeters. The presence of low-density, loosely packed material on top of a hard surface might lead to a "lubricating" situation that results in the inability of MPL to come to rest in the required azimuthal orientation or the inability of the DS2 probes to penetrate the surface and remain upright.

The topics that follow were considered by the second group, which focused on aerodynamics and the atmospheric entry conditions:

1. *Heatshield design heritage.* Mars Pathfinder design, manufacturing and test heritage and deviations therefrom (size, ballistic coefficient, thickness, lack of spin). Discussion of worst-case effects of each deviation on landing-site accuracy, integrated heating load, structural g-loads.
2. *Heatshield physical integrity/workmanship.* Deviations from the Mars Pathfinder manufacturing/inspection process (limited). Rework/handling incidents prior to launch (one to the heatshield substructure, none to the TPS). Tooling pinhole issue discussion.
3. *Entry body mass properties.* Center of mass/center of pressure mismatch, mass properties, and effect on landing site or hypersonic entry survivability. Hypersonic entry orientation: specification of propulsion tank axis (30 degrees from vertical; relationship to downtrack and cross-track errors). Natural frequencies of heatshield aerodynamics and propellant tanks fuel slosh/transfer during variable dynamic pressure/deceleration field and potential for coupling.
4. *Small-forces discrepancies between telemetry and radio metric reconstructions.* Magnitude, possible causes (thrusters, mass properties, etc.); implications for entry state and/or hypersonic entry.
5. *Delivery to the entry state.* Cross-track drift from TCM-4 to entry. Discussion of possible causes. TCM-4 execution errors (subsequently shown to be statistically consistent with expected errors for a maneuver of the size encountered), small forces, etc. Rationale for lack of cross-range adjustment capability at TCM-5.
6. *MPL parachute/backshell touchdown separation from the lander.* Addressed the concern that the parachute/backshell may have come down near/on top of MPL.

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

FAILURE MODE DESCRIPTION

Errors in the navigation delivery to the atmospheric entry point can cause loss of the spacecraft due to atmospheric "skip-out" under the following conditions:

- If the trajectory is too shallow.
- If there is not sufficient time to complete parachute/propulsive deceleration.
- If the trajectory is too steep or causes the spacecraft to be sent into unacceptably hazardous terrain in the up-, down-, or cross-track directions.

These effects can also be caused by incompatibilities between the spacecraft inertial mass properties and aerodynamic properties. This section discusses the effects of all such failures, as well as potential causes due to navigation delivery errors. Due to the interdisciplinary nature of this failure mode, several other causes of failure are discussed elsewhere (specifically, aerodynamic properties are discussed in 7.1.2, center-of-mass motion due to mechanical shifting is discussed in 7.2.2, and center-of-mass motion due to propellant migration is discussed in sections 7.5.3 through 7.5.5).

INTRODUCTION

The delivery of the spacecraft to the targeted atmospheric entry conditions within the allowable tolerances was to be accomplished by the navigation team after collecting radio metric tracking data, performing a series of orbit-determination solutions, and specifying a series of propulsive maneuvers as required. Ultimately, the parameters of interest were reduced to the control of entry flight-path angle (critical to both hypersonic entry and landing-site accuracy) and the cross-track error (primarily influencing only the landing-site accuracy). These effects can also occur if there is a large misalignment between the aerodynamic center of pressure and the physical center of mass of the entry body, and can cause the lander to follow a trajectory that is either too steep or too shallow. Mass properties primarily contribute to the in-plane (steep/shallow) error and not to the cross-track error. This is because the primary source of uncertainty in spacecraft mass properties is due to potential mass migration between the two propellant tanks. These tanks lie on a line only 30 degrees from the entry plane, as discussed in sections 7.2.2 and 7.5.3 through 7.5.5.

MISSION NAVIGATION OVERVIEW

During project development, a navigation plan was created to confirm that, given certain assumed spacecraft performance characteristics, the flight team could execute a navigation strategy (including periods of orbit determination, followed by planned course corrections) that would result in delivery to a point in space from which the lander could commence a safe entry into the atmosphere and a safe descent to the desired zone on the surface. This pre-launch analysis included assumptions regarding the number of small-force events (thruster firings for attitude control or re-orientation) and the ability of the flight team to measure or model the effects of each of these items on the trajectory. These assumptions were folded into the development of a maneuver strategy intended to ensure that the penultimate maneuver (TCM-4) would be small enough to correct all but the smallest trajectory errors (errors so small that they could only be seen once inside the gravity well at Mars). These final errors (believed to be predominantly in the entry flight-path dimension or along-track) were to have been corrected by the execution of TCM-5, approximately 6 hours prior to entry. Because of the concern of a potential operator error in designing a maneuver from scratch at this critical point, the project made the decision to pre-design a series of along-track maneuvers; at the appropriate time, the project would uplink the maneuver that was closest to the desired solution. This technique was previously employed on Mars Pathfinder, MGS, and Magellan.

For reasons described below, it became more difficult to meet the expected navigation performance after launch while following the plan described above. The first event that caused difficulty was an anomaly encountered immediately after launch affecting the spacecraft's Star Camera. Stray light from the spacecraft interfered with its ability to use the camera to perform gyro and attitude updates without slewing the spacecraft away from its normal cruise attitude. This would ultimately increase the number of small-force events encountered by the spacecraft throughout cruise, adversely affecting the navigation accuracy.

The second unanticipated event occurred after the navigation team was augmented with additional workforce and expertise following the loss of MCO. At this point, it was discovered that the ability to model the effects of small forces (already more numerous than previously planned because of the daily slews required by the Star Camera anomaly) based on telemetry received from the spacecraft was not as good as was previously assumed. During the final weeks prior to entry, significant progress was made in improving the understanding of these uncertainties, yielding information that could have been put to better use if uncovered earlier in the mission. Finally, given the new environment of more frequent small-force events, and the increased uncertainty associated with each, the size of TCM-4 was recalculated. Predictably, the magnitude of the maneuver had increased in size over the previous plan.

The recalculation of TCM-4 caused the magnitude to cross a boundary within the spacecraft performance space that led to unanticipated, nonlinear increases in the execution errors associated with this burn. The spacecraft performance requirements typically call for side errors between 1 and 2 percent of the commanded velocity for maneuvers that are either short enough to avoid creating off-axis disturbances or long enough to allow the control systems to damp these disturbances out. In between these extremes, there is a region of maneuver magnitudes where larger errors (up to 10 percent) build up before the control system has time to zero these out. As previously noted, the navigation plan did call for an opportunity following TCM-4 to correct the along-track component of these errors, but there was no plan to correct the cross-track errors, which had previously been assumed to be smaller. Eventually, this led to a delivery that was quite close to the expected center of the desired landing-zone along-track, but that was at the western extreme of the cross-track dispersions. A detailed description of these events and the corresponding analysis follows.

DESIGN DESCRIPTION

During the spacecraft development, the planned entry corridor for MPL was ± 0.54 degree at a 3-sigma confidence level. This corresponded to an error in the navigation delivery of 10.7 kilometers, 3 sigma in the B-plane semi-major axis, and a semi-minor axis of 2.6 kilometers, 3-sigma (predominantly contributing to cross-track errors). As previously discussed, these statistics included models and assumptions regarding the following:

- The nature of the small forces that the spacecraft produced in course-maintaining attitude control and performing required slews (including the uncertainties in these forces, as was reported in telemetry).
- The usefulness of new tracking data types to be employed for the first time on MPL (for example, near-simultaneous tracking of the lander on approach, together with an additional spacecraft already at Mars, either MCO or MGS).
- Maneuver-execution errors estimated based on the planned sizes of each trajectory correction.

Additionally, in order to achieve the desired landing ellipse on the surface of Mars, the analysis assumed that the spacecraft center of mass could be controlled to within 2.8 millimeters of the centerline of the entry body. The resulting surface ellipse had dimensions of 85 kilometers semi-major axis (along-track) by 5.4 kilometers semi-minor axis (cross-track), both 2 sigma. Figure 7-1 shows the landing ellipse estimate at the time of the site selection several months before EDL, based on earlier 3DOF/4DOF LMA Monte Carlo simulations, adjusted in orientation to the new landing latitude of –76° S. (*Note*: The landing latitude was –75° at launch.)

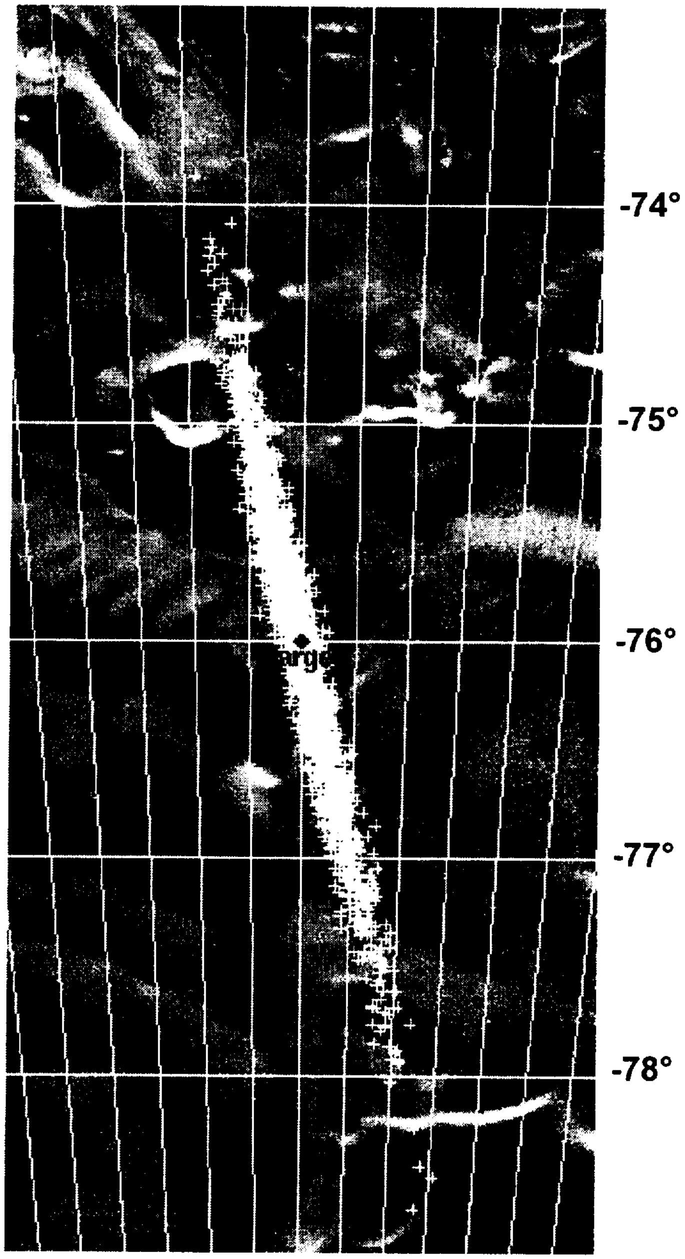


**Figure 7-1. Site Selection Ellipse —
Based on LMA Scatter for 75° S, Rotated for 76° S Landing Site**

FINDINGS

As noted above, after the loss of MCO, additional navigation expertise was added to the project to help ensure a successful delivery to atmospheric entry. At this point, the assessment of small-forces assumptions and the improvements to be expected from near-simultaneous tracking were revisited. A new set of entry statistics was calculated on 10 November 1999 that resulted in an expected B-plane error ellipse of dimension 19.3 kilometers × 3.0 kilometers, 3 sigma, including orbit determination and maneuver-execution errors (for the magnitude of TCM-4 assumed in the pre-launch navigation plan). This corresponded to a 3-sigma entry flight-path angle of 0.94 degree, 3 sigma, which was still believed to be within the spacecraft design capabilities, even though this was considerably larger than previously planned for. The resulting surface ellipse, including the effects of an updated atmosphere model, had dimensions of 138 kilometers semi-major axis (along-track) by 5.4 kilometers semi-minor axis (cross-track), both 2 sigma. Figure 7-2 shows the TCM-4 planning ellipse, based on 3DOF LaRC simulations. Both the width and orientation of the landing ellipse are comparable to the estimates developed based on navigation analyses before the MPL launch; however, the length of the ellipse is considerably larger. This graph represents the data set available to the project to make the TCM-4 decision.

Analyses performed after EDL revealed that the effects of maneuver-execution errors were larger than expected. The TCM-4 planning ellipse was based on a maneuver magnitude of 0.35 meter per second, the best estimate available at that time. The final TCM-4 maneuver magnitude was 0.6 meter per second. This maneuver magnitude resulted in considerably larger execution errors than had been previously assumed. For very short burns, execution errors are small because little time is available for pointing errors to develop. For longer burns, errors are also small because the control system will steer back to the desired attitude. The executed burn magnitude fell in between these extremes and, therefore, was subject to a larger set of expected errors. This increased the size of the 3-sigma B-plane error to as high as 20.5 kilometers × 13.8 kilometers, using worst-case requirement estimates of maneuver-execution errors. (Typical or "expected" maneuver-execution errors led to substantially smaller B-plane errors (18.3 kilometers × 6.2 kilometers). This widening effect is illustrated in Figure 7-3, which shows both the narrow TCM-4 planning ellipse, based on the assumed maneuver magnitudes and associated error statistics, and the wider ellipse, based on the actual maneuver magnitude and associated error statistics. This graphic represents the difference between the delivery accuracy that the project assumed was achievable at the time of TCM-4 versus what is now believed to be the best estimate, after the fact. Also shown is the center of the final navigation solution based on tracking data after TCM-5 through the loss of signal.

On the basis of the final pre-entry tracking, the desired in-plane entry conditions appear to have been met. The entry flight-path angle was reconstructed at –13.10 degrees against the target zone of –13.25 ± 0.94 degrees (revised from the original –13.25 ± 0.54 degrees). The cross-track error in the B-plane was within 7.2 kilometers of the planned target, which corresponds to a motion of approximately 8 kilometers at the surface. This distance is marginally consistent (within approximately 2 sigma) with the eventual understanding of the uncertainty surrounding the spacecraft small-forces environment and TCM-4 execution errors, which are discussed above. In Figure 7-4, the yellow (light) data once again reflect the best estimate of the delivery accuracy after TCM-4; these data are based on analysis after the fact. Also in Figure 7-4, the green (dark) data represents the best estimate of where the lander actually did go, eliminating effectively all navigation errors by using the final tracking data arc through loss of signal, but continuing to represent scatter around that final solution due to atmospheric and aerodynamic uncertainties.

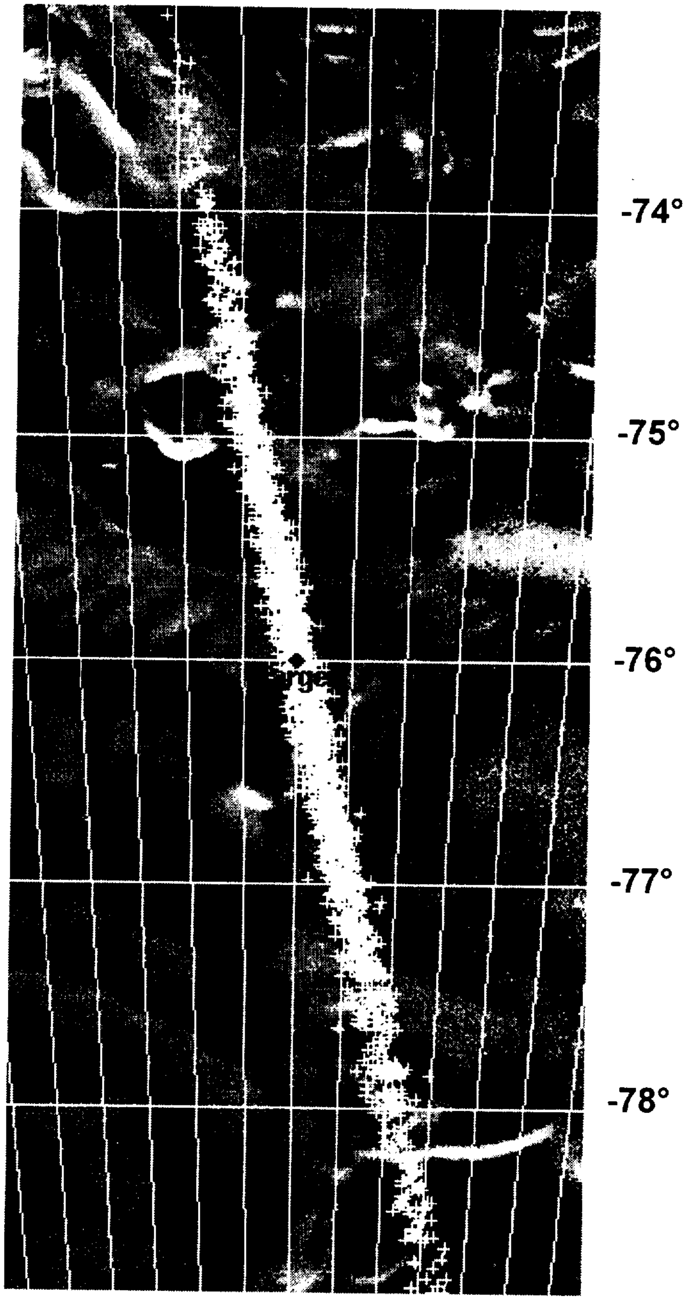


Figure 7-2. TCM-4 Planning Ellipse — LaRC 3DOF Scatter, 11/23/99

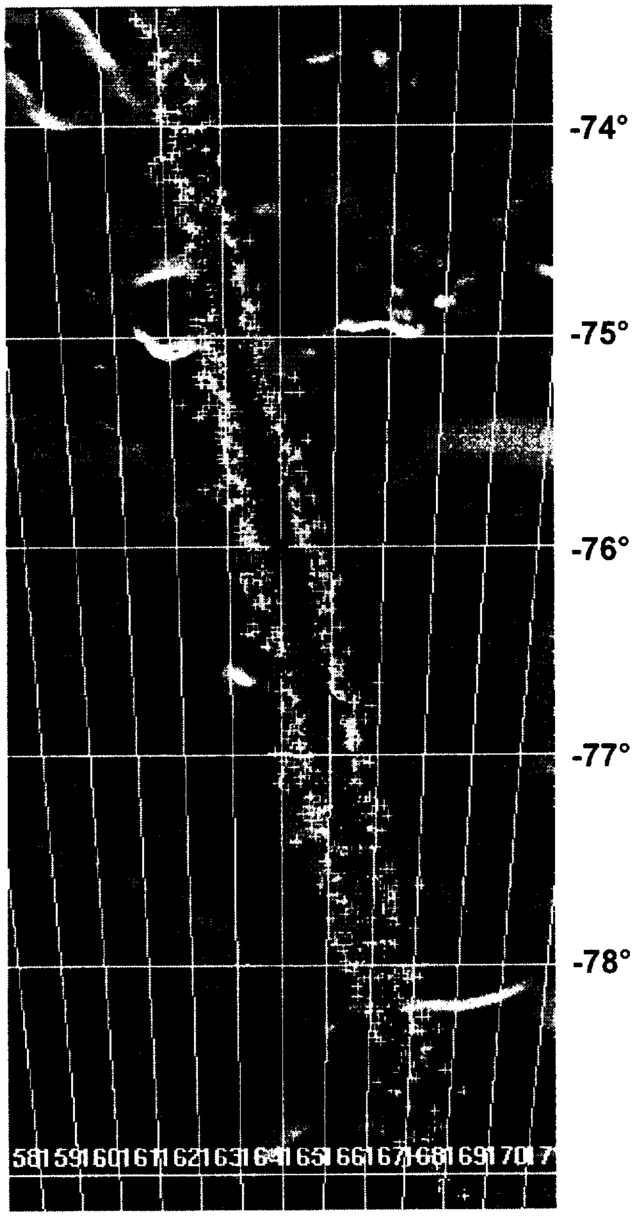


Figure 7-3. Required Maneuver-Execution Errors, LaRC 6DOF 3/3/00 (Yellow [Light]) and TCM-4 Planning Ellipse, LaRC 3DOF 11/23/99 (Green [Dark])

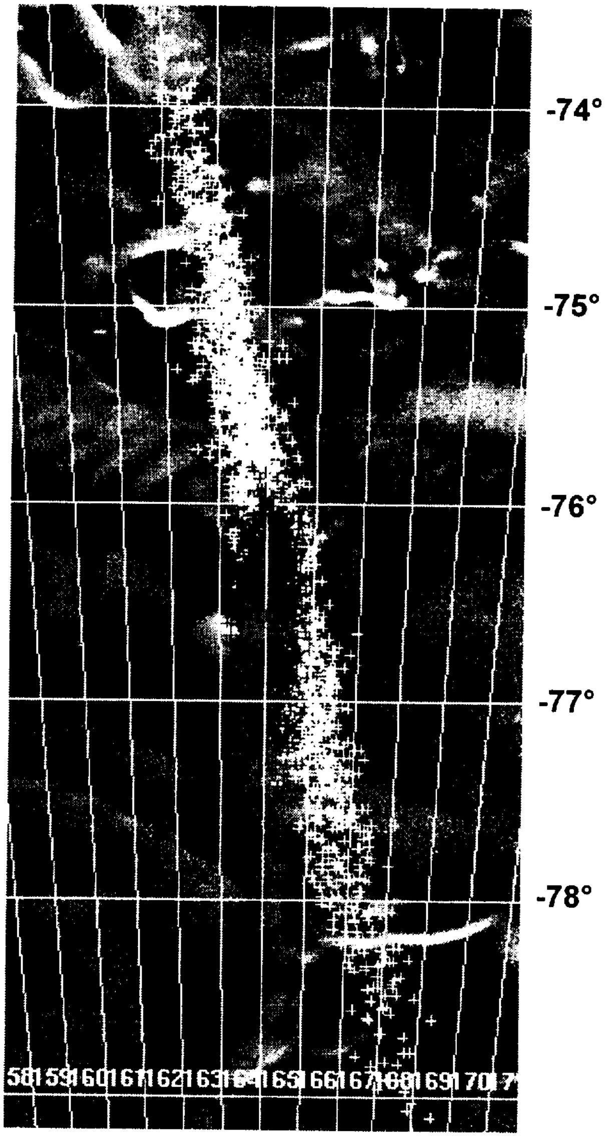


Figure 7-4. Required Maneuver-Execution Errors, LaRC 6DOF 3/3/00 (Yellow [Light]) and Final Estimated Ellipse, LARC 6DOF 3/3/00 (Green [Dark])

Some concern has been expressed regarding how close the ultimate landing site was to a questionable terrain feature immediately to the west of the reconstructed landing site. Features equally hazardous appear further north on the western edge of the planned landing ellipse and on the eastern edge of the landing ellipse. These risks were known and accepted when the landing site was selected and did not represent risks that were higher than any alternative landing site during the early fall of 1999 at the time when a burn could have been executed to move the landing site. During the days prior to EDL, the cross-range drift (subsequently attributed to TCM-4 execution errors) was observed; however, as previously discussed, the project maneuver strategy did not allow for cross-track corrections at TCM-5.

Additionally, as discussed in the introduction to this section, questions have been raised during the post-EDL anomaly investigation regarding whether or not the expected control on center of mass was actually achieved in flight (see sections 7.5.3 through 7.5.5). In the extreme, if it is postulated that all fuel used during cruise might have been drawn from one tank or the other, rather than evenly from both, this would lead to motion of the center of mass of 12 millimeters, against the specification limit of 2.8 millimeters. This is not believed to be the case. There are in-flight data as late as TCM-5 showing that this probably had not happened. The potential for this effect is discussed further in Sections 7.5.3 through 7.5.5. Note that in the extreme northern case (12 millimeters motion of the center of mass, causing steep entry), simulations predict that the lander has a less than 19-percent chance of completing the parachute/propulsive descent before impact or touchdown.

PROCESS ASSESSMENT

The spacecraft design and the manner in which it was required to operate were not well suited to the levels of navigation accuracy that the project was attempting to achieve. The elements that follow necessitated a significant effort on behalf of the entire JPL navigation community to meet the demands of the mission's entry corridor:

1. Spacecraft operability issues — for example, an uncoupled thruster, which made the system much more susceptible to short-pulse modeling errors that were uncharacterized until late in cruise.
2. Post-launch anomalies — for example, Star Camera view-angle restrictions, which caused more frequent attitude/thruster disturbances.
3. Overly optimistic assumptions regarding the quality and obtainability of new unproven navigation data types — for example, near-simultaneous tracking.

The staff for the project navigation team originally planned prior to the loss of MCO would probably not have succeeded in meeting these entry conditions had they followed the pre-launch navigation plan while simultaneously conducting both MCO aerobraking and the MGS mapping mission.

LESSONS LEARNED

1. Increase the level of involvement of peers outside of the project in the future development of navigation plans and navigation requirements on the spacecraft and tracking systems.
2. Ensure that adequate attention is paid to spacecraft operability features (for example, coupled thrusters) if tight navigation control is required for the mission. Alternatively, if cost is the chief driver, accept larger accuracy errors by constraining landing site options.
3. Conduct in-flight validation of the assumed small-forces disturbance environment either with an early cruise calibration or via another onboard sensing technique (for example, appropriately scaled accelerometer, body-rate/impulse calibration).
4. Develop a maneuver strategy to ensure that all desired entry conditions are met (along-track and cross-track). This is less sensitive to unvalidated assumptions regarding the performance of either the spacecraft (small-forces frequency or accuracy, or maneuver-execution accuracy) or of new

tracking data types. Maintain sufficient resources during the operations phase so that, if necessary, the strategy can be revisited after launch once the assumptions have been validated or invalidated. Post-launch changes to the plan must be communicated expeditiously to all concerned parties via a formal change control process.

5. Maintain a level of control of the spacecraft center of mass — accounting for all sources — that is adequate to achieve precision landing site control.
6. Develop and institute a high-fidelity end-to-end EDL simulation capability during spacecraft development. Assign single-point responsibility for the development and application of this capability. Ensure proper interfaces between this simulation and the spacecraft and navigation teams. Update this simulation at several discrete points during operations but well prior to Mars arrival.

7.1.2 Heatshield Design or Physical Flaw

FAILURE MODE DESCRIPTION

The failure of the heatshield to protect the lander from the hypersonic atmospheric flow or to hold the lander's orientation during entry could result in catastrophic mission loss. The most credible source of heatshield failure is burnthrough as a result of a cavity created by the impact of a micrometeoroid.

FINDINGS

The MPL heatshield design, manufacturing, and verification methodology have a high degree of heritage to the successful Mars Pathfinder heatshield. An instrumentation package on board Mars Pathfinder provided significant design validation data in the Martian environment after the successful landing of that spacecraft. The environment for MPL is generally less stressing than that seen by Pathfinder, and the thickness of the thermal protection system (TPS) was correspondingly reduced.

PROCESS ASSESSMENT

One deviation from Mars Pathfinder heritage was noted: the inclusion of a tooling fixture hole in the support structure underlying the TPS. Earlier testing on Mars Pathfinder with unsealed holes demonstrated the possibility of burnthrough under such conditions. After the implications of this deviation were considered, the project completed arcjet testing to verify that the presence of this hole posed no EDL threat to MPL. A sample was prepared using the same manufacturing process as the flight article, which included "sealing" flow from the TPS through the hole with adhesive material. The arcjet testing was completed with no signs of TPS or heatshield compromise.

The cavity size created by a micrometeoroid impact in the heatshield material has not been quantified; however, in many materials the cavity size is approximately an order of magnitude larger than the micrometeoroid. The size of the cavity required to cause heatshield burnthrough is also unquantified, but is probably larger than in PICA heatshield material (this size is also uncertain; however, it appears to be approximately 6 millimeters). The combination of these uncertain (but in combination probably conservative) assumptions with the standard micrometeoroid flux model gives a failure probability of approximately 1 percent. Because micrometeoroid damage calculations seem to consistently overestimate damage probability, this 1-percent value can reasonably be considered an upper bound estimate, with a lower bound estimate approximately an order of magnitude smaller. A bumper shield would provide substantial protection against micrometeoroid impact; however, this has not been incorporated on past entry vehicle missions (Pioneer Venus, Galileo, Pathfinder) as a cost/benefit decision.

Overall, the Board concludes that the heatshield design contains substantial margins and that there are no indications of any significant opportunity for damage prior to EDL.

LESSONS LEARNED

The phenomenology of burnthrough in unsealed holes does not seem to be well understood. If future projects intend to fly TPS systems over support structures containing such discontinuities, additional testing should be conducted to ensure that the purported "sealing" mechanism does in fact adequately address this failure mode for surface discontinuities of the appropriate dimension.

The assessment as to whether or not a micrometeoroid bumper shield is warranted should be made on a project-by-project basis, with appropriate consideration for the overall Mars Program objectives, and taking into account not only the probability of catastrophic micrometeoroid impact damage, but the cost of loss of vehicle relative to the cost of such a bumper.

7.1.3 MPL Landing Site Unsurvivable

FAILURE MODE DESCRIPTION

MPL was designed to survive landing site conditions incurring slopes of up to 10 degrees, with a load-bearing strength capable of ultimately imparting at least 222.5 N (50 lbf) to any of the three landing leg pads, and free of rocks or other obstacles taller than 35 centimeters. Terrain exceeding these limits could potentially overturn the lander or cause damage to the lander's undersides or internal components. Additionally, the lander must control its azimuthal orientation on landing to achieve the desired orientation for maximal solar power and MGA articulation range of motion. Nominally, this is achieved by the control system prior to touchdown (to within an accuracy of 5 degrees). However, unforeseen conditions on the surface (for example, loose material at the surface covering a hard, frozen subsurface) could compromise this requirement, causing the lander to "spin out" on touchdown and come to rest in an orientation incapable of achieving MGA downlink on the first sol. This would prevent the lander from generating enough power to survive until the UHF contact attempt two sols later.

FINDINGS

The pre-launch test program appears to have adequately demonstrated that the lander could survive the specified landing conditions without damage to the structure and that the terrain would not result in the lander tipping over. Verification that azimuthal rotations will be achieved on touchdown was shown by analysis, not test, with certain surface properties assumed. Definitive statements regarding whether or not the specified landings were actually achieved at touchdown cannot be made.

The laser altimeter data from MGS indicate that the large-scale (100-meter footprint) slopes are much less than 10 degrees in the MPL landing ellipse. The exception is a large depression that covers 5 to 10 percent of the landing ellipse; this depression appears to contain slopes greater than 10 degrees. Furthermore, these data do not preclude the possible existence of steeper local slopes on the scale of the lander. Thermal-emission data from MGS also indicate that the surface of the landing site is covered with a material that has a low thermal inertia, typically indicative of loosely packed material. The thickness of this material cannot be definitively ascertained, although the MGS data suggest that it uniformly covers most of the surface to a depth of at least 1 centimeter. The presence of large rocks on the surface, which cannot be ruled out via the MGS imaging data, is deemed highly unlikely on the basis of remote-sensing thermal-inertia data.

PROCESS ASSESSMENT

The validation of lander survivability, given all known data regarding the landing site, appears to have been adequate. The lander design relies upon achieving a preferred azimuth attitude orientation in order to generate adequate power for the entire mission. The MGA's limitations could also preclude immediate contact once on the surface.

LESSONS LEARNED

On the basis of the intrinsic limitations of orbital remote-sensing data, the decision as to whether or not active hazard avoidance is warranted should be made on a project-by-project basis. Appropriate consideration should be given to the overall Mars Program objectives. The cost of the loss of vehicle relative to the cost of developing and qualifying such a system should also be considered.

The inclusion of a low-gain transmit antenna provides an added degree of robustness against the loss of communications due to spin out at touchdown. However, this does not provide protection against rotations large enough to compromise the lander's ability to maintain positive energy balance.

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

FAILURE MODE DESCRIPTION

At approximately 1.2 kilometers above the surface of Mars, the lander determines that it is at an appropriate altitude (based on residual velocity) to begin its propulsive terminal descent and releases itself from the backshell/parachute assembly. If the backshell/parachute assembly comes to rest in close proximity to the lander after it has completed its propulsive descent to the surface, the lander may be damaged and unable to complete its mission. For example, the lander would not be able to deploy mechanisms such as the solar array, MGA, and the science masts/arms.

FINDINGS

Simulation of the descent of the backshell/parachute assembly — conducted independently by teams at NASA LaRC/JPL and LMA — indicate that it is possible, although not likely (<1-percent probability) that the backshell/parachute came to rest on the surface of Mars in close enough proximity to allow the parachute or its riggings to drape over the lander. The probability of the backshell structure itself recontacting the lander on the surface is considerably smaller (recontact prior to touchdown of the lander was also analyzed and shown to be implausible). The simulation shows that the timing of events is such that the backshell/parachute assembly would be on the ground and potentially draped over the lander prior to any of the deployments autonomously commanded by the lander.

PROCESS ASSESSMENT

The possibility of this occurring was not seriously considered or analyzed until after EDL. No analysis was performed to characterize the likelihood of such an event; therefore, no design modifications were considered to mitigate this failure mode.

LESSONS LEARNED

Future lander projects should consider some mechanism or maneuver to increase the horizontal separation distance between the landing sites of the lander and the parachute/backshell, if this can be done without increasing other mission risks to a probability higher than what has been identified for this mode.

Bibliography

Analysis of MGS/MOC Observations of the Mars Polar Lander (MPL) Landing Zone, Michael Malin, February 24, 2000, HTML Publication.

Analysis of MGS/MOC Observations of the Mars Polar Lander (MPL) Landing Zone — Supplementary Data, Michael Malin, March 7, 2000, HTML Publication.

CG Offset Effect on Landed Location — Willcockson and Wynn, January 26, 2000, viewgraph presentation to Environment and Landing Site Review Team at LMA, February 1, 2000.

Heatshield Review — Ron Turner, February 1, 2000, viewgraph presentation to Environment and Landing Site Review Team at LMA, February 1, 2000.

Heatshield Structure Pinhole Arc Jet Testing — Jan Thornton, February 1st, 2000, viewgraph presentation to Environment and Landing Site Review Team at LMA, February 1, 2000.

Lander/Backshell Recontact Analysis, MPL/DS2 Mishap Investigation — Spencer (JPL), Desai, and Queen (LaRC), February 1, 2000, viewgraph presentation to Environment and Landing Site Review Team at LMA, February 1, 2000.

MOC Photoclinometry — Mike Malin, 1/24/2000, viewgraph presentation to Environment and Landing Site Review Team at JPL, January 24, 2000.

MPL Area Analysis of Pulse Widths [from MGS MOLA] — Maria Zuber to Casani, Whetsel, Murray, and MacPherson, February 6, 2000, e-mail correspondence.

MPL Entry Risk Status Report — MacPherson et alia, November 19, 1999, viewgraph presentation to JPL MPL EDL Red Team.

MPL Lander to Backshell Clearance — Bill Willcockson, February 1, 2000, viewgraph presentation to Environment and Landing Site Review Team at LMA, February 1, 2000.

MPL Landing Estimates — Phil Knocke, January 13, 2000, viewgraph presentation to Environment and Landing Site Review Team at LMA, February 1, 2000.

MPL Maneuver Overview — Phil Knocke, January 13, 2000, viewgraph presentation to Environment and Landing Site Review Team at LMA, February 1, 2000.

MPL Small Forces Issues — Stu Spath, January 19th, 2000, viewgraph presentation to Environment and Landing Site Review Team at LMA, February 1, 2000.

MPL/DS2 Aero Environment Splinter, Entry Body Mass Properties — Kim Barnstable, February 1st, 2000, viewgraph presentation to Environment and Landing Site Review Team at LMA, February 1, 2000.

MPL/DS2 Review — Environment Review Team Session #1 Agenda — Charles Whetsel, January 24, 2000.

MPL/DS2 Review — Environment Review Team Session #2 Agenda — Charles Whetsel, February 1, 2000.

Presentation — MPL Aeroshell Environments and TPS Design, — Willcockson, Edquist, and Thornton, February 1, 2000, viewgraph presentation to Environment and Landing Site Review Team at LMA, February 1, 2000.

Re: Actions from 1/24 MPL/DS2 Landing Site Splinter, Ken Herkenhoff to Charles Whetsel, March 7, 2000, Email Correspondence.

Re: MPL Landing Site... [Absence of Terracing] — Tom Duxburry to Charles Whetsel, February 11, 2000, e-mail correspondence.

TCM-5 Rationale – Cross-track Capability — Phil Knocke, February 1, 2000, viewgraph presentation to Environment and Landing Site Review Team at LMA, February 1, 2000.

7.2 MPL Mechanical Systems

INTRODUCTION

This section summarizes the failure mode examinations and findings of the Mechanical Systems Review Team. The reviews were conducted in two main parts: first, two full days of meetings with LMA mechanical systems engineers at Denver on 19–20 January 2000. The second was a 5-hour teleconference on 3 February to review follow-up actions produced from the 19–20 January meetings. Several additional teleconferences were held to cover various related subjects. Meetings and teleconferences were conducted with hardcopy presentation charts (see Bibliography).

7.2.1 Lander/Aeroshell Fails to Separate from Cruise Stage

FAILURE MODE DESCRIPTION

This failure results in the catastrophic entry and descent of the unseparated cruise stage and the lander/aeroshell. The following sub-failures lead to the primary failure:

a) Release nut fails to release bolt. There are six release nuts at this interface. This failure can be caused by other specific failures in nut mechanical actuation, NSIs, pyro cabling, or pyro electronics.
b) Push-off spring fails (broken spring). Insufficient separation spring force.
c) Separation connector/ESD cover and/or other drag forces/energy exceeds separation spring forces/energy.
d) Cold welding of aluminum-to-aluminum interfaces.
e) Mechanical hang-up between separating hardware.

INTRODUCTION

The Mechanical Systems Review Team met with LMA engineering on 19 January 2000. Materials handed out at this meeting, as well as other materials gathered at subsequent meetings and via e-mail, are listed in the Bibliography. All the failure modes were examined. Follow-up actions were produced at this meeting and subsequently closed.

FINDINGS

The cruise stage separation simulation shows that, under stacked worst-case conditions, the separating rings may have one glancing contact during the first inch of separation travel. This contact occurs with one 50 percent failed push-off spring and maximum differential connector pull forces. In this case, separation is fully successful. LMA has analyzed the potential contact to ensure that this condition does not prevent separation. There is no hang-up. Connector pull forces used in the analysis were twice the magnitude of forces measured in connector qualification tests on MSP '98 and '01. Nominal separation conditions, which include worst-case differential connector pull forces, produced no contact between separating bodies. No condition was found that would prevent separation or damage hardware. Cruise stage separation velocity is 4 inches per second.

There is a momentary, small, negative force balance between connector pulls; however, the energy balance at this point is generous. The separation joint energy margin is 1.4. This momentary condition is judged to be acceptable.

There are six equally spaced release nuts and push-off springs at the flanged ring separation joint. Two diametrically opposite ITT Canon connectors are differentially lanyard-pulled at 0.3–0.6 inch and

0.5–0.8 inch of separation travel. There are also two hard-mounted RF connectors. The MPL ATLO system separation test verified that the connectors separate properly.

The release devices are 1/4-inch Hi-Shear nuts. These are highly reliable devices with substantial flight history. Lot acceptance and qualification tests of the devices were performed. The flight separation nuts were tested during the system-level deployment and separation tests. A release nut failure is unlikely. However, given that one of the release nuts failed to release its bolt, there is enough structural compliance to allow push-off springs to open the separating rings by the amount necessary to release at least one DS2 probe. Push-off springs were test verified for force and stroke during system-level separation tests. Springs were load tested and cycled at the component level.

Potential cold welding of the 2219-T851 chromate, conversion-coated aluminum surfaces at the separation interfaces was found not to be credible. Low compressive loads and conversion surface film prevent cold welding. An LMA materials expert made the presentation; the JPL materials expert was in agreement.

A system-level, quasi-static separation test was conducted over the full range of separation distance using live pyro firings and flight separation devices. These ATLO tests verified flight connector and spring forces, and separation clearances. There were no interferences or anomalies. Separation clearances open up quickly after the first inch of travel.

Margins for the separation system and its components are adequate.

PROCESS ASSESSMENT

The design, analysis, and verification process for this separation joint was more than adequate.

LESSONS LEARNED

For future designs, providing more radial clearance between the separating rings to avoid any possibility of glancing contact would be an improvement.

7.2.2 Center-of-Mass Migration Due to Mechanical Shifting

FAILURE MODE DESCRIPTION

A lateral migration of center of mass beyond requirements produces mission-critical aeroshell entry dynamics: skip-out, too steep, excessive coning, etc. The question here is: Are there credible failure modes for mechanical displacement of hardware that could account for center-of-mass shifts large enough to produce apparent loss of mission? *Note:* Center-of-mass shift due to propellant migration was reviewed by the Propulsion and Thermal Review Team.

INTRODUCTION

The Mechanical Systems Review Team met with LMA engineering on 20 January to review this mode. LMA made the presentation; there were no follow-on actions.

FINDINGS

For significant center-of-mass migration due to mechanical shifting to take place, component structural failure and displacement must occur. Various hypothetical mass properties cases were examined and no credible scenario was found. All inserts were pull tested and structure was static tested. Center-of-mass uncertainty due to heatshield-to-backshell hole tolerances represents the largest plausible mass moment shift. This uncertainty has already been accounted for in the mass properties predictions. No failures of this nature were evident during cruise.

PROCESS ASSESSMENT

The structural design, testing of the system, and mass properties analysis used in mitigating this failure mode were found to be acceptable.

7.2.3 Parachute Fails to Deploy and Inflate

FAILURE MODE DESCRIPTION

This failure can be caused by any of the following:

a) Mortar fails to fire/deploy.
b) Mortar cover fails to separate.
c) Parachute fails to inflate.
d) Parachute fails to sustain loads.

INTRODUCTION

The Mechanical Systems Review Team met with LMA engineering on 20 January to review this mode; LaRC participated via telephone. LMA made the presentation. All the failure modes were examined. Prior to this meeting, a parachute design consultant from NASA LaRC interviewed cognizant LMA engineers, and the report "Justification for Non-Standard Disk-Gap-Band (DGB) Parachute on Mars Pathfinder Project" (document ME-2589-Rpt., Rev. A) was reviewed.

FINDINGS

1. Mortar fails to fire/deploy — The mortar gas generator was qualified for Mars Pathfinder and MPL. It has dual NSIs and is a highly reliable system. The reliability of the gas generator and mortar to deploy the parachute is high. The energy margin provided by the gas generator to deploy the parachute is high.

2. Mortar cover fails to separate — The only difference between the MPL mortar system and the Mars Pathfinder mortar system is that from Mars Pathfinder to MPL the cover thermal protection was changed from Sirca to SLA-561. The mortar cover is held in place by three screws, which tear out when sufficient force is generated by the mortar deployment. The energy provided by the mortar deployment is several times that required to remove the cover and screws. This same mortar cover design has been deployed literally dozens of times without failure.

3. Parachute fails to inflate — The MPL parachute was a true heritage item from Mars Pathfinder. The only difference between the two parachutes was that the Mars Pathfinder logo was removed from the MPL chute.

   The parachute is a disk-gap-band (DGB) design. The original Mars Pathfinder design was based on the Viking design, scaled down and modified. The modifications were made because the lateral oscillations of the Mars Pathfinder lander beneath the chute were considered to be unacceptable (up to 24 degrees) for the firing of the Mars Pathfinder rocket-assisted descent (RAD) rockets. The modification consisted of widening the band beneath the gap, which decreased the lateral oscillations to an acceptable level.

The deployment conditions for the MPL parachute are estimated to have been between M 1.7 and 1.85, and at a dynamic pressure of between 440 and 564 N/m^2. It should be noted that the entry ballistic coefficients of the Mars Pathfinder and MPL configurations are almost identical (62 to 63).

Neither the Mars Pathfinder nor the MPL parachutes underwent any high-altitude supersonic deployment qualification tests. Such deployment qualification was done by similarity with the Viking design. Deployment Mach number was qualified by similarity up to M 2.3. A panel of parachute experts was surveyed to determine if any of these experts had reservations about using the modified DGB parachute, and what, if any, additional tests they would recommend. Three out of nine recommended high-altitude (supersonic) deployment tests either in flight or in a wind tunnel. This survey is documented in the report, "Justification for Non-Standard Disk-Gap-Band (DGB) Parachute on Mars Pathfinder Project," document ME-2589-Rpt., Rev. A, written by the Pioneer Corporation.

The Mars Pathfinder program did, in fact, perform a series of low-altitude, subsonic deployment tests, which were all successful. MPL also performed three successful deployment tests, including one at nearly five times the expected MPL deployment dynamic pressure of 2700 N/m^2.

The packing and installation in the mortar canister was performed by the same individual that packed the Mars Pathfinder chute.

4. Failure of the parachute to sustain loads — As previously stated, the MPL parachute design was tested at approximately five times the MPL deployment dynamic pressure.

PROCESS ASSESSMENT

The design of the Mars Pathfinder/MPL parachute was acceptable. Regarding qualification testing, although the low-altitude, subsonic deployment tests were highly successful and qualified the parachute for dynamic pressure and snatch loads, uncertainty still exists regarding the supersonic deployment performance and stability of the parachute. The qualification program was lacking in this regard.

LESSONS LEARNED

There is a small chance, however unlikely, that the MPL parachute did not inflate properly due to supersonic inflation dynamics and failed to decelerate the lander. A more comprehensive qualification program using either analysis (CFD) or test (actual design configuration and expected supersonic deployment conditions) would reduce the risk of this type of failure.

It is recommended that future missions conduct representative flight qualification tests wherever possible, unless compelling analysis or modeling strongly convinces the program to do otherwise.

7.2.4 Heatshield Fails to Separate from Backshell

FAILURE MODE DESCRIPTION

This failure prevents the lander from separating from the backshell. A recontact of the heatshield with the lander/backshell causing critical damage to the lander, or preventing its subsequent separation from the backshell, is an associated failure mode. The following sub-failures lead to the primary failure:

a) Release nut fails to release bolt. There are six release nuts at this interface. This failure can be caused by other specific failures in nut mechanical actuation, NSIs, pyro cabling, or pyro electronics. The Avionics and Flight Software Review Teams verified performances requirements for power.

b) Separation springs fail to provide required separation force/energy (failed spring).

c) "Stiction" forces of Furon foam between separating surfaces larger than modeled and prevent separation (see page 4.4.2-13 of Entry and Descent Separation Analyses and Tests, LMA document VR022).

d) Simultaneity between the last two release nuts fired exceeded 20 milliseconds, causing structural failure/hang-up at the last attachment fitting. The Avionics and Flight Software/Sequencing Review Teams verified simultaneity.

e) Aerodynamic coupling force and suction force between separating heatshield and backshell potentially larger than expected, or incorrectly modeled, allowing recontact of heatshield and subsequent critical damage to the lander (see page 4.4.2-11 and 4.4.2-13 of LMA document VR022).

INTRODUCTION

The Mechanical Systems Review Team met with LMA engineering on 19 January 2000. LMA presented the material. All failure modes were presented and reviewed; follow-up actions were closed.

FINDINGS

An analytic simulation model was used for verification of heatshield separation. MPL relied on the Mars Pathfinder engineering development unit (EDU) heatshield separation test and the correlated modeling approach. Stacked worst-case configuration of parameters was used in analysis (wind gust, one spring failed, maximum/minimum dynamic pressures, aerodynamic coupling, suction, and maximum stiction). Analysis showed that worst-case for separation of the heatshield occurs at minimum dynamic pressure. The net static force margin is 1.1. The analysis also shows no recontact. The separation model was checked by an independent analyst.

A system-level, first-motion heatshield separation test was not performed and the release nut NSIs were not fired. Although this test was planned to be performed along with all other system deployment tests, late concerns about possible damage to the fragile TPS, high confidence in separability of the joint, and reliance on the Mars Pathfinder EDU heatshield separation test resulted in this test being cancelled. To mitigate the loss of system-level verification, two things were done. First, a bench test of one of the six separation modules using all of the active separation components was successfully completed. This test imposed worst-case loads as boundary conditions. Second, the pyrotechnic circuits were checked for continuity. Since the NSIs were potted onto cabling pigtails, no pyrotechnic firing at the system level was done.

Deletion of the system-level, first-motion separation test compromised the verification process and was inconsistent with performing that test on every other deployable element. The generally accepted method for verification of separation joints is to perform a full-up, system-level, quasi-static separation test. Early attention to ground handling test support equipment and lander test configuration would have made this test deletion unnecessary.

The heatshield was easily installed and removed several times during MPL ATLO. This is a relatively uncomplicated separation joint, with generous clearances.

Stiction test results were conservatively applied to separation analysis. Furon foam configuration on the MPL heatshield was identical to Mars Pathfinder. Separation interface configuration and materials were identical to Mars Pathfinder. A stiction force eight times larger than the modeled value would have been required to prevent separation.

Twelve separation nuts were fired during lot acceptance. No live firings were conducted at system level. A component-level test of one separation nut/spring/fitting assembly was performed. The same release and push-off devices were used on Mars Pathfinder.

The hardware design was straightforward and the component verification process was acceptable. The separation analysis and margins were acceptable.

PROCESS ASSESSMENT

Deletion of the system-level, first-motion separation test compromised the test verification process. Otherwise, the separation system design and component verification process was well done.

LESSONS LEARNED

For future missions, perform a system-level, first-motion heatshield separation test.

7.2.5 Legs Fail to Deploy

FAILURE MODE DESCRIPTION

This failure could result in the lander not surviving touchdown, or in the overturning of the lander and subsequent inoperability of the UHF antenna, MGA deployment and pointing, solar panel deployment, etc. Some of the failures causing the primary failure on any leg are:

a) G&H release nut fails to release bolt.
b) Leg or stabilizer deployment spring fails.
c) Retarding forces/energy during leg and stabilizer extension are larger than available spring forces/energy (for instance, friction at temperature and aerodynamics).
d) Leg or stabilizer latch fails to engage.
e) Leg hardware was incorrectly disassembled/reassembled for final stow, thereby preventing deployment.
f) Interference with adjacent hardware in stowed configuration prevents deployment.
g) Deployed and latched leg does not carry design loads.

The Mechanical Systems Review Team met with LMA on 20 January. LMA engineers made the presentations. All failure modes were examined; follow-up actions have been closed.

FINDINGS — TOUCHDOWN SENSOR

A review of previous EDU testing showed that during development testing of the legs, two deployment tests were performed in which the touchdown sensors were monitored. During the test, no sensor triggering was observed on any of the three legs. The leg springs were redesigned to improve latching by increasing the deployment force. Following redesign, another deployment test was performed, during which two of the three legs triggered. See Section 7.7.2 for further details.

FINDINGS — LEG DEPLOYMENT

EDU leg mechanical qualification testing was complete. Testing included drop tests, lateral loads, descent vibration, deployment and latching, touchdown sensor actuation, and overturning stability. Flight leg testing included static loads, thermal cycling, deployment and latching, touchdown sensor actuation, and overturning stability. Flight legs were successfully deployed at qualification cold temperature and under adverse gravitational loading of 0.7 g.

The flight legs were successfully deployed during MPL ATLO system test. This test included pyrotechnic firing of release devices and manual actuation of touchdown sensors. The worst-case deployment energy margin = 3.7. This margin is robust. Static test load factor was 1.1 times 35 g's. Structural elements showed positive margins. The design, analysis, and test verification process for the legs was found to be adequate.

Possible loading of the propulsion lines due to the potential stowed stabilizer strut to P-clamp grommet interference was evaluated when the issue was discovered at Kennedy Space Center. The evaluation determined that launch loading of the stabilizer could induce a deflection of the descent thruster feed manifold of 0.064 inch. The analysis included a load uncertainty factor of 1.25, and no compliance from thermal blankets or P-clamp grommet where interference was likely to occur. Applying all worst-case assumptions to the potential interference resulted in acceptable loading of the propulsion manifold and thruster feed tubing. This potential interference is in a configuration that would not impede deployment of the stabilizer.

PROCESS ASSESSMENT

The touchdown sensor spurious signal was a known characteristic of leg deployment. The design and verification process for the touchdown sensor was satisfactory.

There are no concerns relative to the successful deployment of legs, the actuation of the touchdown sensors, or the ability to withstand the design landing loads and stability. The design is satisfactory and has adequate margins. The design verification process is acceptable.

LESSONS LEARNED

Electrical interfaces between mechanical and electrical sensors and software must be specified and controlled as part of the system design process.

7.2.6 Lander Fails to Separate from Backshell

FAILURE MODE DESCRIPTION

This failure would result in the lander/backshell crashing on the surface. The following sub-failures can lead to the primary failure:

a) The two release nuts adjacent to the guide rails are fired before the release nuts at the other two locations; i.e., firing sequence is backwards.

b) The simultaneity between firing the last two nuts at the guide rails exceeds the 10-millisecond requirement.

   Note: Failures a) and b) can result in large loads at the guide rails, which would retard separation.

c) Release nut fails to release bolt. There are four release nuts at this interface. This failure can be produced by other failures: nut does not actuate, NSIs fail to provide required energy, electrical pyro cabling is damaged, and pyro electronics fail to meet power requirements.

d) Push-off springs fail to provide the required separation force/energy (failed spring).

e) Separation connector drag forces are high enough to prevent separation.
f) Friction coefficient between sliding backshell guide rod and lander guide tube was unconservatively determined or modeled. Degraded condition of guide rail surfaces produces retarding forces, which prevent separation.
g) Cold welding between interfacing surfaces prevents separation.
h) Larger than predicted bending moments and deflections applied to guide rails during separation result in retarding forces high enough to prevent separation; separation model parameters were unconservatively defined and/or modeled.
i) Interference during separation between backshell and lander, caused by larger than predicted lateral shear deflection and/or angular tip-off rotation, prevents separation. Separation model parameters unconservatively defined and/or modeled.

INTRODUCTION

The Mechanical Systems Review Team met with LMA on 19 January 2000. LMA engineers made the presentations. All the failure modes were examined; follow-up actions have been closed.

LMA identified and presented the following additional sub-failure mode: The Framotome lander separation connector lanyard fails due to higher than expected connector pull forces, or less than expected lanyard load capability. The connectors would be pulled apart in this case by the extended backshell connector cabling. The lander could be beyond guide rail engagement when the anomalous disconnects occur. This would cause higher than predicted retarding forces and higher than predicted transverse angular tip-off rates.

FINDINGS

The proof test data for the Framotome connector lanyard were not available to verify lanyard capability. As a result of the review action, LMA completed lanyard proof tests and extensive connector pull force tests at ambient and predicted cold temperature. Test results showed acceptable lanyard strength margins and upper bound connector pull forces.

Framotome connector separation pull tests for the MSP '01 project, performed at –100 degrees C, produced significantly larger separation forces than were measured in the MSP '98 Framotome connector pull tests. The MSP '01 project Framotome test results, with a generous factor of two, have been applied to the MPL lander separation analysis. The initial MPL tests did not adequately measure connector pull force and, therefore, did not verify the design function.

On 5 February 2000, the separation analysis was updated to include the current upper bound estimate of Framotome and Canon connector pull forces. Even with larger than expected connector pull forces or a Framotome lanyard failure, the large net force and energy margins make failure to separate the lander unlikely.

The absence of a Framotome lanyard proof test or other bounding analyses and the subsequent establishment of lanyard pull-force margin compromised the pre-launch design verification process.

The guide rails are used to align the separating bodies during the first 11 inches of separation travel. The design required these to prevent contact between close-proximity hardware. EDU quasi-static separation tests verified guide rail performance parameters, including moments and friction. Guide rail tests used the design requirement for parachute angle to backshell of 6 degrees, as compared to the nominal estimate of 2.5 degrees. The test set-up was fixed rather than free–free. This is conservative and would produce larger induced moments than could be expected in flight.

Analytic model simulation was used to verify separation under worst-case conditions. The model used test verified push-off spring forces, connector drag forces, REM seal disconnect forces, and guide rail moments. The analysis methods used in verifying the dynamic separation were acceptable and conservative.

A flight system-level quasi-static separation test was successfully performed using live pyro release nut firings, push-off springs, separation connectors/lanyards, and REM seals, over the full distance of guide rail engagement. Force versus displacement measurements were taken throughout the separation travel. Predicted minimum clearances were visually verified.

There are large separation force and energy margins. A factor of three times the conservatively modeled retarding forces is required to stop separation. High margin is due primarily to the work of Mars gravity.

Separation nuts and push-off springs (four each) are high-reliability components and were adequately qualified.

PROCESS ASSESSMENT

The verification process for validating the Framotome connector pull force and lanyard capability was not satisfactory.

The lander separation system is considerably more complex than either the cruise stage or backshell systems. The lander separation system was well designed. Large separation force and energy margins ensure separation. With the exception of the initial Framotome connector force and lanyard proof test verification issues, the verification process for the separation system was satisfactory.

LESSONS LEARNED

Connector pull-force tests at cold conditions should be conducted with fully configured connectors. Include proof test requirements for connector lanyards in vendor specifications, or verify lander performance during qualification tests.

7.2.7 Propulsion Dynamics Interaction with Structure

FAILURE MODE DESCRIPTION

Rupture of propellant lines feeding the descent engines is a potential failure mode. It could be caused by water hammer forces interacting with propellant-line structural supports of insufficient stiffness to prevent excessive deflection of the lines. Excessive deflection of lines produces bending stresses in lines and fittings which, when added to propellant pressure stresses, could cause rupture. (See also Section 7.5.10.)

INTRODUCTION

The Mechanical Systems and Propulsion and Thermal Review Teams jointly met with LMA on 20 January 2000. LMA engineering presented the materials; follow-up actions were closed.

FINDINGS

The descent engine cluster structural attachment to the spacecraft was acceptably designed and analyzed, with adequate margins.

Late changes in the descent engine duty cycle increased the dynamic interaction with the propellant tubing support system. This produced larger deflections and bending stresses in the tubing than the system had been designed and built for. This condition was addressed and resolved while the flight spacecraft was being prepared for launch at Kennedy Space Center.

The propulsion feed tubing material is 321 annealed stainless steel, a ductile material with good fatigue properties. It work-hardens and is weldable. Tubing is supported by elastomer lined clamps attached to fiberglass thermal isolation brackets. These brackets are attached to the core structure. Strength margins on the support system are satisfactory.

A test-correlated finite-element model (FEM) was used to analyze and predict dynamic loads in the tubing. The model was driven with the worst-case propellant pressure transients. A 1.25 model uncertainty factor was applied to the resulting loads. Damping used in the analysis was conservative relative to the flight installation. A comparison between the approximate method used for the MSP '98 analysis and a more accurate coupled structure fluid analysis showed the approximate method to be conservative in terms of both peak loading and number of cycles.

The model predicted yielding of material at two locations. The minimum ultimate strength margin of safety was positive. A worst-case fatigue analysis was performed at critical welds and showed positive margins above the required four lifetimes of cumulative fatigue effects. All stress concentration factors were applied. Eight weld specimens were dynamically tested with applied reversible bending moments and worst-case mismatch at welds. These data were used in conjunction with other applicable fatigue analysis data.

The configuration of the support system was satisfactory. The support system design stiffness was marginally adequate to handle the final water hammer loads. In this case, robustness at the early phase of the design would have more easily accommodated late developing increases in loads.

PROCESS ASSESSMENT

The propellant lines have the capability to withstand the imposed stresses. The analytic process used to determine loads and validate the propellant line and structural system integrity was conservative and satisfactory.

LESSONS LEARNED

Provide adequate design margin in the propellant line structural support system for all operating conditions.

7.2.8 Landed Solar Array Fails to Deploy

FAILURE MODE DESCRIPTION

Failure to deploy the solar panel adjacent to the MGA would prevent the MGA from scanning. Articulation of the MGA with a stowed panel would probably result in severe damage to the feed and fragile graphite epoxy (Gr/E) antenna. The sub-failures are:

a) Release nut fails to release bolt. There are two release nuts for each panel deployment. This condition can be produced by non-actuation of the mechanical elements of the nut, damaged cabling, and insufficient power from the electrical system.
b) Deployment springs have insufficient force to rotate panel center of mass upward to over center deployment position (spring failure).
c) Blocking of elastomeric material used as deflection limiters between stowed panel faces produces stiction forces large enough to prevent deployment.
d) Power cabling service loop over hinge line produces sufficient retarding torque to prevent deployment.

INTRODUCTION

The Mechanical Systems Review Team met with LMA engineering on 20 January 2000. LMA made the presentation. All the failure modes were examined; there were no follow-up actions.

FINDINGS

The hinge-line monoballs were satisfactorily shielded from surface contamination with felt seals. Several well-simulated, ambient panel deployment tests were conducted. Thermal–vacuum deployment tests were performed with worst-case spring and gravity conditions. Hinge-line deployment torque margins were measured.

Flight system-level solar array deployment tests, including actuation of burnwire release devices, were successfully performed. Qualification and acceptance tests were performed on all mechanical devices. There is no stiction at Furon deflection limiters. The Furon interface surface is separated by Teflon. No contact pressure exists except intermittently during launch. The deployment hardware designs were found to be robust. Deployment margins were adequate. The verification process was complete.

PROCESS ASSESSMENT

The design, analysis, and test verification process was fully acceptable.

7.2.9 MGA Fails to Deploy

FAILURE MODE DESCRIPTION

A failure of the MGA to deploy could result in the loss of telecommunications signal. This could occur if the stowed MGA fails to unlatch or if the two-axis gimbal system fails to articulate.

INTRODUCTION

The Mechanical Systems Review Team met with LMA via teleconference on 3 February to examine this mode. LMA presented the material. There were no follow-up actions.

FINDINGS

The gimbal had a redundant and cross-strapped optic encoder, and redundant stepper motor windings Qualification-level random vibration, static load, and stiffness tests were performed on an EDU two-axis gimbal (TAG). EDU thermal–vacuum and 14× life tests were performed. A protoflight-level random vibration test was performed on the MGA TAG. The MPL ATLO system-level unlatch and full range-of-motion test was performed on the release device and the MGA TAG. There are generous torque margins over the beginning and end of life. Lot acceptance tests of the G&H separation nut were satisfactory. The same MGA gimbal was used on the MSP '98 Mars Climate Orbiter solar array, with no cruise anomalies.

PROCESS ASSESSMENT

The MGA mechanical system design and test verification process was fully acceptable. The functional margins are high.

SUMMARY

The LMA mechanical systems designs were very well executed and verified, and the LMA team was highly experienced and motivated. The quality of the mechanical system–level integration of the spacecraft was outstanding.

The design review process was too hurried to allow LMA engineers sufficient time to reflect on their designs and prepare presentation materials. Also, there was insufficient time for the reviewers to absorb and penetrate the design. During the development process, peer reviews that focused on specific problem areas were very effective.

Bibliography

Entry and Descent Separation Analyses and Tests, LMA document VR022, Lowell Cogburn, 10 December 1998.

Justification for Non-Standard Disk-Gap-Band (DGB) Parachute on Mars Pathfinder Project, document ME-2589-Rpt, Rev. A.

Legs Sensor, 24 February 2000, e-mail message from Lad Curtis.

LMA Comments on MPL/DS2 Loss Review Board report, e-mail from Lad Curtis, to John Casani, 2/15/00.

Mars Polar Lander Premature Descent Engine Termination Due to Touchdown (TD) Indication Conclusions, LMA charts, H. H. Curtis, R. Gehling, J. Bene, G. Bollendonk, February 25, 2000.

Mars Polar Lander Touchdown Sensor Code Issue, LMA charts, H. Curtis, January 20, 2000.

Mechanical Failure Review Splinter — Action Item Review handout package, February 3, 2000.

Mechanical Failure Review Splinter handout package, January 18–19, 2000.

TD Sensor PIE and Involvement, 25 February 2000, e-mail message from Lad Curtis.

7.3 MPL Dynamics and Control

INTRODUCTION

The Dynamics and Control Review Team conducted a careful review of the MPL control system, including hardware elements, algorithms, sequences, software implementations, analyses, and testing. In support of the review process, a number of meetings, presentations, and analyses were performed. The documentation presented and used in the evaluations is listed in the Bibliography. Most items reviewed have been found sufficiently robust that they are considered to be "implausible" contributors to the loss of MPL. However, 11 items were found to require further study, either because of their importance to the EDL sequence, or because of the uncertainty in design margins. The following 11 items are discussed in detail in this section:

- Radar Data Lockout
- Radar–Terrain Interaction
- Inertial Measurement Unit (IMU) Performance
- Model Fidelity
- Inadequate Stability Margins
- Fuel Slosh
- Center-of-Mass Migration/Uncertainty
- Flexible Body Interactions
- Zero Velocity Singularity
- Margin at Minimum Thrust
- Radar–Heatshield Lockup

It was noted that a number of items were not truly failure modes per se, but could lead to effects that result in failure, and are therefore included in the list. These are Model Fidelity, Fuel Slosh, Center-of-Mass Migration/Uncertainty (including nonlinear effects and mixing logic), and Flexible Body Interactions. It is important to note that most of these items were considered by themselves to be an unlikely cause of the loss of MPL. However, a concern exists that the combined effects of the nonlinear pulse-width modulation, fuel slosh, mixing logic, propulsion dynamics (water hammer), etc., each contribute to the erosion of stability margins, and that the true stability margins are unknown.

7.3.1 Radar Data Lockout

FAILURE MODE DESCRIPTION

In this potential failure mode, the Radar Doppler velocity measurements are never used and the system fails to achieve the required low landing velocity at touchdown.

A Mars-relative velocity estimate is initialized before entry and propagated using IMU measurements throughout entry and descent. The first Radar velocity measurement must be within a predetermined threshold of the IMU-propagated estimate or the Radar measurement will be rejected. This test is needed to prevent acceptance of bad Radar measurements. If the IMU estimate has a very large error, however, all Radar measurements will be rejected.

FINDINGS

During pre-launch design and verification, this failure was mitigated by the IMU calibration performed by the manufacturer and verified by the system contractor.

In-flight verification included cruise TCMs and reorientation maneuvers that were performed successfully throughout cruise. This gives a level of confidence that both the accelerometer and gyro modules of the IMU were operating well, though the available data are insufficient to re-verify all alignments and scale factors.

Frequent star update periods in cruise after tens of hours with no stars allow in-flight gyro bias and bias drift calibrations. These exonerate bias drift as a problem unless there was a gyro failure after the final star calibration.

This possible failure mode was investigated extensively in the month prior to Mars entry by the project and the Red Team. As a result of the investigation, the threshold was loosened to decrease the probability of this failure mode causing a problem. The threshold as set is loose enough that, for an IMU performing within specifications, the likelihood of such large IMU propagation errors is statistically remote. This failure mode requires IMU hardware operating significantly out of specification or unexpectedly harsh entry environments.

PROCESS ASSESSMENT

There is no logic in the software that takes corrective action in the event of continuous rejection of Radar measurements. This would have made the design more robust.

LESSONS LEARNED

Use of single measurements can lead to Radar data rejection. Multiple self-consistent Radar velocity measurements should be required before presenting a measurement for comparison with the IMU-propagated velocity estimate.

Added logic to the software could provide corrective action to eliminate the possibility of continuous rejection of Radar velocity measurements.

7.3.2 Radar–Terrain Interaction

FAILURE MODE DESCRIPTION

In this potential failure mode, Radar measurement of sloped terrain produces a biased horizontal velocity measurement. This measurement error can produce horizontal velocities at touchdown that exceed the specification.

FINDINGS

The MPL Radar design makes use of broad radar beams. Based on the measured altitude, the Radar sets narrow time gates on the return pulse and assumes that the direction of the return is that corresponding to flat, level terrain. The actual measurements may be thought of as being made in a coordinate system with a vertical axis perpendicular to the plane of the measured surface. The attitude of this measurement coordinate system is unknown, hence the measurement error.

PROCESS ASSESSMENT

This effect was discovered about a month before landing and the simulations were corrected to demonstrate it. For the MPL system design (including the specifics of Radar measurement cutoff altitude and transition to constant velocity descent), the bias at touchdown is approximately 0.2 meter per second horizontal velocity for each degree of slope at Radar cutoff. This gives 2 meters per second for 10-degree slopes. This effect occurs in regions of slope of large (>50 meters) extent. Pre-launch simulations attempted to include slope effects on Radar measurements, but the implementation was in error such that these effects were not observable in the simulations.

LESSONS LEARNED

Landing areas of small slopes or lower vertical velocity at Radar cutoff should be chosen. This may be accomplished by lowering the Radar cutoff altitude or raising the altitude of transition to constant velocity.

A Radar that does not have vulnerability to landing area slopes should be selected. For example, the Viking lander Radar used small beams, knew which direction the returns came from, and so was able to construct the velocity measurement in the lander reference frame. Another possibility is to study the feasibility of augmenting the NAV filter to be more robust to horizontal velocity errors due to the effect of landing site slope.

7.3.3 Inertial Measurement Unit (IMU) Performance

FAILURE MODE DESCRIPTION

Failure of the IMU to meet the performance requirements results in degraded terminal descent control.

The IMU provides the Guidance and Control System measurements of three axes "total angle" and velocity. From Guidance System initialization at L −15.5 minutes, the IMU performance requirements are:

- Attitude accuracy (per axis) — 0.15 degree, initialization to touchdown (1.5 hours duration from last calibration). Some reduction in accuracy is allowable after entry.
- Velocity accuracy (per axis) — 20 meters per second (from 6000 meters per second) until "Data Validity Check" is made with Radar velocity estimate.

The IMU-propagated attitude affects Radar-determined velocity. The IMU-propagated velocity is mixed with the Radar-determined velocity after acceptance of the Radar data, which are critical to terminal descent control requirements of 2.4 meters per second, vertical, and 1.4 meters per second, horizontal.

FINDINGS

Two units, provided by Honeywell, were launched on MPL. The supplier performed all the inertial instrument quality testing. The performance figures are described in Honeywell document 596-18884R. This is an exceptional IMU. Performance described is within the requirements of the MPL Attitude Control System.

Both units have been used in flight — one at a time, through launch and cruise. The A unit was selected for most of the cruise phase and EDL. Because of the 0.15-degree-per-axis attitude determination requirement, the last IMU calibration sequence using the Star Camera was performed and completed, as planned, 1.5 hours before touchdown. All spacecraft attitude maneuvers and TCMs utilized the IMU for attitude and velocity control and all were successful. All were performed under quiescent conditions. No in-flight calibration of gyroscope scale factor or accelerometer scale factor was performed. Supplier performance data were used.

PROCESS ASSESSMENT

Based on the available documentation, it is believed that the projected performance of this IMU is excellent. The IMU was an excellent selection, well-suited to the task at hand.

LESSONS LEARNED

The IMU calibration update process could be improved by correcting the stray light interference of the Star Camera. This allows IMU calibration without performing turns.

7.3.4 Model Fidelity

FAILURE MODE DESCRIPTION

Incomplete and/or incorrect modeling of the spacecraft and/or of the Mars environment could have resulted in an inaccurate assessment of EDL system performance and of safety margins, which may have been below what is required for a successful landing.

FINDINGS

The MPL team understood the importance of modeling during the design, validation, and testing phases of EDL development, and considerable project resources were used in developing models of different degrees of fidelity and for different testbed environments. These models were incorporated into a Monte Carlo time simulation that becomes the main tool to assess system performance over a large range of system uncertainties.

This large modeling effort, however, may have not been enough to ensure success given the choice in the design phase of some of the system components, such as the propulsion system and the landing Radar, and given some aspects of the design of the Guidance and Control (G&C) algorithms/software, which resulted in a system that was extremely difficult to model and more sensitive to model errors than it might have been. The choice of pulse-width modulation (PWM) for controlling the thrust of the descent engines, while conceptually simple, presented a tremendous modeling challenge that the MPL team responded to with one of the most comprehensive water-hammer modeling efforts in the industry. While the quality of the work involved in this effort was outstanding and the resources invested considerable, it may have not been enough. The complexity of the interactions between the feed system, the thrusters, the structure, the G&C sensors, and the G&C algorithms that the PWM approach creates, practically dictate that the only way of verifying the system with high confidence is with a full-scale closed-loop test of the system. This test was prohibitive from a cost and schedule point of view and it was not done.

In addition, the choice of landing Radar with its broad beams resulted in a system whose performance is affected by the topography of the landing site and the spacecraft attitude, thus requiring for verification a very complex model of the Radar beams and of the Mars surface. The MPL team did not properly understand the technical issues associated with this surface interaction and as a result they used an incorrect model to test the system (see Section 7.3.2). Other aspects of the landing Radar, however, were extensively and properly modeled.

PROCESS ASSESSMENT

While the modeling effort was perhaps not good enough to determine system margins and ensure mission success, the problem lies more with the hardware choices made early in the program, which resulted in a system that was extremely difficult to model and very sensitive to modeling errors, rather than with the commitment and the resources that the MPL team assigned to system modeling. In addition, the rigid allocation for attitude control torques of 10 milliseconds out of 100 limited the robustness of the Attitude Control System (ACS).

LESSONS LEARNED

A full-configuration, closed-loop firing of the descent engines should be performed — or at the very least, a static test should be performed using all the engines firing pulse trains consistent with EDL powered descent. In addition, an extensive model of the landing Radar that properly models the interactions with the terrain should be developed and validated with additional drop tests. Finally, the G&C algorithms should be modified to make the system more robust to modeling errors, in particular in the area of landing Radar data validation, capability to handle unmodeled center-of-mass offsets, parachute dynamics, etc.

During component selection system, engineers should consider the effort and feasibility required to model a particular component as an extremely important criteria in the selection.

7.3.5 Unstable Limit-Cycle Behavior During Terminal Descent

FAILURE MODE DESCRIPTION

This potential failure mode could have resulted from inadequate stability margins due to lack of nonlinear element characterization.

FINDINGS

LMA used "Flowtran" modeling for water hammer, which they correlated with hardware tests (including hot firings). Furthermore, the actual flight code and timing was used for the descent controller. There is no reason to suspect that the simulations performed did not reflect the actual performance of this nonlinear path. It is also probable that the Monte Carlo runs flooded the parameter and timing space.

PROCESS ASSESSMENT

This type of controller must exhibit limit cycle behavior and there was no analytical assessment of its magnitude nor whether the system might "fall off a cliff" to a large magnitude cycle. There is absolutely no evidence of such behavior and such behavior is not suspected, but a nonlinear analysis would yield increased confidence. The MPL descent control loop is very complex and nonlinear. There are few analytical tools to help in assessing the likelihood of unstable limit cycling occurring in such a controller, and the final arbiter must be the highest fidelity simulation possible. One of the key nonlinear paths in the controller is from desired torque to the actual applied torque. This path involves mixing logic with possible saturation, the PWM scheme, the thruster characteristics (including mount flexibility), and water hammer effects.

LESSONS LEARNED

The mathematical technique of harmonic balance has long been used in the analysis of nonlinear systems, e.g., Krylov–Bogoliubov (1934), and is applicable to the desired torque to actual torque nonlinearity. The Describing Function (Kochenburger) technique could be used to characterize this nonlinearity. This should prove useful for future margin assessment.

This technique will not address interactions due to the large amount of energy generated at the PWM frequency, its harmonics, and, with water hammer delays, possibly subharmonics. Nonlinear effects, such as rectification, could possibly translate this energy into sensing within the controller baseband.

The only certain way to eliminate control problems, to say nothing of the other effects of water hammer, etc., is to use a throttle control on the engines. Margins for throttle control are easily assessed and full-range control may be utilized with little complexity.

7.3.6 Fuel Slosh

FAILURE MODE DESCRIPTION

In this potential failure mode, the pulse-mode descent thruster control excites propellant slosh modes in a way that erodes the stability margin of the control system.

FINDINGS

Propellant slosh was not simulated in the design of terminal descent control. Propellant slosh models were developed for use during cruise, but they are not applicable for terminal descent analysis.

PROCESS ASSESSMENT

The modeling that has been done does not rule out the possibility that slosh modes might be at frequencies that could be significantly excited by the 10-Hz, pulsed-mode descent thruster operation. Propellant slosh was not sufficiently addressed during the design to determine its effects on margin erosion. Analyses were performed on the free-tank case, but there was no extrapolation to the diaphragm case for EDL.

LESSONS LEARNED

Model the slosh dynamics in the presence of the diaphragm (supported by test) and assess any control system margin degradation.

7.3.7 Center-of-Mass Migration/Uncertainty

7.3.7.1 Cruise Phase Center-of-Mass Migration

FAILURE MODE DESCRIPTION

This potential failure mode results in an angle of attack that is greater than 1 degree during entry if the cruise phase center-of-mass migration is greater than 2.8 millimeters from the design requirement location. Much larger angles of attack (>2×) could result in atmospheric skip-out, auger-in, or more benignly, large cross-range landing errors.

FINDINGS

Spin balancing of the spacecraft in launch configuration and of the cruise stage was performed. The entry module center of mass was verified by subtracting the cruise stage from launch configuration results.

TCM telemetry was analyzed and, although significant uncertainties still exist, bounds the cruise module center of mass to within 0 millimeter ±3.6 millimeters, indicating that propellant migration was within expectation.

PROCESS ASSESSMENT

The process to ensure that the center-of-mass requirement was met relied on two major components:

1. Pre-flight spin balancing.
2. A propulsion system design that would restrict differential propellant flow between the two propellant tanks during cruise to negligible levels.

Component 1 is accepted practice. Component 2 may not have been valid, since it seems to have been based only on analysis/engineering judgment. (See Section 7.5.4 for details.)

LESSONS LEARNED

Reliance on the Propulsion Subsystem in meeting design requirements critical to attitude control should be verified by testing, if possible. (See Section 7.5.4 for details.)

7.3.7.2 Landing Phase Center-of-Mass Migration

FAILURE MODE DESCRIPTION

This potential failure mode could result from propellant migration prior to and during terminal descent. If the center of mass is more than 22.9 millimeters from the design requirement location, a large moment imbalance generated by 68-percent nominal duty cycle of symmetrically placed descent engines would result. Larger offsets could result in loss of attitude control authority due to exceeding the allocated ±10 percent (±10 milliseconds) off-pulsing budgeted for attitude control.

FINDINGS

The lander center-of-mass requirement was met through a combination of analysis and the spin balance results of the cruise stage. Cruise module spin balance results imply lander center of mass to be within expectations, given that lander analysis is correct. However, significant propellant migration during descent is an unaccounted for possibility.

PROCESS ASSESSMENT

Allocation of control authority margins relative to center-of-mass requirements was inadequate with respect to accepted practice. This can be attributed largely to unsubstantiated confidence in the design of the propulsion system with respect to limiting the amount of propellant migration. See Section 7.5.7 for further discussion of the propellant migration issue.

LESSONS LEARNED

Reliance on the Propulsion Subsystem in meeting design requirements critical to attitude control should be verified by testing, if possible. See Section 7.5.7 for details.

Consideration should be given to designing a more robust control system. In particular, transient behaviors that can temporarily absorb control authority margins should be considered when allocating margins. Such events can include large dynamic disturbances injected into the control system due to mode-switching or events occurring at certain phases of the descent.

7.3.8 Adverse Flexible Body Interaction with Terminal Descent Controller

FAILURE MODE DESCRIPTION

This potential failure mode could result from flexing of the lander structure (excluding propellant slosh, which is covered elsewhere), causing an instability or large errors to accrue by interacting with the control system. Historically, these types of interactions have caused many problems.

FINDINGS

MPL, in the descent configuration (legs deployed), was modeled by LMA using a finite-element model in NASTRAN format. The NASTRAN output for free–free modes up to 100 Hz shows that the lander is very stiff with the lowest mode around 78 Hz and this mode only involves a solar panel in an "appendage" mode, not an "in-the-loop" flexibility. Such a cursory inspection indicates immediately that the gain stabilization of the loop along with the anti-aliasing filters would eliminate flexibility as a problem.

The University of Southern California was contracted to study the NASTRAN data and construct a simulation containing the lower 104 frequency modes. The study concluded that "Linear analysis based on the rigid spacecraft model is adequate for this case" and "flexibility does not cause limit cycling."

The simulation developed in the course of this study (Simulink™) did not include the acceleration loop and thus was not a general-purpose simulation.

Although pre-launch testing and in-flight verification were not performed for this particular failure mode, flexible body interaction (excluding slosh) adversely affecting the controller is an unlikely (implausible) cause for the loss of MPL.

PROCESS ASSESSMENT

Analyses that were done were carefully executed, but determination of true stability margins would have required a more detailed modeling and characterization incorporating a nonlinear simulation.

7.3.9 Zero Velocity Singularity

FAILURE MODE DESCRIPTION

This potential failure mode would occur if the lander vertical velocity approaches zero. Under this circumstance, the gravity turn guidance law would command large pitch and yaw turns to compensate for small horizontal velocity errors, leading to an attitude control instability and/or a landing with a large attitude deviation from the vertical.

FINDINGS

The MPL team was aware of this singularity condition during the design phase of EDL, and they saw large attitude oscillations in the simulations during testing. Consequently, they introduced a design change to make the guidance loop less sensitive to horizontal velocity errors as the vertical velocity approached its minimum value of 2.4 meters per second. This modification was tested and verified through simulations and analysis to be effective down to a vertical velocity of 1.4 meters per second. Vertical velocity is controlled in a closed-loop way, and as long as the control authority can be regulated down below one Mars g (see Section 7.3.10 below), there is no known mechanism for the vertical velocity to go below 1.4 meters per second.

PROCESS ASSESSMENT

Assessment of effects below 1.4 meters per second was not done in sufficient detail.

LESSONS LEARNED

The singularity can be removed totally from the system by stopping the gravity turn guidance law and switching to a proportional guidance law at a certain altitude or vertical velocity. In this way, horizontal velocity is still controlled while keeping the bandwidth of this loop constant and independent of vertical velocity.

7.3.10 Minimum Thrust Margin

FAILURE MODE DESCRIPTION

This potential failure mode would occur if the thrust level required to control to constant descent velocity required a lower throttle setting than is available.

FINDINGS

All pre-launch simulations show adequate margin; minimum expected throttle setting is comfortably above minimum achievable throttle setting.

PROCESS ASSESSMENT

There was a minimum throttle setting command of 25-percent level on all thrusters. More detailed modeling of water hammer and thruster performance shows higher thrust impulse per command setting, meaning less margin above the 25-percent setting. If actual thrust impulse exceeds this model by 10 percent, the system will not be able to set the deceleration low enough to prevent the vertical velocity from being reduced to zero, after which the vehicle would rise instead of fall with respect to the Mars surface. In addition, the control system becomes unstable near zero velocity, and would not be expected to keep the vehicle upright. This is an additional contribution to erosion of control margin.

LESSONS LEARNED

Use proportional throttle valve control or ensure that there is ample margin for setting thrust levels as low as required. This may be achieved by changing the strategy for allocation of thrust on time to deceleration vs. attitude control, or by allowing some thrusters to go to 0-percent duty cycle if necessary.

7.3.11 Radar–Heatshield Lockup

FAILURE MODE DESCRIPTION

In this potential failure mode, the Radar locks up on the separated heatshield. This would cause premature parachute separation, and the lander could run out of propellant prior to touchdown and impact the surface with high velocity.

FINDINGS

During development, it was assumed that the heatshield would fall to the ground quickly or drift out of the field of view of the Radar. The design includes a search limit (accept only returns from >1220-meter distance) that prevents the Radar from locking onto the heatshield for 25 seconds after heatshield release. At 25 seconds, when the heatshield is nominally 700 meters away from the lander, this limit is dropped to 40 meters. A February 2000 study by the Radar supplier indicates that there is greater than 9-dB margin below the signal required to lock up on the heatshield at a range of 700 meters.

PROCESS ASSESSMENT

Although the process for addressing Radar lockup was properly done from a radar perspective, the actual conditions under which lockup could occur were not adequately understood.

LESSONS LEARNED

The maximum distance at which heatshield lockup is possible should be determined. Design the Radar processing algorithm to avoid lockup within this distance.

Bibliography

AACS Algorithm: Entry Navigation Kalman Filter, Report Rev. 2, dated 3/11/98, presented on 01/26/00 at LMA.

AACS Algorithm: Radar Commanding, Report Rev. 4, dated 5/25/99, presented on 01/26/00 at LMA.

AAS Algorithm: Radar Processing, Report Rev. 4, dated 06/23/99, presented on 01/26/00 at LMA.

B3. ACS Lander Hardware Description — Kent Hoilman, 01/25/00, viewgraph presentation at LMA.

CG Offset Effect on Landed Location — Bill Willcockson and Jason Wynn, 01/25/00, viewgraph presentation at LMA.

Collection of Action Item Responses from the Dynamics and Control Review Team meeting on 01/25–26/00 at LMA.

Entry Systems — Bill Willcockson, 01/25/00, viewgraph presentation at LMA.

Entry, Descent and Landing (EDL) Overview — John Cuseo, 01/25/00, viewgraph presentation at LMA.

IMU Descent Vibration Environment — Kent Hoilman and Jim Chapel, 01/25/00, graph presented at LMA.

Integrated Propulsion and GN&C System Modeling and Results; Flowtran Propulsion Modeling — Tim Martin, 01/26/00, model presented at LMA.

Lander Entry State File (LESF) — Tom Kelecy, 01/25/00, viewgraph presentation at LMA.

L-GN&C Subsystem Test/Verification — Tom Kelecy, 01/25/00, viewgraph presentation at LMA.

Mars Polar Lander EDL Attitude Determination — Tom Kelecy, 01/25/00, viewgraph presentation at LMA.

Mars Polar Lander EDL Inertial Navigator — Tom Kelecy, 01/25/00, viewgraph presentation at LMA.

Mars Polar Lander Propulsion System Schematic — John Cuseo, 01/25/00, viewgraph presentation at LMA.

Mars Surveyor Program Landing Radar Overview of Flight Tests and GN&C Interfaces — John Cuseo and Bradley Haack, Report AAS 98-067, presented on 01/25/00 at LMA.

MPS Landing Radar Overview — John Cuseo and Dave Cwynar, 01/25/00, viewgraph presentation at LMA.

Radar Test Review — John Cuseo and Brad Haack, 01/25/00, viewgraph presentation at LMA.

Slosh Model — Philip Good, 01/26/00, report presented at LMA.

Surveyor PDS Analysis — via fax Jim Chapel to Bill Ely and Joe Protola, 01/24/00, presented at LMA.

Terminal Descent Phase Overview — John Cuseo, 01/25/00, viewgraph presentation at LMA.

7.4 MPL Communications/Command and Data Handling

The Communication/C&DH Review Team charter was to review the telecommunication and command and data handling hardware, software, and system interaction to identify failure modes that could have contributed to an unsuccessful landing and/or failure to establish a telecommunications link. The Review Team met with the MPL team at LMA in Denver, Colorado, on 31 January and 1 February 2000.

The LMA personnel were very open, and non-defensively addressed questions raised by the Review Team. They seemed extremely eager to assist the process of fact-finding and brought in additional expertise as required. Additionally, the Review Team focused on design features that could exacerbate failures, making seemingly recoverable faults non-recoverable. Many of these design features could not be used to explain all the observable data.

The operations team did a good job of scheduling and having appropriate telecommunications coverage. The first 36 hours, in particular, had continuous 70-meter DSN station coverage as well as full-spectrum recorder and open-loop receiver backups. The contingency plans were understood and implemented correctly. The personnel for the first ~20 hours were experienced and knowledgeable about spacecraft communication losses.

This section deals with potential failure modes, findings, and Lessons Learned. In the case of the telecommunications links, more that one event is required to preclude communication with either Earth or MGS; for example, going into safing coupled with a hardware failure. One exception is a landed configuration that would not support a link through any of the antennas.

A separate UHF Subteam looked at the Stanford University testing of the UHF link.

The topic of reviews was discussed with the telecommunications team. An inheritance review was done between the JPL transponder engineers and the LMA telecommunications engineers. The waivers and Problem/Failure Reports (P/FRs) were discussed, including the Red Flag P/FRs. As far as peer reviews, what were called "peer reviews" were presented at the Telecommunications Preliminary and Critical Design Reviews, which were at a high level, as would be expected at a subsystem-level design review. As indicated by LMA, these reviews did include engineers from JPL and from suppliers. Table-top reviews that included experienced engineers from outside the project were not done on all the hardware elements.

7.4.1 C&DH Reset During EDL

FAILURE MODE DESCRIPTION

The failure or reset of the C&DH during EDL would be mission catastrophic.

FINDINGS

The unit was environmentally tested (thermal cycling, random vibration, pyroshock) at the component level. It also was installed on the lander during system-level environmental testing. Live pyrotechnic testing was performed at the system level. There was an Unverified Failure Martin Anomaly Reporting System (MARS) written against the C&DH for a processor reset. It occurred prior to the

Pre-ship Review and was never repeated. This MARS was identified by the MPL Mission Safety and Success Team as a residual risk for EDL.

An SEU event might cause a reset of the processor during EDL. Resources were allocated to analyzing the susceptibility of the processor to SEU events and the probability of a reset occurring during EDL. These analyses were tightly coordinated with JPL and the project used their reliability and radiation experts to calculate the risk to the mission. The results of this study indicated that the probability of a mission-ending reset was less than 0.5 percent.

Extensive testing of the EDL sequences was performed on the spacecraft during ATLO and in the STL prior to and during cruise. Six EDL sequence tests were conducted during ATLO (five on the "A" side and one on the "B" side), and two power profile tests were conducted (also running EDL sequences). All eight EDL runs were completed successfully without processor resets.

Several unplanned C&DH prime swaps occurred in the beginning of the mission. After the cause of this problem was identified, the rest of the mission was flown with the "A" unit of the C&DH prime.

More than 100 EDL sequence runs were conducted in the STL, with more than 55 of them conducted within the last two months before EDL alone. These tests were also completed end to end without any processor resets.

PROCESS ASSESSMENT

The component-level environmental test program was a good program. Redundancy is usually included for two reasons: First, it provides a backup so that random failures, which would otherwise shorten a mission can be overcome; second, it increases the availability of the needed functionality in dealing with transient faults during time critical and demanding mission events (such as EDL). The MPL design added redundancy, but did not substantially increase functional availability for dealing with transient faults during critical events.

LESSONS LEARNED

Missions that have time-critical phases should include a single fault-tolerant design to processor resets to increase the probability of success.

7.4.2 EEPROM Errors After Landing

FAILURE MODE DESCRIPTION

A reset of the C&DH after landing could be mission catastrophic under certain circumstances; e.g., sometime after launch, a stuck bit occurs in the prime string flight computer EEPROM. Since there is no parity nor error detection or correction (EDAC) on the EEPROM, the stuck bit or bits corrupts the flight code in the prime string. After landing, fault protection is re-enabled. A pending fault results in a reset and reload of the flight computer. The corrupted EEPROM is read and begins to execute. It is corrupted in such a way that the heartbeat test in the C&DH Module Interface Card (CMIC) is passed, but then resets again. This process occurs indefinitely with no swap to the alternate string. No MGA antenna deployment occurs and commands never enter the lander.

FINDINGS

When the EEPROM code was burned, it was CRC checked to insure that the stored file matched the desired file. Following launch, several string swaps occurred that exercised the EEPROM, with no evidence of a stuck bit.

PROCESS ASSESSMENT

Sometime during flight, a stuck bit in EEPROM could have developed. EEPROM integrity was never verified after launch. A failure of this type could be created. The radiation test data for the EEPROM need to be assessed for its robustness to radiation damage and SEUs.

LESSONS LEARNED

Flight computer designs should include EDAC on the EEPROMs and should fail the load process if the EDAC indicates a double bit error. Critical memory used to store flight code should be protected from the adverse effects of single stuck bit or SEU faults.

7.4.3 CMIC Errors After Landing

FAILURE MODE DESCRIPTION

A reset of the C&DH after landing could be mission catastrophic under certain circumstances; e.g., sometime after launch a bit flip occurs in the CMIC SRAM. This memory is shared by both C&DH strings. The CMIC SRAM is used to store patches to code, which overlay the main program each time the C&DH reloads. There is no parity or EDAC on the CMIC SRAM. After landing, fault protection is re-enabled. A pending fault results in a reset and reload of the flight computer. The corrupted CMIC is read, corrupting the flight code in the prime string. This code begins to execute, resulting in another reset. The CMIC hands control over to the other C&DH string. It powers up and loads its code from EEPROM and then loads the patches from the CMIC. The same corrupted code is transferred into the new string, which then also resets and follows the same path as the previous prime string. This occurs indefinitely, preventing spacecraft control. No MGA antenna deployment occurs and commands never enter the spacecraft.

FINDINGS

When the CMIC code was updated, it was CRC checked to ensure that the stored file matched the desired file. The CMIC patches and files were controlled by the project change process. Even so, the CMIC file list grew from three at launch to over 100 before EDL. Following launch, several string swaps occurred that exercised the CMIC.

The CMIC SRAM is a single, 1-megabit, radiation-hardened part manufactured by Lockheed Martin Federal Systems. The part has a total dose hardness greater than 1×10^{6} rad (Si). The lander total dose at the time of landing would have only been a few krads. The part was tested for SEU immunity at LET >120 MeV/mg/cm^{2} and found to have an error rate of 1×10^{12} errors/bit-day. Assuming that all bits of the CMIC SRAM are written to once (effectively) over the length of the mission, this leads to a predicted error rate of 3.3×10^{4} errors due to SEUs. Thus, stuck bits can only be attributed to hardware failures within the memory elements. When the files are written to the SRAM, the contents are read back and verified against the original file. No errors were detected during cruise during this process. Thus, any failures within the SRAM would have had to occur after the time that the file was placed into memory.

PROCESS ASSESSMENT

CMIC memory integrity was verified prior to EDL. A failure of this type could occur after the pre-EDL verification and not be detected.

LESSONS LEARNED

C&DH designs should have EDAC on the CMIC card. Without this, the design is not single-fault tolerant. Critical data should never be stored in a memory where a single fault can incapacitate both strings.

7.4.4 Power Controller Unit Fails

FAILURE MODE DESCRIPTION

Any common-mode housekeeping power supply (HKPS) failure that affected both power converters would be mission catastrophic at any time. These two potential failures were examined:

1. The loss of either of the diode OR'ed 15-volt power supply rails. The +15 volt and –15 volt outputs of each HKPS are diode OR'ed and then used to drive some logic. This design allows the failure of either supply without loss of the functions using the diode OR'ed output. However, a failure that causes the loss of the diode OR'ed output would eliminate all the functionality tied to this supply.
2. The A/B SEL (Select) line fails such that each Power Controller Unit (PCU) on the HKPS card alternately powers on and off. The A/B SEL line is a single line driven by an OR gate. Toggle faults on this line would be mission catastrophic.

FINDINGS

The PCU design was thoroughly tested pre-launch. Following launch, several C&DH string swaps occurred that exercised the PCU swap logic. After these swaps, no other incidents occurred to test this logic.

PROCESS ASSESSMENT

The schematics for the PCU were reviewed to see if the common 15-volt rails represented a significant risk. In each instance where this voltage was used on the PCU, the voltage was not tied directly to any parts, but was resistor isolated from the components that used this voltage. These voltages are also sent "off-board." However, each client for these voltages used fuses to protect these rails from a short at the point of use. The risk from this type of fault seems extremely low.

The second fault introduces a fault condition that was not addressed by the FMECA. A failure of this type would be mission catastrophic, but not very likely.

LESSONS LEARNED

Eliminate all common-mode failures from the PCU design. Perform a FMECA that covers both stuck-at and toggle faults. Provide a design that allows both strings of the C&DH to be powered at the same time, but that does not require them to both be powered at the same time.

7.4.5 Landed Orientation Prevents Communication

FAILURE MODE DESCRIPTION

In this potential failure mode, X-band and/or UHF link cannot be established due to the landed orientation.

MGA Uplink and Downlink

The MGA should have been able to support 125 bps commanding up to 6 degrees off boresight in the main beam, and a similar angular range for 2100 bps downlink at a 70-meter station. Neither the onboard sequence nor the subsequent post-EDL commands would have selected a different command rate than 125 bps for the MGA. Thus, any pointing-error greater than 6 degrees is problematical for commanding.

If gyro compassing worked, and the MGA gimbals were functional, then the MGA would have been commanded to track Earth throughout the pass. A gyro-compassing error of greater than 6 degrees would be required to preclude commanding. Commanding via the MGA would also be impossible if the landed azimuth was such that Earth was never inside the gimbal space.

On sol 0, Earth was above 10 degrees elevation for azimuth angles of −150 degrees to +75 degrees (in the nominal landing attitude). Earth elevation peaked at ~32 degrees above the horizon. The azimuth and elevation "soft stop" ranges are: −138 degrees < AZ < 51.5 degrees, 2 degrees < EL < 57 degrees. The sol 0 Earth geometry is shown in Figure 7-5.

Since the extent of azimuth variation of Earth above 10 degrees is 225 degrees, and the gimbal azimuth range is 189 degrees, Earth is inside the gimbal range for all landed orientations. However, since the MGA is only tracking Earth for a period of up to four hours in a day, or about 60 degrees of azimuth, there is indeed a range of landing orientations that would keep Earth out of the gimbal space during contact periods.

Assuming a good gyro-compassing solution, the four-hour contact periods should effectively add ±60 degrees to the 189 degrees azimuth range of motion (because of Mars's rotation during the tracking period). In other words, the range of azimuth angles not visible during the MGA tracking period is approximately 360 degrees – 309 degrees = 51 degrees. These would be the azimuth angles directly behind the center of the azimuth gimbal range at –43 degrees, which would put the landing Earth azimuth range for no MGA uplink at approximately 137 degrees ±25. This would correspond to a landing azimuth error of ~180 degrees ±25. As long as the elevation angle off nominal is less than the specified 16 degrees, the "blind" range above should not be affected too greatly.

For downlink, the "blind" zone is similar if no "touchdown power-on reset (POR)" scenario occurs that would kick off the autonomous Find the Earth (FTE) sequence (see Figure 7-6). Otherwise, the Telecom Subsystem would have been configured for carrier-only downlink for the duration of the sequence, which increases the field of view around the MGA to approximately 30 degrees. In carrier-only mode, a downlink signal would almost certainly have been observed from Earth during the FTE sequence, if the landing azimuth error had been less than 36 degrees (6 degrees FTE minimum "pad" plus 30 degrees field of view).

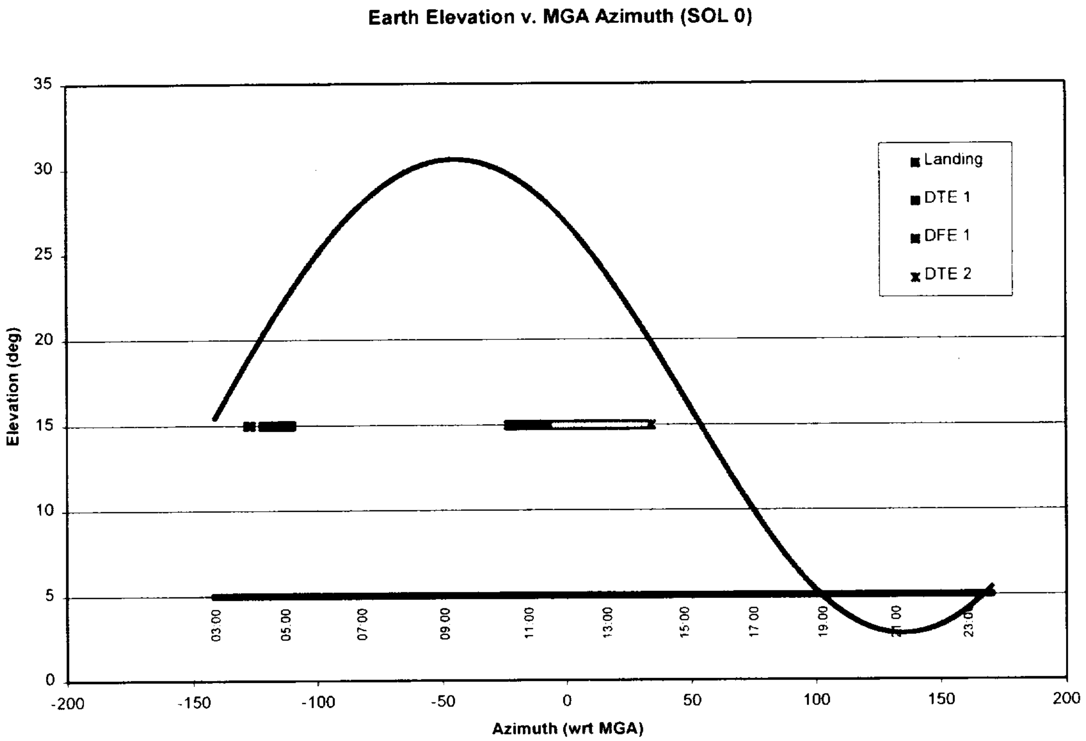


Figure 7-5. Earth Geometry for the Nominal Landing Orientation and Site on Sol 0

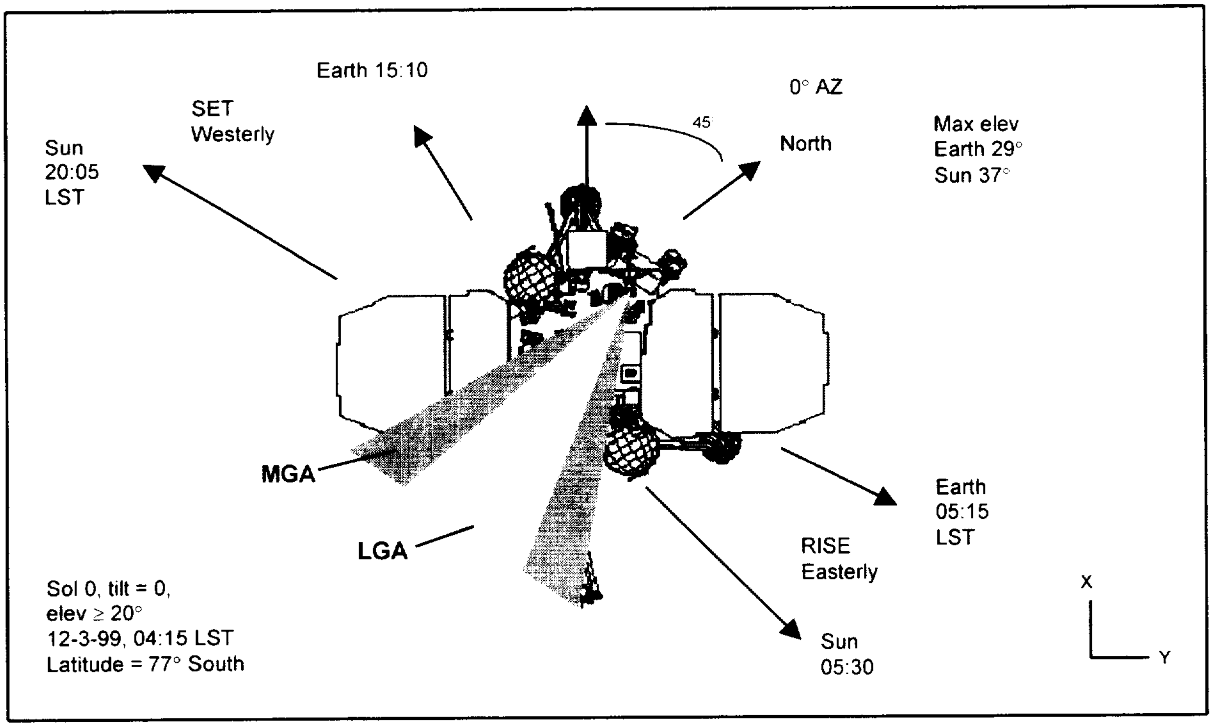


Figure 7-6. Command-Blind Zones in Azimuth for MGA (125 bps) and LGA (7.8125 bps)

Low-Gain Antenna (LGA) Uplink

The LGA is fixed and pointed at the approximate center of the nominal Earth azimuth range. In elevation, the LGA boresight is pointed approximately 43 degrees above the lander deck and the nominal horizon line. The mean Earth elevation angle is approximately 17 degrees above the horizon. In the worst-case azimuth orientation (180-degree error), the mean Earth would be 120 degrees off boresight. At 7.8125 bps, an uplink can be received by the spacecraft at up to 135 degrees off boresight. So there is at least a chance of getting an uplink into the spacecraft in the worst-case azimuth orientation. However, since Earth is frequently at lower than mean elevation, it is probably more realistic to consider a region of ±16 degrees (elevation error) around the worst-case landing azimuth error to be a "command blind" zone.

Only if the onboard sequence is cancelled (stopping the nominal UHF pass) *and* the landing azimuth error puts the lander in the "command blind" zone (see above) would the lander be in a configuration that would not support either an X-band or UHF link. UHF is not especially azimuth sensitive, as long as there is a reasonable elevation angle. The peak elevation angles for the Sequence C UHF passes were 82.8 degrees on DOY 341, 56.5 degrees on DOY 342, and 86.6 degrees on DOY 343.

FINDINGS

It was a project decision not to have a direct-to-Earth X-band link through the LGA. The two downlink paths were to be either through the MGA at X-band direct-to-Earth or the UHF antenna to MCO.

There is a landed orientation in which an X-band uplink cannot be established through the MGA or the LGA. Precluding the establishment of an uplink path requires either a malfunction of the gyro compassing function or a severe rotation of the lander at touchdown.

PROCESS ASSESSMENT

The lack of an X-band LGA downlink was reviewed many times during the project and accepted. This is recognized as a significant limitation; however, without the confirmation of an X-band uplink, it is not clear that even with an LGA the downlink would be detected. There are two aspects to the landed orientation issue: (1) the lander is oriented such that not all antennas are able to support a link, or (2) the lander went into safing at touchdown and the LGA X-band uplink and MGA downlink are pointed outside their view of Earth.

LESSONS LEARNED

Review the antenna coverage and determine under what possible landed orientations a telecommunications link can be maintained. Maximize the configuration to obtain initial link acquisition and engineering health and safety data return.

7.4.6 Coaxial Transfer Switch Fails

FAILURE MODE DESCRIPTION

In this potential failure mode, the coaxial RF transfer switch (S10) fails to transfer from cruise mode to landed mode. There was a MARS written on this type of coaxial switch on MGS for hanging up mid-way between positions. This in itself would result in a loss of approximately 3 dB. Of concern is the failure mode where the switch would not transfer at all as a result of cold welding, for example. The isolation in this mode would be sufficient to preclude an X-band uplink in the landed configuration.

There is also a coaxial RF single pull double through switch (S5) that switches between the LGA and MGA. The failure of this switch to transfer would preclude the use of one of the antennas.

FINDINGS

This same design was used on MGS and MCO, with only the one problem related to the ability to transfer. The unit was environmentally tested (thermal cycling, random vibration, pyroshock) at the component level. It also was installed on the lander during system-level environmental test. The coaxial switch was not exercised during cruise.

PROCESS ASSESSMENT

The problem with this application is that it is only used once at the end of the mission. It is nearly impossible to simulate long storage times in vacuum to verify operation. The materials used in the reed and mating contact are gold-plated beryllium-copper, which addresses the cold weld concern.

The failure of S10 would address the issue of not having a command link to the lander, but would also require the landed configuration to be off Earth point or a failure of a transmitter component with the lander entering safing, resulting in the loss of both X-band and UHF. Likewise, the failure of S5 would address the possible loss of X-band uplink if the remaining antenna could not establish a commandable path.

7.4.7 Failure to Establish UHF Link Between the Lander and Mars Global Surveyor

FAILURE MODE DESCRIPTION

In this potential failure mode, the UHF link cannot be established between the lander and MGS.

FINDINGS

A compatibility test on 31 May 1996 demonstrated compatibility between a Cincinnati Electronics (CE) breadboard UHF transceiver and the CNES MGS Mars Relay (MR) UHF transceiver. An airlink was established by separate transmit and receive vertical whip antennae mounted to railings above the MGS spacecraft. When the CE breadboard completed MR BTTS handshake in RC1, MR indicated a noisy TC. The noisy TC was determined to be the result of the CE breadboard missing an inverter in the convolutional encoder.

A compatibility test on 18–19 July 1996 demonstrated compatibility between a CE breadboard UHF transceiver and the CNES MGS MR UHF transceiver. Successful TC on MR was achieved with the CE breadboard. MR RC1, RC2, RC3, and TC tones were measured with a frequency counter. Failure of the tone detector board required manual operation of the BTTS cycles. The MOC captured 1.5 Mbits and sent to CNES, where 5 of 7 BTTS frames were verified for a BER of 2.8×10^{-5}.

A system thermal–vacuum test operated the UHF with antenna disconnected and verified uplink and downlink via coax.

The MPL UHF transceiver and MGS UHF transceiver hardware were individually acceptance tested.

Post-launch there was a series of tests performed with MGS, a beacon test during cruise, and Stanford tests in Mars orbit. There was also a compatibility test between the CNES MR test set and MPL hardware.

PROCESS ASSESSMENT

It is understood that the original UHF link was supposed to be MCO, and that all the emphasis was on verifying that link. The MGS test could only be run as it was because of the phasing of the two projects. The point of the assessment below is to identify some of the issues that might contribute to the inability to establish a link with MGS.

The compatibility tests performed did not constitute a complete end-to-end MPL/MGS system test for the following reasons:

1. Compatibility was not performed with MPL flight hardware.
2. The CE breadboard used signal generators as frequency references instead of spacecraft hardware.
3. Tone frequencies were verified with a frequency counter, but tone detector hardware failure prevented verification of tone activation of BTTS handshaking.
4. The loss of 2 of 7 BTTS frames without errors is not a reliable result for signal levels used.
5. The BER test was performed at only one uncalibrated signal level of E_b/N_0.
6. Noise was not induced into the link.
7. Testing was performed at ambient temperature only.

It was decided not to risk an uplink to change the C&DH EEPROM for the MR mode as default until after landing. This left a vulnerability of an unusable UHF link if an undervoltage condition occurred before the uplink to change the C&DH EEPROM. Therefore, if an X-band problem occurred, the UHF link would also become unusable.

The UHF link appeared to have been tested in pieces, rather than an overall end-to-end. The "pieces" all appear to be accounted for, and the recent tests with Stanford and MGS were helpful in this accounting.

The MGS-to-lander link margin is approximately 10 dB. If the path loss were of this magnitude for any reason, the lander would not respond with a transmitted signal.

LESSONS LEARNED

1. End-to-end, system-level compatibility tests should be performed for all telecommunication modes.
2. Program in emergency communication modes before they would be required.
3. Consider in-flight verification with onboard checkout and with ground communications.

7.4.8 Transponder Power Supply Fails

FAILURE MODE DESCRIPTION

In this potential failure mode, the Deep Space Transponder (DST) power converter fails. The DST has a single power converter to power the receiver, the command detector unit, and the exciter. The failure of this board could result in the loss of X-band uplink and downlink capability. The prime transponder was the Cassini spare (S/N 004), which had a Red Flag P/FR written against it for an open via on the +6 volts going to the exciter. A jumper wire was installed and the unit temperature cycled 0 degrees C to +65 degrees C for 10 times as the Power Converter Assembly, and to 0 to +55 as an assembled transponder, and no other problem was observed.

FINDINGS

The environmental test requirements were reviewed for consistency between Cassini and MPL. The random vibration, pyroshock, and thermal requirements were different, and the Cassini engineering model (S/N 001) was tested over the MPL ranges. However, the Cassini spare was not environmentally tested at the subassembly level. It was tested as part of lander system-level environmental tests (pyroshock, acoustic, and system thermal–vacuum).

The Cassini spare transponder, which was the prime transponder, was used during cruise with no problems with the uplink or downlink.

In a review of the component-level fault protection, it was determined that a failure in the power converter that resulted in a current draw of <200 milliamps would have resulted in a DST swap, even during EDL. The nominal current level, receiver and CDU only, is approximately 250 milliamps. If the problem of open via occurred such that a secondary voltage to the receiver was lost, the resultant decrease in receiver current would have caused a DST swap. If the open via occurred on the CDU interface, the reduction in current (40 milliamps) may not result in a DST swap.

An inheritance review was conducted and the Red Flag P/FR discussed; however, it was not included with the other program unverified failures at project-level reviews.

PROCESS ASSESSMENT

The Cassini engineering model and spare transponder did go through an inheritance review between the JPL DST engineers and the LMA telecom engineers. The Red Flag P/FR in question was discussed at that time and it was discussed with LMA management. However, it was not presented at major project reviews. If it were, there might have been some discussion as to whether the Cassini spare should be considered as the prime flight unit.

LESSONS LEARNED

The JPL "Standards Document Problem/Failure Reporting System, Guidelines and Procedures" (JPL D-8091) should be updated to include the reporting of all the pertinent Red Flag P/FRs at all project-level reviews.

7.4.9 Medium-Gain Antenna Gimbal Fails

FAILURE MODE DESCRIPTION

Failure of the MGA gimbal would result in the loss of X-band downlink communications.

FINDINGS

MGS had a failure in its gimbal, reducing the coverage the high-gain antenna could achieve. If a similar failure occurred on MPL, there would be no X-band downlink to verify the uplink commanding. No in-flight verification was possible.

PROCESS ASSESSMENT

The information about the gimbal temperature given at the Pre-EDL Readiness Review was that it would be "above minimum qualification temperature." If the temperature was below expected, the gimbal could have stuck in a non-usable region.

While this failure would not have affected the UHF transmitter, colder than expected temperatures could have affected the overall mission.

LESSONS LEARNED

Add an LGA transmit capability as a backup X-band for an emergency downlink function.

7.4.10 Command Detector Unit Fails

FAILURE MODE DESCRIPTION

Failure of the Command Detector Unit (CDU) to process the subcarrier and decom commands would result in the loss of X-band uplink. Because of the way the command loss algorithm was configured, it would not switch to the backup CDU.

FINDINGS

This same design was used on MCO. The unit was environmentally tested (thermal cycling, random vibration, pyroshock) at the component level. It also was installed on the lander during system-level environmental test. There were no MARS written against the CDU performance. The prime CDU was used all through cruise. The redundant unit was not operated in cruise. A DST swap would entail a CDU swap.

PROCESS ASSESSMENT

The component-level environmental test program was a good program. It did not include a vacuum test, but considering the application, this is not considered a shortcoming. The failure of the CDU would address the issue of not having an X-band uplink from the lander, but would also require the landed configuration to be off Earth point for the MGA downlink path not to work. Also, in order not to have a UHF downlink signal, the lander would have had to experience a CDU failure, enter safing at touchdown, and have a pointing problem.

7.4.11 Diplexer Fails

FAILURE MODE DESCRIPTION

Failure of the X-band diplexer could affect the X-band uplink and downlink performance, depending on the failure mode. Of concern is the failure condition that would increase the insertion loss of the diplexer such that its signal levels would be below those necessary to support the link. The diplexer is silver plated. If there were a plating problem that generated particles of sufficient size to short the diplexer, this could cause such a problem.

FINDINGS

This same design was used on MCO. The unit was environmentally tested (thermal cycling, random vibration, pyroshock) at the component level. It also was installed on the lander during system-level environmental test. There were no MARS written against the diplexer performance or noncompliance on performance identified in the end-item-data-package. The lander X-band diplexer was not exercised during cruise.

PROCESS ASSESSMENT

The component-level environmental test program was a good program. It did not include a vacuum test, but considering the application, this is not considered a shortcoming. The failure of the diplexer would address the issue of not having an X-band downlink from the lander, but would also require the landed configuration to be off Earth point for the LGA uplink path not to work, and have either a pointing problem or UHF hardware failure in order not to get a UHF downlink signal. Evaluation of the design shows sufficient gaps and no plating in the threaded tuning holes.

7.4.12 Telemetry Modulation Unit Fails

FAILURE MODE DESCRIPTION

Failure of the Telemetry Modulation Unit (TMU) to modulate data onto the subcarrier and pass it to the DST would cause the loss of data but would not result in the loss of the X-band downlink carrier.

FINDINGS

This same design was used on MCO. The unit was environmentally tested (thermal cycling, random vibration, pyroshock) at the component level. It also was installed on the lander during system-level environmental test. There were no MARS written against the TMU performance. The prime TMU was used all through cruise.

PROCESS ASSESSMENT

The component-level environmental test program was a good program. It did not include a vacuum test, but considering the application, this is not considered a shortcoming. The failure of the TMU would not address any of the observations associated with loss of X-band commandability or X-band downlink carrier.

7.4.13 Solid-State Power Amplifier Fails

FAILURE MODE DESCRIPTION

In this potential failure mode, a failure of the SSPA results in the loss of X-band downlink communications.

FINDINGS

The pre-launch design and verification were robust. In addition, another identical SSPA performed throughout MPL on the cruise stage without incident. No in-flight verification of the SSPA on the lander was possible because of concerns that RF radiation might initiate a pyrotechnic event.

PROCESS ASSESSMENT

There is an issue with this design. There have been a number of units that have exhibited as much as a 1 to 2 dB drop in RF output power. There has been no evidence that this is a life-limiting failure mode. It can be cleared by cycling power on and off. No other issues were identified with the SSPA; it was included for the sake of completeness. This failure would not have affected the UHF transmitter.

7.4.14 Uplink/Downlink Card Fails

FAILURE MODE DESCRIPTION

Failure of the Uplink/Downlink (ULDL) Card could result in the loss of all communications except the X-band downlink carrier.

FINDINGS

The pre-launch design and verification were robust. The ULDL Card operated throughout cruise without incident. The backup ULDL Card operated early in cruise as a result of other fault protection.

PROCESS ASSESSMENT

The inability of the flight software to start the command loss algorithm makes this a potential single-point failure. There was also no single finding that would make this failure more plausible, but coupled with the loss of the MGA (by pointing or hard failure) or the loss of the SSPA, an inability to start the command loss algorithm would completely explain the X-band observables (see Section 7.7.1).

Bibliography

AACS Algorithm: GyroCompass — Handout, LMA Meeting 01/31/00.

Battery power capability — via Kyle Martin e-mail 02/07/00.

Brace Concerns — Handout, LMA Meeting 01/31/00.

C&DH CDR Peer Review, D-14523, dated 12 November 1996.

CMIC_map — Handout, LMA Meeting 01/31/00.

Detection of a Candidate Signal from the Mars Polar Lander — via Richard L. Horttor, 02/17/00, original memo from George Resch to Richard Cook, Mars UHF Signal and Analysis.

Diplexer and bandpass filter plating — via Kyle Martin e-mail 02/04/00.

DST Environmental Comparison MSP98 vs. Cassini — Handout, LMA Meeting 02/01/00.

DST Fault Protection — Lad Curtis e-mail 02/08/00.

EDL Electrical States — Handout, LMA Meeting 02/01/00.

FSW Overview — Handout, LMA Meeting 01/01/00

Fault Protection enable/disable states — via Kyle Martin e-mail 02/07/00 with the following attachments: EDL FP State Changes; MSP_11.pdf Section 11 Component-Level Fault Protection; MSP_12.pdf Section 12 Performance-Level Fault Protection; MSP_13.pdf Section 13 System-Level Fault Protection.

In-Flight Verification of Telecom, C&DH and Flight Software — Handout 6, LMA Meeting 01/31/00.

Lander Configuration After EDL — Handout, LMA Meeting 01/31/00.

Mars Global Surveyor Mars Relay Flight Test Final Report, D-14423, John L. Callas, dated 1997 March 14.

Mars Polar Lander Surface Power Constraints — Handout, LMA Meeting 01/31/00.

Mars Polar Lander Touchdown Sensor Code Issue — Handout, LMA Meeting 01/31/00.

Mars Surveyor Program '98 Fault Protection Description Document, D-14512, dated 5 January 1998.

Microwave component plating — via Kyle Martin e-mail 02/04/00.

MPL software changes and problem reports — via Lad Curtis e-mail 01/28/00.

MPL Telecom Fault Protection Enables/Disables — Handout, LMA Meeting 02/01/00.

MPL Telecom Screen Shots (Telemetry Data) — Handout, LMA Meeting 02/01/00.

MPL Uplink logs — via Kyle Martin e-mail 02/02/00 with the following attachments: MPL UL Log.xls MPL Uplink Log; MPL edl_uplink_sum.xls MPL Uplink Summary — EDL Uplinks; MPL landed_prep_uplink_sum.xls MPL Uplink Summary — Landed Prep Uplinks; MPL FIS Access.doc MPL FIS Access Information.

MPL Uplink Loss Response Timer — Change control package, LMA Meeting 01/31/00.

MSP Landed STV Test Profile — Handout, LMA Meeting 02/01/00.

MSP Telecom Subsystem CDR Peer Review, D-14526, dated 13 November 1996.

Post-Landing Loss of Signal Fault Tree — Handout, LMA meeting 01/31/00.

Results of May 31, 1996 MR Compatibility Test at Lockheed Martin Astronautics, Denver, Colorado, Release July 2, 1996.

Results of July 18–19, 1996 MR Compatibility Test at Lockheed Martin Astronautics, Denver, Colorado, Release July 25, 1996.

RF Switch Materials — via Kyle Martin e-mail of 02/10/00, response from Teledyne re: possible cold welding.

Sequence C — Sequence of Events, Generated December 1 03:20:20, 1999.

SOL 0 and Landed Init Timeline — Handout, LMA 01/31/00.

SOL 0 to SOL 33 Timeline — Handout, LMA 5/6 January 2000.

Spider Architecture — Handout, LMA Meeting 01/31/00.

STL Sequence Runs — Handout, LMA Meeting 01/31/00.

Telecom Overview — Handout, LMA Meeting 01/31/00.

The Extent of the Post-Launch MGS Mars Relay Mode Confirmation, John Callas e-mail, 03/09/00.

7.5 MPL Propulsion and Thermal

7.5.1 Introduction

This section summarizes the findings of the Propulsion and Thermal Review Team. The Review Team convened in early January and was briefed on the design, implementation process, and flight telemetry at two in-depth reviews held at LMA in Denver. Detailed information was collected from phone calls, action-item responses, and project documentation. Six generic areas in propulsion and/or thermal were identified as potential failure mode candidates:

- A Reaction Control System (RCS) propulsion component fails prior to terminal descent.
- A larger than allowable offset in propellant center of mass occurs:
  - Cruise phase
  - Hypersonic entry phase
  - Parachute phase
  - Powered descent phase
- Inadequate thermal control of the Propulsion Subsystem.
- A propulsion component fails during terminal descent (other than caused by water hammer effects).
- A terminal descent propulsion component fails during terminal descent (caused by water hammer effects).
- Adverse thruster plume interactions during terminal descent and touchdown.

The MPL propulsion and thermal personnel were knowledgeable, experienced, and well qualified for the job. However, it appears that the two groups were overworked and did not have enough time to sit back and reflect on critical issues. Further, the coordination and communication between the two groups was not adequate.

From a review of the designs, component heritage, and test programs, it was concluded that the propulsion components would have functioned reliably, even in the severe water hammer environment generated during terminal descent. However, the Propulsion Subsystem and thermal designs did contain four potentially serious, if not catastrophic, weaknesses. These were:

- Descent thruster inlet manifold and catalyst bed thermal control.
- Propellant tank outlet thermal control.
- Propellant migration between tanks during "zero g" cruise and parachute operations.
- Flow control in the parallel branches during terminal descent (this item represents slightly less concern than the first three).

The first of these was discovered during the MCO failure review process by outside reviewers and corrected before EDL. The second was discovered and evaluated by the project after TCM-3. The last two were evaluated but were not completely addressed during the development phase. Implications are discussed in this section.

Telemetry taken during the TCMs indicates that the temperatures near the tank outlets could have been extremely close to the freezing point of hydrazine. This could have had several undesirable effects on Propulsion Subsystem performance (see Section 7.5.8).

If sufficient propellant migration occurred between tanks during "zero g" cruise, it could have shifted the aeroshell center of mass and resulted in large displacements in the landing site. One worst-case scenario leads to excessively high touchdown velocities and mission failure. The potential for this failure depends on nonlinear folding patterns in the diaphragms. A test is currently being conducted to better characterize the phenomena. Preliminary results indicate that the diaphragms would collapse in a way that would minimize any significant amount of migration from occurring (see Sections 7.5.3 and 7.5.4 for discussion of this concern).

During the subsequent parachute operational phase, any initial offset in propellant center of mass would have grown larger due to the effect on lander orientation. This could have had a serious impact on controllability during the tip-up maneuver at the beginning of powered descent. Following the tip-up maneuver, imbalances in flow resistances in the two parallel branches could occur due to near-freezing temperatures at the tank outlets or variations in the flow resistance across the two normally closed pyro valves (see Figure 7-7). This would have further aggravated the center-of-mass offset and affected lander control authority (see Section 7.5.7).

Water hammer pressures approaching 2200 to 2500 psi were generated by the 12 pulsing 60-lbf descent thrusters. This severely stressed the design margins and reliability of the descent system and introduced oscillations into the structure and control system that were difficult to characterize. However, after reviewing the results of LMA's rigorous water hammer testing and analysis, it was concluded that the subsystem would have survived this environment (see Section 7.5.10).

7.5.2 RCS Propulsion Component Fails Prior to Terminal Descent

FAILURE MODE DESCRIPTION

After telemetry was lost, but prior to hypersonic entry, failure of an RCS propulsion feed system component (regulator fail open, RCS thruster valve fail open/closed, etc.) or RCS thruster (loss of thrust) could lead to improper orientation of the cruise stage and/or aeroshell, subsequently leading to an incorrect descent trajectory, excessive velocities, displacement of the landing ellipse, or failure of the heatshield. If this occurred during parachute operations, it could lead to either unacceptably high spin rates or possibly to an unsuccessful separation of the backshell/parachute.

FINDINGS

One of the last propulsion-related events that occurred prior to telemetry loss was pressurization of the two propellant tanks. Tank pressure telemetry verified that the pressurization was normal and that the regulator "locked up" at the correct regulation pressure. Although these components are single string, they were verified with a sufficiently robust test program and were observed to be operating normally throughout cruise.

PROCESS ASSESSMENT

Appropriate design, implementation and verification processes were followed.

7.5.3 Larger Than Allowable Propellant Center-of-Mass Offset

INTRODUCTION

There are propellant center-of-mass management requirements for each of the mission phases. The objective was to prevent unacceptable offsets in spacecraft center of mass that affect the angle of attack of the aeroshell during hypersonic entry, and loss of control during powered descent. This was made more difficult because the propellant is simultaneously fed from two parallel tanks. The tanks contain diaphragms to separate the pressurant gas from the hydrazine. Each tank was filled to

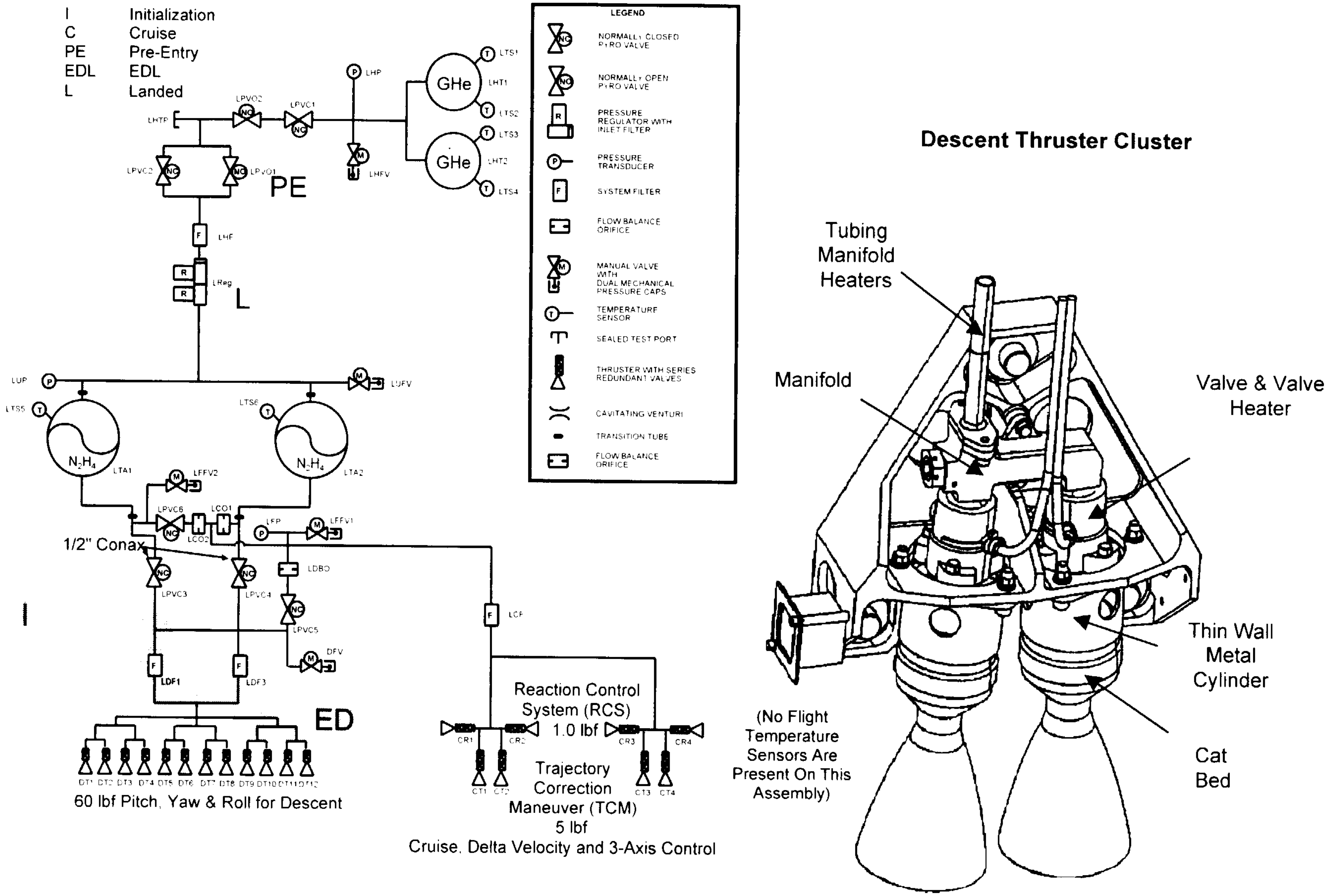


Figure 7-7. MPL Propulsion Subsystem Schematic

approximately 85 percent (which is the maximum before the diaphragms are stretched). The propellant center of mass can shift from nominal because of the following:

1. Inaccurate propellant loading pre-launch.
2. Variations in diaphragm shape and propellant center of mass within each tank following launch.
3. Unequal depletion during the RCS, TCM, or descent thruster firings.
4. Low flow (hours to days) migration between tanks during periods of "zero g" cruise due to differences in elasticity and folding configuration of the two diaphragms.
5. High flow (seconds) migration between tanks due to separation events and parachute operation.

Table 7-1 lists the mission phase, center-of-mass shift mechanism, reasons for constraint, preventative design features, and overall assessment.

Table 7-1. Mechanisms for Propellant Center-of-Mass Offset

Mission Phase	Mechanism	Constraint	Preventative Feature	Assessment
Pre-Launch	Uneven fill.	Launch control.	Loads claimed to be measured to within 0.03 kilogram.	TCM-1 data indicate center of mass was OK.
Launch	Migration between tanks due to non-symmetric acceleration forces and sloshing; center-of-mass displacements within each tank.	Launch control.	Pyro isolation valve.	Tanks are isolated. Analysis indicates that center-of-mass shift within each tank is minimal.
TCMs and RCS Thruster Operations	Unequal depletion due to unbalanced flow resistance upstream of branch point of 1-lbf and 5-lbf thrusters.	1-degree angle of attack on aeroshell during hypersonic entry.	Trim orifices in 1-lbf/5-lbf branches.	The orifices balance 5-lbf TCM thrusters and to a lesser degree the 1-lbf RCS thrusters. RCS propellant usage is small.
"Zero g" Cruise	Migration due to differences in stiffness and folded configuration between the two diaphragms.	1-degree angle of attack on aeroshell during hypersonic entry.	None, other than hysteresis "lockup" in the diaphragms, which hasn't been measured and may not be significant.	Specification is 2.8 millimeters. Flight data based on steady-state analysis of the site adjust maneuver (SAM) indicate that a shift of less than 5 millimeters had occurred prior to SAM. It is unlikely that much more occurred between SAM and the end of cruise. A test to better characterize diaphragm stiffness, configuration, and hysteresis is being conducted at LMA. The results are not expected to increase the "reasonable " worst-case estimate above.

Mission Phase	Mechanism	Constraint	Preventative Feature	Assessment
Hypersonic Entry	Migration between tanks due to hydrostatic head developed during hypersonic entry (if there is an initial center-of-mass offset).	1-degree angle of attack on aeroshell during hypersonic entry.	Flow orifices and limited time.	Specification is 2.8 millimeters. Survivability threshold is between 9 and 12 millimeters. Reasonable estimate of upper limit at beginning of hypersonic entry is approximately 5 millimeters. This initial center-of-mass offset will affect angle of attack in direction to cause more flow and increase offset. LMA analysis indicates that any additional shift during this phase would be less than 1 millimeter.
Heatshield Separation	Migration due to sloshing and transient accelerations.	13-millimeter propulsion specification on maximum center-of-mass shift for controllability during powered descent.	Flow orifices and limited time.	Potential migration is negligible.
Parachute Operations	Additional migration during parachute deceleration due to initial center-of-mass offset and resulting angular misalignment. (Flow orifice protection is lost when 3/4-inch lines are opened up during last 60 seconds of parachute operations.)	13-millimeter propulsion specification on maximum center-of-mass shift for controllability during powered descent.	Limited time.	Propulsion specification is 13 millimeters. Survivability threshold during tip-up maneuver at beginning of next phase is approximately 25 millimeters. With reasonable worst-case initial offset taken as 6.5 millimeters (equivalent to 5 millimeters in cruise phase), parachute operations could add an additional 4 to 6 millimeters, to result in an accumulated total of 10.5 to 12.5 millimeters. This would have to be added vectorially to a 10-millimeter mechanical offset.

Mission Phase	Mechanism	Constraint	Preventative Feature	Assessment
Powered Terminal Descent (60-lbf Thruster Operation)	Unequal depletion due to potential imbalance in flow resistance upstream of branch point in the feed system. This results from uncertainty in the flow resistance of normally closed pyro valves, potential for partial freezing at tank outlets, and uncertainties introduced by water hammer environment (dynamic flow resistance, unequal gas out of solution, etc.).	13-millimeter specification on propellant center-of-mass offset to assure controllability during powered descent.	Flow balance provided by matched resistance of normally closed pyro valves once opened (analysis and similarity to other valves)	Specification is 13 millimeters. Survivability threshold during the tip-up maneuver at the beginning of powered descent is approximately 25 millimeters. For the remainder of powered descent, the threshold is closer to 50 millimeters. Propellant center-of-mass offset could grow from a maximum of 12.5 millimeters at start of powered descent to 17.5 millimeters or more, depending on the match in flow resistances of the two normally closed pyro valves and whether there is any partial freezing at the tank outlets. This effect must be added vectorially to the 10-millimeter mechanical center-of-mass offset.

7.5.4 Larger Than Allowable Propellant Migration During "Zero G" Cruise Prior to Hypersonic Entry

FAILURE MODE DESCRIPTION

Propellant migration between tanks due to differences in the stiffness of the tank diaphragms could shift the spacecraft center of mass by enough to adversely affect the angle of attack of the aeroshell during hypersonic entry. This could cause large displacements in the landing location or, if severe enough, excessively high terminal velocities and/or heat loads.

The driving potential for the migration is the difference in the elasticity (or stiffness) and folding configurations of the two tank diaphragms. The gas sides of the two tanks are connected; gas-side pressures will quickly equilibrate after a short expulsion cycle. However, the liquid side pressures may temporarily develop a pressure gradient, which is relaxed with the transfer of propellant. Due to variations in the build process and localized folding and buckling during the expulsion cycle, the elastic forces within the two diaphragms will probably be different. Differences in these forces will temporarily build up a delta P gradient, estimated at several hundredths of a psi, across the liquid sides of the two tanks. If this pressure gradient exceeds the reversing hysteresis of one of the diaphragms, liquid will flow, at a low rate, from one tank to the other until the diaphragms reposition themselves into new equilibrium positions. There is nearly a complete lack of knowledge of the diaphragm configuration, nonlinearities, and hysteresis effects in "zero g." It is believed that a new equilibrium could be established after small amounts of propellant transfer or, with almost equal probability, that flow would continue until one of the two tanks is filled (to the 85-percent limit before the diaphragm begins stretching).

FINDINGS

The worst-case propellant imbalance resulting from this "zero g" migration is equal to or even (very) slightly greater than the propellant consumed by the TCMs and RCS thrusters prior to EDL, with one tank being full (to the loaded capacity of 85 percent) and the propellant in the other tank being reduced by the propellant consumed. Approximately 8.66 kilograms was consumed prior to EDL. This could result in a spacecraft center-of-mass offset on the order of 12 millimeters at hypersonic entry, as opposed to the requirement of 2.8 millimeters. Note that the total consumption for MPL was 8.66 kilograms versus an allocation of 20 kilograms (the problem could have been much worse).

Based on curves supplied by LMA, had the full possible 12-millimeter shift occurred, it would have resulted in either a downrange shift of 150 kilometers or an uprange shift of 60 kilometers in the landing location. If the latter had occurred (survivability threshold is between 9 and 12 millimeters), the entry angle would have been too steep to allow a safe landing. Predicated on the SAM analysis, a 9-millimeter or greater shift is considered highly unlikely.

In-flight telemetry has been used by LMA to place bounds on the amount of center-of-mass shift due to "zero g" propellant mass transfer. In particular, steady-state analysis of the SAM, which occurred approximately 9 months into the cruise phase, has been interpreted to limit the shift to ±4 millimeters. The maximum possible transfer prior to SAM was 6 kilograms. If this had occurred, it would have corresponded to a 7-millimeter shift in center of mass. These and other in-flight data have led LMA to conclude that 5 millimeters is a maximum bound on the shift that occurred prior to hypersonic entry (refer to LMA Memo No. MSP-AC-00-0381, Rev. A, 2/24/00, MPL Center-of-Mass Estimation Using TCM Telemetry Data, J. Wynn to L. Curtis, et al.).

PROCESS ASSESSMENT

The potential for incurring propellant migration during "zero g" cruise was not given proper attention by the project, even though it was recognized that there were very tight requirements on aeroshell center of mass. Concerns raised at the Propulsion CDR over "zero g" migration appear not to have been fully understood or characterized. On the other hand, concerns brought up at CDR over propellant migration during launch and hypersonic entry were adequately addressed by LMA.

LESSONS LEARNED

The use of parallel tanks on systems for missions with tight center-of-mass constraints should be avoided. If this cannot be accomplished, isolation ought to be provided between tanks. This can be done on the gas side during all periods other than pressurization or long burns or on the liquid side, whichever is more practical. Gas-side isolation will prevent any significant amount of "zero g" migration from occurring; however, this is not totally straightforward because large tank-temperature imbalances will cause some limited propellant transfer. State-of-the-art active or passive thermal control can be used to keep the temperature difference between tanks to within acceptable limits.

7.5.5 Larger Than Allowable Propellant Migration During Hypersonic Entry

FAILURE MODE DESCRIPTION

Any propellant imbalance that exists at the start of hypersonic entry increases due to acceleration forces during hypersonic entry. The flow is restricted by the orifices and small-diameter lines and the time is limited (about 200 seconds). LMA analysis (LMA Memo FSMO-00-008, Rev. A, MPL EDL Propellant Shift Analysis, T. Martin to G. McAllister, et al., 3/10/00) shows that, starting with an assumed offset of 5 millimeters, shifts due to this effect would be less than 1 millimeter and can therefore be neglected.

7.5.6 Augmented Propellant Migration During Parachute Operation

FAILURE MODE DESCRIPTION

Larger than allowable propellant migration while the lander is being decelerated by the parachute could result in larger than acceptable offset of the center of spacecraft mass. This could lead to an inability to control attitude during the powered descent.

There were some 60 seconds during parachute descent when the 1/2-inch pyro valves (LPVC3 and LPVC4) were open, providing a low-resistance path between the liquid sides of the two tanks. Any center-of-mass offset in the lander at the beginning of parachute operations would have tipped the lander until the center of mass was aligned with the parachute center of pressure along the deceleration vector. This tipping would result in a hydrostatic head developing across the two tanks, resulting in propellant flow in the direction of the initial offset. If the initial offset were due to a propellant center-of-mass offset, the propellant center-of-mass offset would be further exacerbated by the flow. The maximum propellant imbalance was 8.66 kilograms (from consumption during cruise). This corresponds to a maximum center-of-mass offset of approximately 18 millimeters at the start of powered descent.

JPL analysis of this effect was made assuming an average parachute drag force of 3400 N and bridle height of approximately 2 meters, and using pyro flow test data from LMA. As an example of the results, an initial offset at parachute deployment of 6.5 millimeters (equivalent 5 millimeters at the mass of the cruise stage) would grow to between 10.5 and 12.5 millimeters at the start of terminal descent (approximately one-third of this is due to uncertainty in the behavior of the diaphragms and Reynolds Number effects). LMA analysis indicates a smaller shift. This shift due to propellant migration must be added vectorially to the center-of-mass shift due to mechanical offsets from the loss of heatshield balancing mass. The stated propulsion specification requirement was a maximum of 13 millimeters. The lander may go unstable during the tip-up maneuver after completion of parachute operations if the combined center of mass exceeds 25 millimeters. After tip-up, the survivability threshold is thought to be close to 50 millimeters.

PROCESS ASSESSMENT

This effect, which depends on center-of-mass shift during the cruise phase, could have been largely mitigated if the opening of the normally-closed pyro valves LPVC3 and LPVC4 had been delayed until near the end of the parachute phase.

LESSONS LEARNED

When evaluating the center-of-mass shifts occurring during the descent phase, account must be taken of the effect of center-of-mass shifts that could have occurred earlier in the mission.

7.5.7 Larger Than Allowable Center-of-Mass Shift During Powered Descent

FAILURE MODE DESCRIPTION

Additional shifts in the lander center of mass could have occurred during the descent thruster firings if there was a mismatch in the flow resistance of the two parallel lines upstream of the 60-lbf thruster feed-line branch point. After the tip-up maneuver and during powered descent, a total lander center-of-mass shift exceeding approximately 50 millimeters results in a loss of controllability.

The concern for this potential failure mode arises from the following:

1. The sensitivity of the design to small unknowns.
2. The inability to measure the flow resistance of the normally closed pyro valves (after being opened).
3. Uncertainties in flow resistance introduced by the severe water hammer environment (dynamic flow resistance, unequal gas out of solution).
4. The potential for freezing or partial freezing in the tanks and lines near the tank outlets.

FINDINGS

A worst-case offset of up to 60 millimeters could have resulted if one of the tanks depleted before the other. A more reasonable worst-case estimate, unless there was partial freezing at the tank outlets, is an additional contribution of 5 millimeters for a total spacecraft center-of-mass offset (due to propellant imbalance in the tanks) of 17.5 millimeters. This is above the propulsion specification of 13 millimeters, but below the expected control threshold of 25 to 50 millimeters.

Flow resistance in each of the two parallel branches included resistance from the perforation plate at the tank outlet, where the hydrazine is at or just above its freezing point of 1.5 degrees C, a normally closed pyro valve, and associated plumbing. The total flow resistance in each branch was low. As a result, small differences in flow resistance would have had large influences on the relative flows from the two tanks. LMA asserts that flow balance between the two branches was provided by the predicted match in flow resistance across the two normally closed pyro valves, which would by then be open. (Approximately 75 percent of the resistance was due to the pyro valves.) Since these normally closed pyro valves could not be flow calibrated, the accuracy of the estimated flow resistance depended on assumptions in the analysis and on similarity with flow tests of other, already actuated normally closed pyro valves. Flow tests of 10 similar qualification valves indicated flow coefficients (linear with flow rate) that ranged from 4 to 4.7, averaged 4.35, and had a standard deviation of 0.26. If the maximum and minimum test values are assumed, the "reasonable worst case" center-of-mass offset due to propellant migration and uneven depletion would be increased by approximately 5 millimeters to a total of 17.5 millimeters. The effects of an imbalance in flow resistance could have been even higher due to nonlinear effects of water hammer. The magnitude of this latter effect is still being studied, but is not thought to be large.

PROCESS ASSESSMENT

The design approach for balancing flow from the two parallel branches during powered descent increased the risk of exceeding control authority. A statistical process for estimating the allowable flow variation should be used. There was no testing to validate the effects of water hammer on small differences of flow resistance in the two parallel branches. Appropriate margin for uncertainties does not appear to have been added.

LESSONS LEARNED

If parallel tanks must be used, trim orifices should be incorporated into each parallel branch. If this is impractical, use a conservative statistical approach and add significant margin for unknowns.

Do not ignore the nonlinear effects of water hammer on amplifying small imbalances in flow resistance.

7.5.8 Inadequate Thermal Control of Propulsion Subsystem

FAILURE MODE DESCRIPTION

Low temperatures at the tank outlets and adjacent feed lines may have resulted in near-freezing or freezing conditions. Partial freezing in the lines or in the tank outlets, where there are perforation plates, could lead to large flow imbalances from the two tanks, center-of-mass offsets, and loss of control authority.

FINDINGS

Telemetry taken during the TCMs indicates that the propellant line temperatures near the tank outlets were extremely close to the freezing point. Flight telemetry indicates that, during the TCMs, a feed-line temperature 7.5 inches downstream of one of the tank outlets dropped from approximately 13 degrees C to about 4 degrees C, only 2.5 degrees above freezing (the accuracy of the sensor is thought to be about 0.5 degree C). This temperature drop was a direct result of drawing cold propellant from the pedestal end of the tank. This region of the tank was cold as a result of mounting the tank to a sidewall of the spacecraft structure, which was not directly temperature controlled. Although the tank was heated, the heaters were generally located near the tank girth.

During system thermal–vacuum testing, the boss mounting interface reached temperatures of approximately –23 degrees C. While LMA predicted, post–TCM-3, that no "wetted" structure was likely to have been colder than +4.2 degrees C, an absence of test measurements and detailed model validation in this region casts uncertainty on this prediction and leaves open the possibility that some propellant within the tank may have locally frozen. If slush or frozen propellant collected on the perforation plate during powered descent, it would have affected flow balance from the two tanks. There was no temperature sensor on the other tank feed line; a similar condition could have occurred there.

In addition to the above concern, another major deficiency was discovered during a peer review of the Propulsion Subsystem following the MCO failure. LMA thermal–vacuum data indicated that the predicted temperature of the catalyst beds of the 60-lbf descent thrusters was in the –30 degrees C range, and a propellant manifold was predicted to be at –20 degrees C (well below the 1.5 degrees C freezing point of hydrazine). Had the attempt been made to fire the thrusters at this temperature, a failure would have likely occurred in the Propulsion Subsystem or in controlling the spacecraft. The problem was found in time and corrected; however, this reflects poorly on the communications between the propulsion and thermal personnel. Following the discovery, a series of thermal–vacuum tests was conducted at Primex. Based on the results, it was concluded that the thrusters could be brought up to acceptable temperatures by turning on the valve heaters approximately 5.5 hours before terminal descent. Since this now required bleeding hydrazine into 60 degrees C valves, ground tests were also done at temperatures up to 120 degrees C to verify that this would be no problem.

This approach was incorporated into the MPL Operations Plan and successfully accomplished. Review of the MPL Power Subsystem telemetry verifies that all 12 of the MPL valve heaters were turned on at the required time and that catalyst bed temperatures should have attained at least 10 degrees C prior to use.

PROCESS ASSESSMENT

Potentially catastrophic thermal design problems occurred in two separate areas. The process seems to have been flawed. Communication between the propulsion and thermal groups was inadequate. Propulsion temperature requirements and margins were not fully understood by thermal personnel. Misinterpretations of the meaning of "operating" and "non-operating" temperatures, and about whether it was allowable to drop propellant into lines that were well below freezing, both contributed to this misinterpretation. The thermal design effort lagged behind the propulsion design effort and made it difficult to evaluate design adequacy during the PDR and CDR reviews. Concerns were raised but not properly dispositioned. Thermal–vacuum test data were not fully evaluated or understood. Instrumentation on the Propulsion Subsystem — especially near the tank outlet — was not adequate to validate the thermal model, and an error in the tank heater model further complicated the problem. The recovery process and test program that were followed after discovering the low thruster temperatures were well executed.

LESSONS LEARNED

For future missions, ensure that Propulsion Subsystems are thoroughly instrumented for thermal–vacuum tests, that close coordination is occurring between propulsion personnel and thermal personnel during the design processes, and that there is synchronization and validation of the two designs at the Propulsion PDR and CDR. Establish clear thermal-control requirements that wetted surfaces and thruster inlet manifolds be maintained above 10 degrees C (that is, 8 degrees C above freezing) and that catalyst beds be maintained at least 10 degrees above qualification temperatures (preferably above 10 degrees C). Also ensure that adequate flight temperature measurements are allocated to sensitive components likely to be exposed to adverse thermal environments (e.g., propellant valves). Be willing to allocate more engineering telemetry channels to "first-of-a-class" missions to improve insight and reliability on subsequent missions.

7.5.9 Propulsion Component Fails During Terminal Descent (Other Than Caused By Water Hammer Effects)

FAILURE MODE DESCRIPTION

The propulsion components used during descent include the pressurant tank, the gas regulator, two propellant tanks, two normally closed 1/2-inch pyro valves, filters, and 12 60-lbf thrusters with their associated thruster valves, valve heaters, and plumbing. Failure of any one of these components would have resulted in loss of spacecraft control.

FINDINGS

The pressurant tank and propellant tanks retained pressure throughout cruise. The diaphragms in the propellant tanks appear to have functioned normally. The propellant tanks were pressurized to full pressure and the gas regulator was observed to lock up normally just prior to loss of telemetry. Power Subsystem telemetry indicated that the valve heaters were powered on in time to heat the thruster manifolds and catalyst beds (based on recent thermal–vacuum tests at Primex). New components not validated during cruise include the two normally closed pyro valves, the filters, and the 12 thrusters with associated valves and plumbing.

The regulator was a new development by Mu Space Products with some Space Shuttle and Cassini heritage. It is a robust series redundant design to minimize possibility of failure to lock up. Both sensing orifices or a large-bore sensing port would have had to be plugged for the regulator to fail open.

The pyro valves were made by Conax for the Advanced X-ray Astrophysics Facility (AXAF) to specifically avoid the detonation problems experienced by other vendors' valves when actuated in contact with hydrazine (especially with hydrazine both upstream and downstream, as is the case with the two normally closed valves LPVC3 and LPVC4). The Conax design incorporates a dual series metal-to-metal seal to prevent the combustion blow-by observed on the problem designs. No blow-by of any significance has ever been observed on these Conax valves. The test lot included four 1/2-inch valves tested with hydrazine both upstream and downstream, eleven 1/2-inch valves tested by TRW, and nine 3/8-inch valves tested by LMA with hydrazine upstream. A similar 1/4-inch valve with hydrazine on both sides was fired early in the MPL mission.

PROCESS ASSESSMENT

The design and qualification processes were adequate and commensurate with available funds and schedule.

Since development was completed, 26 of the 1/2-inch valves and approximately 20 of the 1/4-inch valves have been actuated without incident.

The thruster valves are the Small Missile valves manufactured during the 1980s. There is a robust heritage and the valves were put through exhaustive thruster pulse simulations.

The thrusters were newly developed for MPL but had a solid heritage. (The catalyst bed was modified to provide higher thrust.) Although there was only one development/qualification thruster available, it was subjected to rigorous test conditions and behaved as required. Impulse-bit performance and reproducibility during cold transients was determined from test data and provided to the controls group for their controls simulations.

If the water hammer environment is ignored (as in this failure mode), the environmental and lifetime requirements on these components is fairly benign.

7.5.10 Terminal Descent Propulsion Component Fails During Terminal Descent (Caused By Water Hammer Effects)

FAILURE MODE DESCRIPTION

Water hammer pressures generated during terminal descent had the potential to generate or shake loose contamination from the filters, yield or crack defective weld joints, damage valve seats or catalyst beds, excite structural resonances in the feed lines, and adversely affect spacecraft control.

FINDINGS

Using pulse control is a risky approach for a lander. Pulse control on an upper-stage booster or orbital injection system is difficult. A lander has even more constraints on propulsion and is less forgiving to anomalous performance. Using pulse control with mid-size multiple thrusters can generate high and difficult-to-characterize water hammer environments.

The 60-lbf descent thrusters were operated in a pulse mode wherein all 12 thrusters were turned on and left on for periods of 25 to 85 milliseconds every 100 milliseconds. (The control law required that all be closed within +10 milliseconds of each other.) This pulsing generated water hammer pressures in the feed lines as high as 2200 to 2500 psi. These pressure waves (termed water hammer) affected flow rate, chamber pressure, and thrust. Based on Method of Characteristics analysis techniques, LMA propulsion engineers modeled the feed system fluid dynamics, interfaced the feed system model with a thruster model provided by Primex, and validated the combined model with a water hammer test program that attempted to simulate the flight feed system configuration. Because of cost constraints, the test configuration included only one thruster (the development/qualification model). The other 11 thrusters were simulated by valves and downstream orifices. Review of the results indicates that the model correlation with test data was excellent. After validation, LMA interfaced their model with a structural model of the flight feed system. Outputs of the model were also provided to the LMA controls group for use in their controls model.

Test data indicate that excessive pressures were generated in the propulsion feed system and that localized yielding was occurring in the propellant lines. This dynamic environment also made it difficult to validate proper system performance (flow rates, flow balance, impulse bits). It also generated difficult-to-characterize accelerations and forces on the structures and controls system that were difficult to model or test. In addition, to compound the concern, there was no full-system, hot-fire test (because of cost constraints). Issues arising from the severe water hammer environment are as follows:

1. *Component and Propulsion Subsystem Integrity*. LMA analyses and tests conservatively indicated peak system (water hammer) pressures approaching 2200 to 2500 psi. In addition to the water hammer tests, LMA pulsed four valves 2000 times each with peak pressures of 2500 psi, with no indication of a problem. It is likely that the propulsion components could survive the actual water hammer forces; however, with this high an environment, any structural weaknesses missed during inspection or acceptance test could prove fatal. Stresses induced in the feed lines exceeded yield, but were deemed acceptable based on fatigue analyses. While the expected reliability of the 12 individual thruster/valve/heater assemblies was relatively high, overall system reliability would have been improved if the design had included a single engine-out capability.
2. *Adiabatic Compression Decomposition (ACD)*. ACD is a catastrophic decomposition of hydrazine resulting from rapid compression of small gas bubbles in a hydrazine system during a water hammer event. ACD was not observed during the extensive series of water hammer tests with saturated propellants and, therefore, probably did not occur in flight.
3. *Structural Interactions*. A water hammer test conducted using a flight-like mockup of a portion of the feed system and its support structure indicates violent movement in the feed line at 10 Hz and 60 Hz, with displacements of ±0.2 inch, peak to peak. The high magnitude dynamic pressure transients impart significant loads to the structure (see Section 7.2 for discussion of this issue).
4. *Control Failures*. See Section 7.3 for discussion of this issue.

PROCESS ASSESSMENT

LMA propulsion personnel did a commendable job with limited funds in testing and simulating the water hammer environment. A more robust test with at least three flight-like thrusters would have alleviated any residual concern over unknown and potentially adverse interactions.

LESSONS LEARNED

Future missions (Mars '03 and '05) are looking at a throttle valve configuration to alleviate the concerns over water hammer and thruster interactions. Industry-wide Requests for Information should be released to determine what is available. Use of a throttle valve instead of pulse-off control is preferred.

7.5.11 Adverse Plume Interactions During Terminal Descent and Touchdown

FAILURE MODE DESCRIPTION

Adverse interactions between plumes of adjacent thrusters can result in shock waves, stagnation regions, and some reverse flow during descent. This could have led to high heat loads to the lander and a reduction in the control authority of the thrusters. Interaction between the plumes and the ground during landing would have built up back pressures that, in combination with any inclination in slope, could produce an overturning torque. Interaction with the soil would have generated dust clouds and may have carved holes or trenches into the surface at the landing site. The concern is heightened by the fact that there were no vendor or system contractor analyses or tests to characterize these potential phenomena. (It is understood that some of these tests were requested by the LMA propulsion group during development; however, because of cost constraints, the request was rejected.)

FINDINGS

Plume effects were addressed by LMA at a meeting during the third week of January 2000. Results of CFD analysis performed by LMA for the Mars '01 development indicate that there would not have been any significant adverse effects due to interaction between adjacent plumes. However, the analysis does indicate that back pressures build up between the lander and the ground, exerting up to 80 lbf (average of 35 lbf due to duty cycle) on the lander just prior to touchdown. The effects of non-uniformities in surface slope and margins for lander stability were not evaluated.

Soil interactions are also a concern, particularly since thruster firing is not terminated until 50 milliseconds after first landing pad contact. The thruster plume disturbs a significant amount of dust and bores holes or trenches into the surface that could upset the lander. No work was done on this potential threat to MPL, but rough analysis scaled from analyses for the Viking lander optimistically (did not account for the effect of pulsing) concludes that the 12 thrusters could have disturbed up to a total of 300 liters of dirt before cutoff. Conditions at the MPL landing site may have very well been different.

PROCESS ASSESSMENT

Undue risk was incurred by the project in not characterizing the plume interactions. Apparently, the issue was raised several times during the development cycle, but was rejected. At the very least, the project could have resurrected some Viking test data and extrapolated to the MPL configuration.

LESSONS LEARNED

Plume–soil interactions should be modeled and verified by test for all future landers. Plume-to-plume interactions should be validated whenever adjacent thrusters are designed to fire simultaneously.

7.5.12 Other Issues

7.5.12.1 Small Forces During Cruise

The JPL Division 35 MCO Focus Group addressed small forces resulting from the RCS thrusters effecting the spacecraft trajectory. The issue was worked extensively prior to MPL entry and is not considered to be a plausible cause of the MPL loss. There are two issues, which will be addressed briefly here.

1. Evaluation of the acceptance test data of the RCS thrusters revealed that (1) tests run to characterize the thrusters did not acquire adequate limit cycle data and were not corrected for shutdown impulse; and (2) there was no Propulsion (neither JPL nor LMA) review of the test data. The acceptance tests conducted to characterize the delivered impulse for specific duty cycles were not run to equilibrium conditions and, therefore, did not provide accurate data. JPL Propulsion and Navigation later worked together to estimate the actual delivered impulse during limit cycle operation of the thrusters, and reasonable results were generated. Testing to improve the understanding of the magnitude and duration of the non-measured impulse delivered between the limit cycle pulsing of the thrusters (very low thrust after shutdown) is currently practical but lacks the funding to proceed.

2. LMA AACS personnel identified two thrust vector corrections ("fudge factors") for the MPL thrusters during cruise. The first is a factor of 1.6 on impulse bit, which could be approximately explained by failure to account for the missing shutdown impulse due to the "dribble volume." The second is an 11-degree offset in the thrust vector. There was some thought that it may be due to the effects of the scarfed nozzles and free molecular flow that could occur after shutdown; however, there is no agreement on this. For several reasons, it does not appear as though it has anything to do with a potential shift in the propellant center of mass (refer to the controls group).

   Additional tests and analyses are recommended to improve the understanding of the impulse delivered and resultant thrust vector of the thrusters used during long cruise periods of interplanetary spacecraft. The tests will involve instrumenting a small thruster with a highly sensitive pressure transducer to measure the rate at which the "dribble volume" propellant (the volume between the valve seat and the thruster catalyst bed) evaporates, reacts, and provides thrust. This is a known effect identified over time on actual spacecraft, but not measured in ground tests. Hardware is currently available to test at a smaller but representative thrust level.

7.5.12.2 Peer Review Process

The review process was less than desirable. The scope, the degree of JPL and LMA peer involvement, and the process for closing action items does not appear adequate. Formal subsystem PDRs and CDRs were replaced, not augmented, with "PDR or CDR peer reviews" that had less formality than the traditional subsystem reviews but no greater depth of penetration (such as is desired in a peer review). The PDR peer review was supported by JPL Propulsion via a videocon; only one JPL Propulsion representative was present at the CDR peer review. Also, there was no LMA off-project peer present at the reviews. Little time was given for preparation prior to the reviews. According to the LMA propulsion personnel, neither the PDR nor CDR peer review processes went into as much depth as the JPL MPL Failure Review Board meetings. In addition, the thermal design of the Propulsion Subsystem was too immature to be evaluated at the time of the propulsion reviews and, as a result, thermal interface issues were inadequately examined. Lastly, it isn't clear that the JPL project was rigorous in coordinating action item responses with JPL originators.

7.5.13 Conclusions

1. LMA did very good work in most areas.
2. Design deficiencies were found in the approaches used for:
   a) Managing the center of mass of the propellant in the two tanks during cruise and parachute operations.

   b) Ensuring flow balance from the parallel tanks during terminal descent.
   c) Maintaining propellant-tank outlet temperatures at a sufficient margin above freezing.
   d) Maintaining the descent thruster temperatures at a sufficient margin above freezing.
3. Pulse-mode control used during terminal descent generated severe water hammer pressures in the feed lines that stressed component margins, introduced high vibration loads into the propellant feed lines, affected pulse shape, and complicated the interface with the control system; however, it probably did not result in any catastrophic failure. Future missions should strive to incorporate a throttle valve.
4. The descent system design contains a large number of single-point catastrophic failure modes; however, these probably did not result in loss of the spacecraft.
5. The verification test program should have been more robust, considering the number of critical failure modes and the unproven system architecture.
6. The interface between thermal personnel and propulsion personnel appears to have been inadequate. More flight-temperature measurements should have been allocated for propulsion components, especially the propellant valves.
7. The review process was not as thorough as needed for such a complex subsystem.

Bibliography

AAIA-98-3665, Test and Modeling of the Mars '98 Descent Propulsion System Water Hammer — T. Martin, L. Rockwell, C. Parish, LMA, 7/13-15/98, Joint Propulsion Conference & Exhibit at Cleveland, Ohio.

Additional Information of MPL Prop Peer Review Process — via Lad Curtis, 2/24/00, e-mail from Greg McAllister on 2/22/00 regarding Propellant Isolation AI from Prop CDE, Electronic format.

Additional Information on MPL CM Offset Calculations From Flight TCM Data — Lad Curtis, 3/7/00, e-mail responding to Questions on MPL CM Offset Calculations from Flight TCM Data, H. Curtis, J. Wynn.

Additional Information on MPL Tank Outlet Temperature — via Lad Curtis, 2/21/00, e-mail from Kevin Miller on 2/18/00 regarding MSP '98, Memorandum to Greg McAllister, Tim Martin on 9/16/99, MSP '98 MPL Fuel Tank Status.

Additional Information on Propulsion: Zero-G Fuel Transfer Considerations — Lad Curtis, 2/17/00, e-mail of report from Tim Martin regarding Consideration of MPL Zero-G Fuel Transfer During Design and Development.

CFD Analysis of Mars '01 Lander Near-Ground Environments — Joe Bomba, Pete Huseman, 2/24/00.

EDL Propellant Tank Modeling and Analysis, LMA IOM FSMO-00-007, J. Wynn to Jim Chapel, Bill Willcockson, Tim Martin, 3/8/00.

FBC#2 — via Philip Garrison e-mail, 1/13/00, from John McNamee e-mail on 12/23/99.

Feed System Transient Pressure Effects on Operational Thruster Performance For a Pulse Modulated Controlled Multiple Thruster Planetary Lander, Report #D99-41717 — 12/23/99, Timothy Martin, William J. Bailey, Kelly R. Scheimbert, LMA

Fuel Tank Outlet — via Marilyn Morgan, 2/29/00, e-mail from Lad Curtis on 2/28/00, and Kevin Miller on 2/28/00, attachment: MPL Fuel Tank Outlet Discussion, 2/24/00.

JPL FRB Question: Entry Center-of-Mass Requirement — Lad Curtis, 1/13/00, e-mail reporting on center-of-mass requirement for entry on 1/12/00.

Latest Revision of MPL FRB Section 7.5 on Propulsion and Thermal — Carl S. Guernsey, 2/28/00, e-mail.

Lessons Learned Report from Mars Polar Lander Descent Engine Cold Catalyst Bed/Cold Inlet Manifold Issues — Milt Hetrick, Kevin Miller, LMA, 11/24/99, memo to Bill Meersman, Larry Talafuse, Lad Curtis, Al Herzl.

Mars Polar Lander, Cold Descent Engine Issue Close-out — H.H. Curtis, 11/22/99.

More Info on Flow Split, LMA e-mail, T. Martin to J. Leising, 2/25/00.

More Rebuttal — Timothy Martin, 2/18/00, e-mail regarding section 4.0 of the draft MPL failure review board findings.

MPL Center-of-Mass Bound for TCM-4 and TCM-5 — Jason Wynn, 2/15/00, e-mail regarding center-of-mass offset via spacecraft rate of telemetry.

MPL Center-of-Mass Estimation Using TCM Telemetry Data — Jason Wynn, 2/17/00, GN&C PDO Technical Memo MSP-AC-00-0381 to MacPherson, Whetsel, Burdick, Macala, Curtis, Euler, Chapel, Willcockson, Cwynar, Spath.

MPL EDL Propellant Shift Analyses, Rev. A — Timothy Martin, 3/08/00, memo FSMO-00-008 to G. McAllister, M. Hetrick, J. Wynn.

MPL Fuel Tank Outlet Discussion — K. Miller, G. McAllister, 2/24/00.

MPL Questions — Richard Cowley, 2/16/00, e-mail regarding hydrazine freezing and missing data period.

MPL Tank Diaphragm Test ROM — Milt Hetrick, 2/7/00, e-mail regarding a ROM estimate of the test cost to obtain the necessary data on the MPL tank diaphragm.

MSP Lander Flight Propellant Load — J. Greg McAllister, 3/9/00, memo to L. Curtis, K. Barnstable, J. Lenada, C. Cooley.

MSP Lander Propellant Differential Draining Analysis — Timothy Martin, 1/17/97, memo to D. Doub, G. McAllister, P. Sutton.

MSP Lander Propellant Transfer Analysis Update – Rev A — Timothy Martin, 10/24/97, memo to D. Doub, G. McAllister, P. Sutton, W. Willcockson, L. Curtis.

MSP Lander Verification Report VR006, circa Dec 97.

MSP'98 Propulsion Subsystem CDR Peer Review — 10/29/96, CDR Peer Review on 10/2-3/96, LMA.

MSP99-4070, Mars Polar Lander, Descent Thruster MR-107N, Cold Start Verification Test Report — 11/97, Tim Fischer, Kevin Johnson, LMA Propulsion PDO.

Parachute Lengths — Milt Hetrick, 2/14/00, e-mail regarding the distance from the center-of-pressure of the chute to the MPL.

Parachute Propellant Transfer, LMA e-mail, M. Hetrick to J. Leising, 3/10/00.

Plumes — Milt Hetrick, 3/8/00, e-mail.

Reply to Inadequate Thermal Margin and Deviation from Accepted Design Practice — Lad Curtis, 3/6/00, e-mail with attachment regarding Temperature Margin Management on Wetted Propulsion Components and MPL by Kevin Miller, 3/6/00.

Status of Center of Mass Action Items — Glenn A. Macala, 2/28/00, e-mail regarding further update.

STV REA Thermocouple Locations — November 1997.

Surface Dust Disturbance and Deposition During Mars '01 Landing — Carl Guernsey, 4/25/99, memo to Eric Suggs.

Tank Diaphragm Quick Look Data, Rev. A — LMA presentation, M. Hetrick et al., March 15, 2000.

Tank Diaphragm Testing – Centaur Tank — Milt Hetrick, 2/15/00, e-mail regarding update on Centaur water hammer testing.

Testing of the MPL 1/2" Pyro Valves in Propellants — via Lad Curtis e-mail of 1/10/00 from George E. Cain e-mail on 1/7/00.

Throttled Thrusters — Milt Hetrick, 3/8/00, e-mail.

7.6 MPL Avionics

FAILURE MODES

Several failure modes associated with avionics system components have been postulated. In particular, a Radar or IMU function loss or power system failure involving the Pyrotechnic Initiation Unit (PIU), Power Distribution and Drive Unit (PDDU), or battery could result in mission loss.

FINDINGS

Only one finding — possible ionization breakdown of the MGA or UHF antenna — is classified as a key finding. Both assemblies were analyzed for this problem as part of the design activity but not tested for breakdown in the Mars 6-torr environment at either the component or system level. Analysis work (especially in the case of the MGA) is considered necessary but insufficient to guarantee correct operation.

PROCESS ASSESSMENT

The processes associated with the avionics hardware development meet acceptable standards for design, manufacturing, testing and reliability. Combined with nearly perfect operation during the cruise phase, an avionics hardware failure during EDL is considered unlikely.

LESSONS LEARNED

All RF components, including antennas, should be tested for ionization breakdown in the 6-torr Mars environment. As a minimum, testing should be performed at the component level. Where possible, testing should also be performed to verify end-to-end performance at the system level.

OVERVIEW OF MPL AVIONICS

Meetings were held on 31 January and 1 February 2000 to review the MPL system avionics and potential failure modes.

The LMA team and its Spectrum Astro support team proved to be very open, helpful, and professional with regard to questions and action items. Detailed presentations were prepared for each of the review topics and the key avionics system elements were addressed in substantial detail from a design and test perspective. The LMA team also responded to various action items in near real-time and also prepared supplemental presentations associated with questions that arose during the review. Supplemental topics covered beyond the agenda included a review of the MGA two-axis gimbal design and testing, EMC waivers, test and analysis requirements associated with parachute snatch and landing loads, and the Actel design, development, and test process.

SYSTEM DESIGN

The MPL system consists of a relatively complex combination of avionics used during the cruise, entry, descent, and landing phases. In order to reduce mass, some clever compromises were made to the system in order to minimize the duplication of components. The system is fundamentally redundant with the exception of hardware used exclusively for the very short entry and descent segments of the mission.

The portions of the MPL avionics system subjected to review included:

a) Electrical Power System (EPS), consisting of the landed solar array, 16 amp-hour NiH battery, thermal battery, Charge Control Unit (CCU), Pyro Initiation Unit (PIU), and Power Distribution and Drive Unit (PDDU).
b) Attitude Control System elements, consisting of the IMU (–A side used during EDL) and landing Radar.
c) Telecommunications System, consisting of UHF and X-band components with their respective distribution elements and antennas.
d) Electrical interconnect system.

PROCESS ASSESSMENT

1. Review of Initial State

Cruise telemetry plots and trend data were presented with an associated assessment. Performance of the EPS, ACS, telecom system (with high-gain antenna), and thermal system was nominal through the entire cruise phase, with the exception of the star tracker, which experienced a glint problem in certain Sun-pointed attitudes. Due to the star tracker problem, the system experienced an –A to –B side switch early in the cruise phase. Once it was understood, the problem was an annoyance in the cruise phase but did not adversely affect operations. The problem also did not affect EDL since the star trackers are attached to the cruise ring, which is jettisoned prior to entry. As part of the initial troubleshooting activity, the system was returned to the –A side, which functioned normally for the remainder of cruise. Based on telemetry and cruise performance, there is no reason to suspect that any of the electrical system hardware was flawed or would not perform properly during EDL.

2. EDL Sequence and First Operation Summary

Each operational state was reviewed to assess: a) the known status of items already in operation, b) the condition and expected operation of items that were changing state, and c) the best known condition of items subjected to first use. Special attention was paid to the power system status and battery state of charge in the pre-EDL and EDL phases. Telemetry data and trending of cell pressure over the entire cruise period, indicate the batteries entered the EDL segment at approximately 130 percent of 16 amp-hour nameplate capacity.

The system power analysis of the end-to-end EDL sequence showed that the battery charge would be approximately 118 percent at the time of landing. This result is modestly affected by the performance of the thermal battery.

From a transitional or first operation perspective, there were no real surprises with the design. With the exception of ordnance-induced mechanical events, the significant electrical events are: a) operation of the coaxial RF switch (to transfer RF between the cruise and lander systems), b) disabling of the CCU (to deadface the cruise solar array separation connector), c) operation of the landing Radar,
d) activation of the thermal battery, and e) operation of the MGA. The design details and methods of previous verification for each of these operations are discussed below.

3. Electrical Power System

The EPS is a relatively simple unregulated direct energy transfer (DET) design. It is fundamentally string redundant and was operated on the –A side without incident for the entire cruise period. Operation continued on the –A side during the EDL phase of operation.

An overall review of the EPS as a system and a detailed review of each of the EPS components was performed to determine the quality of design and possibility for failure. For the most part, the overall system was found to be well conceived, with acceptable margins. One key concern with a simple DET system is the fact that a short can be catastrophic in some cases. However, this concern was addressed effectively by LMA through review and a series of mitigation strategies.

The individual components were also found to be well designed although there were some areas where the design and implementation could have been improved. Key design information related to the review of each component is summarized below.

a) Battery. The main battery is a 16 amp-hour NiH common pressure vessel (CPV) type with rabbit-ear terminations. Built by Eagle-Picher, it is similar to those used on Stardust and GOES. While the CPV style (which has 2 cells per pressure canister) is not as established as the IPV (single cell per canister) types, there is no reason to think that there is a performance or reliability concern. There is a single battery, however, so it is a single-point failure for the system. The battery was used during the cruise and landing segment of the mission and, as noted above, was functioning perfectly at the time of entry. Overall, the design and qualification of the battery looks satisfactory, although there are a few issues worth noting.

First, in order to get a little more power margin for the system, the decision was made to use 23 cells rather than the more traditional 22 cells. The odd number of cells resulted in the need to have 11 CPV cells plus a single IPV cell where the IPV cell was basically a CPV canister loaded with one instead of two cells. This partially loaded cell is judged only marginally qualified by its similarity to the other cells.

Second, there was a vibration failure on the original flight battery where two cells developed internal shorts. The cause of the problem was poor process control during assembly of the cells where a staking step was omitted. This was corrected for the flight lot on MSP '01 but x-ray screened cells from the original lot were used for the MSP '98 mission. The corrective action approach appears well conceived, but there is a residual concern regarding the robustness of the design and adequacy of the manufacturing process.

Third, as will be discussed under item 8 below, no test was performed on the battery pack to qualify it for the parachute mortar shock/load, snatch load, or landing load. Instead, an analysis (albeit a convincing one) was performed that showed that each of these loads are essentially quasi-static. It was also determined (less convincingly) that the loads are enveloped and thus verified by the random vibration test.

b) Thermal Battery. The thermal battery used on the lander is an Eagle-Picher type EAP12137 from the same lot as the unit used for the Mars Pathfinder mission. It is activated during EDL using an internal NSI and has an active life of approximately 8 minutes. The thermal battery is connected in parallel with the main battery and is isolated by two series diodes. Its main purpose is to supply supplemental power during key high energy EDL events. This function was tested and verified at least twice during spacecraft ATLO activities.

Qualification of the thermal battery was performed in 1994 for the Mars Pathfinder mission and consisted of an acceptable series of tests. Since the battery is both electrically and thermally isolated from the lander system, there is no single-point failure that can propagate into the rest of the system. A failure of the battery would also not be a problem given the high level of main battery capacity. It should be noted that the battery was a relatively late add-on to the design. In order for it to be accommodated, the main harness was spliced with hard-wire connections.

c) Solar Arrays. The surface solar array configuration consists of four elements, including the two fold-out main panels plus two smaller fixed panels used for the Lazarus mode and the CCU bootstrap start-up. The surface arrays are basically identical to the cruise arrays (29 40-cell strings for surface vs. 30 41-cell strings for cruise), consisting of 7.5-mil GaAs/Ge cells with 6-mil cover glass and integral diodes. The cruise and surface arrays were both designed by Spectrum Astro and built by Spectrolab. The use of small arrays for the Lazarus and bootstrap functions is unusual but no design or manufacturing issues were identified.

d) Charge Control Unit. The CCU is well designed and performed perfectly during the cruise segment of the mission. The flight system consists of two redundant units running in parallel. The pair flown on the mission consisted of a protoflight and flight unit. Both units were subjected to adequate testing prior to flight.

There is one operational issue associated with the CCUs that has a potential impact on lander reliability. In order to eliminate current flow from the cruise solar arrays before cruise stage separation, a latching relay in the CCU is commanded to turn off the charge control switches 2 seconds prior to separation. This approach effectively deadfaces the power connector at the separation interface but with the result that it must be re-enabled on the surface in order to generate power. Since there is a separate command for CCU-A and CCU-B, it would take a failure of two commands in order to lose power. As well, there is sufficient battery capacity at the time of landing such that a failure of both CCUs would not result in an initial loss of contact.

e) Power Distribution and Drive Unit. The PDDU is a relatively sophisticated internally redundant unit consisting of nine cards and a common backplane. The interface to the spacecraft is via the multifunction bus (MFB). Internal to the unit, the EPS switch card has eight n-channel 10-amp MOSFET switches that control power to downstream loads within the PDDU. Four of the 10-amp circuits power forty 3-amp switches on the two load switch cards, which power the various switched loads on the lander system. Two more of the 10-amp circuits power a redundant 28-volt DC–DC converter, each side of which provides five switched 3-amp outputs used in places where regulated 28 volts is required (such as the Deep Space Transponders). The last pair of 10-amp switches provide power to the redundant Motor Articulation Drive (MAD) module, which controls the 2-axis MGA gimbal system.

A review of the individual cards concentrated on the power switch and motor drive functions, since these elements contained circuits where critical first operations occur. The review was performed down to the circuit level and identified some minor design deficiencies, but nothing that would greatly increase mission risk. In all cases except for the motor drive, operation of similar circuits occurred routinely during the cruise phase. The test program on the ground was also reviewed and found to be effective. However, the unit did require rework and retest due to the cracked diode problem discussed under item 12.

As noted above, the MAD is only used with the MGA after landing and cannot be operated during cruise. It is basically a heritage card from P59 and Stardust where it was used successfully in the solar array drive application with an identical motor and gimbal system. The card contains an Actel 1280 field-programmable gate array (FPGA) and uses standard Schaeffer harmonic drive hybrids (common buy with P59 program) for motor control. The card is well designed ,although it is worth noting that an inherited P59 FPGA logic problem required modification after unit testing uncovered a logic race condition. This discovery points up a weakness in the project's overall Actel logic design approach that will be discussed under item 10.

f) Pyro Initiation Unit. The PIU consists of a redundant Pyrotechnic Initiator Module (PIM) and a Propulsion Valve Drive Module (PVDM). The PIM consists of two identical driver cards providing redundant pulsed (20 millisecond or 30 millisecond pulses, depending on function) power outputs for the many EDL ordnance functions. The PVDM consists of a single internally redundant card, each with 20 outputs that control the four RCS thrusters, four trajectory-correction thrusters, and 12 descent engines.

The PIU design is similar in concept to the PDDU, but contains added protection to provide triple fault tolerance. Its design is good in most areas, although it is possible to get a very short "burp" through the switches (with much less energy than is necessary to fire a pyro) in response to a bus transient. This is not a real issue by itself, but it is worth noting that the GSE test equipment used with the unit has a trigger threshold above the no-fire threshold for NSIs. Therefore, it is theoretically possible (although implausible) for an unswitched channel to test good with the GSE but still have an inadvertent pulse of sufficient length and duration to fire an NSI.

The test program for the unit was comprehensive and did a good job of verifying functionality at both the unit and system level. Operation of all pyro and engine drive functions occurred during each system test phase, including at the Cape prior to launch. The testing at the Cape included thruster and engine tests where the valves were actuated with N2 gas. It should be mentioned that the PIU was removed and reworked twice after delivery to the Cape. The first instance was due to the cracked diode problem discussed under item 12. The second instance was to remove a programmable array logic (PAL) device that was determined to have faulty and potentially dangerous logic. The PAL issue is a long story that can be summarized by saying that the PIU design was simpler and better without it. While late removal added some risk, the retest and final system test is judged effective at demonstrating both reliability and proper functionality.

4. Attitude Control System

The Attitude Control System (ACS) consists of redundant star cameras and Sun sensors, redundant IMUs (IMU-A and IMU-B), plus a single landing Radar. The glint problem with the star cameras is well documented and affected operations during the cruise segment of the mission. The star cameras and Sun sensors are both ejected with the cruise ring and did not affect EDL. Therefore, the system review activity concentrated on the IMUs and landing Radar with respect to performance and potential failure modes.

a) Inertial Measurement Unit. Redundant IMUs were body mounted on opposite sides of the lander system. Each IMU (the actual name is MIMU: Miniature Inertial Measurement Unit) is a quasi-standard product produced by Honeywell in Clearwater, Florida. Three ring laser gyros elements manufactured by the Minneapolis division of Honeywell are incorporated into the unit, plus three accelerometers built by Allied Signal (now merged with Honeywell). The MIMU unit is commonly used on aircraft and has some spaceflight heritage, including MCO and Stardust. Its operation was flawless during the lander cruise phase as well as on the MCO and Stardust missions.

Each IMU uses approximately 25 watts and is mounted in a cylindrical hermetic enclosure using a single Viton O-ring seal in order to protect the laser components and prevent high-voltage breakdown. It should be noted that enclosure hermeticity is critical to the proper operation. There were initial problems with the seal design that were corrected by careful control of the manufacturing and handing of the sealing surface. The O-ring is also greased with Bray 601 during the final assembly process.

The unit is backfilled with N_2 and a 1-percent He tracer in order to monitor the unit leak rate. Careful testing of the leak rate on the ground showed that the units had acceptable leak rates at the time of

ATP completion. Surprisingly, there was no internal pressure transducer of other direct method of measuring the internal pressure. This lack of monitoring is only an issue for the implausible case of a gross leak where the interior of the unit quickly leaks down to hard vacuum. In this case, the laser would continue to operate properly (assuming it survived the initial leak down) but would fail due to Paschen breakdown upon repressurization to the Mars ambient environment.

A second (and more likely) failure mode due to a fine leak and partial leakdown is not valid for the Mars environment. In order to preclude high-voltage breakdown, it would be necessary for the external pressure at the Mars surface to always be lower than the residual internal pressure. Therefore, there is no possibility that the enclosure would be crushed as the external pressure increased during the descent phase.

b) Landing Radar. Proper operation of the landing Radar system is required in order to achieve a successful soft landing. The Radar design is an F16 HG9550 aircraft Radar altimeter modified to provide Doppler data. Whereas the original design used a single non-coherent beam, the lander Radar was upgraded to four coherent beams that are bi-phase modulated at 4.3 GHz. The hardware and processing algorithms for the Doppler section were adapted from a tail-warning Radar system used on other aircraft programs. To save money (and weight), a major compromise was made through use of a receive/transmit multiplexer (R/T MUX) on the antenna assembly. This approach allows a single antenna to be time-shared between the altimeter and Doppler functions as well as between transmit and receive. The timing of the multiplexer limits the speed of transition between the transmit and receive functions. In turn, this speed limit established the minimum altitude of approximately 40 meters at which the Radar will function.

A Honeywell non-coherent single beam altimeter design of the similar heritage was successfully flown on the Mars Pathfinder system. The Pathfinder system used two antennas of the same design (and hence could fly all the way to the ground) with a similar coaxial feed system. Therefore, the antenna and RF feed system, except for the transmit/receive (T/R) switch and diplexer (part of the T/R switch unit), is qualified for operation in the Mars environment. The power required for the coherent MPL Radar is 100 milliwatts instead of the >500 milliwatts used on the Pathfinder non-coherent version. This eliminates the ionization breakdown concern associated with the fact that the MPL landing Radar was not operated in the transmit mode during the landed thermal–vacuum test.

Based on the data provided and discussions with the Honeywell engineers, it appears that the Radar is well designed and has good heritage. The environmental test program also looks good (the Review Team did not judge the helicopter and aircraft descent test program), although there was one vibration failure associated with programmable delay line. This delay line is operated during the built-in test (BIT) sequence, however, and was known to be functioning at the start of EDL.

The one issue worth noting is the fact that Radar operation in the transmit mode is not possible when enclosed within the aeroshell. Therefore, pre-EDL checkout is limited to certain BIT functions. The Doppler processor function associated with the velocity measurement and the operation of the four antennas could not be verified prior to EDL.

The omission of Doppler testing is because the BIT algorithm was carried over with essentially no modification from the original single function altimeter. The BIT function does include a oblique test of the power amp output and coax feed to the antenna assembly since the test relies on signal leakage in the R/T MUX switch between the transmit and receive inputs.

The consequence of limited functional testing prior to EDL is total reliance on the pre-launch test program. There was an ACS phasing test at the Cape where each antenna was spoofed using an RF hat and special test set. This test was effective at functionally verifying each of the four Radar channels.

5. Telecom System

The lander RF telecom system consists of UHF and X-band elements distributed around the thermal enclosure. With the exception of the X-band antenna, all the system components have flight heritage.

a) UHF Subsystem. The UHF Telecommunications Subsystem is relatively simple, consisting of a Cincinnati Electronics UHF transceiver, a diplexer, and antenna. The design and implementation of the system is straightforward. The lander transmit and receive frequencies are 401.5275 MHz and 437.1 MHz, respectively. Data rates are 8003 and 128,038 bps for frequency shift key (FSK) modulation and 128,038 bps for bi-phase shift key (BPSK) modulation.

The Cincinnati UHF transceiver was a new design for MCO and MPL that was built up from mostly heritage elements. The main reason for not using an existing heritage design was the need for smaller packaging. The design requirements and test program were fairly comprehensive. There was a design requirement but no test requirement to operate in the 6-torr Mars environment. However, the transceiver thermal vacuum test included operation during pumpdown. The transceiver was also operated successfully during the system landed thermal–vacuum test.

A diplexer is required to allow the capability to transmit and receive using the same antenna. It is a heritage item built by Narda (now Lockheed) previously used on Intelsat, STS, IUS, and GPS. Thermal cycling was performed at the component level but there was no thermal vacuum testing. The unit is encapsulated, however, and the engineering unit was altitude tested. Successful operation in vacuum and in the Mars ambient pressure environment also was verified during the landed thermal–vacuum test.

The UHF antenna was manufactured by Litton Amecom. It is a right-hand polarized, quad-helix based on a Space Station design. No thermal–vacuum testing was performed on the flight item. Qualification for the Mars ambient environment was done by analysis, since the maximum expected voltage of ~15 volts makes the chance of ionization breakdown unlikely. It should also be noted that the landed thermal–vacuum test had a direct RF connection out of the transceiver and bypassed the antenna. There was also a concern at the CDR regarding the link margin at low elevation angles. This concern was planned to be mitigated by making the shape of the antenna more conical.

b) X-Band Telecom System. The X-band system is standard in implementation. There is one complication, however, in that the there are two RF interfaces that must be isolated and deadfaced prior to cruise stage separation. By allowing for separation at the RF interface, it is possible to use the same telecom components for both the cruise and landed segments of the mission. Since the cruise system worked perfectly prior to separation, this analysis concentrates exclusively on the lander telecom elements with the exception of the MGA, which is discussed separately under item 6. One note of importance is the fact that a hard RF link was used for virtually all ground testing, including the landed thermal–vacuum test. Therefore, all of the system, with the exception of the MGA, was effectively qualified for the Mars environment.

Redundant Deep Space Transponders (DST1, DST2), in combination with a dedicated Command Detector Unit (CDU) and Telemetry Modulation Unit (TMU), form the heart of the X-band telecom system. Each of these items is well matched to the application and have qualified deep space flight heritage from Cassini, NEAR, and/or Mars Pathfinder. The DST is manufactured by Motorola and the

CDU/TMU units are built by LMA. All three units run off switched, regulated 28 volts provided by the HKPS card in the PDDU. The test program was satisfactory on these items, although DST1, a Cassini spare, did experience a failure during its original test program. DST2 also experienced a failure in the landed thermal–vacuum test where the input current approximately doubled. This problem was definitively reproduced and traced to an open sync line on the power converter. There is no evidence that the Mars ambient environment played a role in the anomaly.

The output of each DST is routed to a 90-degree hybrid coupler, which provides mixing and signal isolation for the SSPA input and the cruise/lander separation interface. Design information on the hybrid couplers was not provided at the review, but has been requested. However, the ports associated with the DST1 input and cruise system RF output are known to have worked correctly. Therefore, it is unlikely that the other ports on the coupler experienced a problem.

The SSPA is a 15-watt RF output unit manufactured by Electromagnetic Sciences. The design was new for MPL but was mostly a derivative of a design used on Milstar. The design isolates the power return and outputs from chassis, runs off the unregulated bus power, and can tolerate a short or open on the output. No data were provided indicating that the SSPA experienced problems during component or system testing. It is worth noting, however, that the lander SSPA and diplexer between the output and antenna could not be operated during cruise. Therefore, the last test of this system happened at the Cape as part of final system test.

The uplink signal path through the MGA is routed through a diplexer in order to isolated the transmit and receive signals. It is then routed through a coaxial switch which selects either the MGA or the LGA. The switch output is then routed through a second coaxial switch made necessary by the need for switching between the cruise and lander antennas. The output of this switch is then connected to DST1 and DST2 receiver inputs. It should be noted that the second coaxial switch is a single point failure for the receiver part of the system that is not operated until after loss of communication at the beginning of EDL. No major issues were found in a review of the manufacturing and test records.

6. MGA and Gimbal System

The MGA was designed and built by Boeing Defense and Space, Seattle, Washington. It was a new, lightweight composite design derived from work for JPL on Pluto Fast Flyby. The design package from the CDR had some preliminary data and did not contain flight drawings for the reflector or feed system. Based on discussions with LMA, however, there were no major issues during development.

As noted above, one critical issue with the antenna is the fact that it was not operated during the landed thermal vacuum test. This leads to a concern regarding the possibility for multipacting or ionization breakdown somewhere in the feed system. The analysis and mitigation activities associated with this issue were unconvincing in the review package.

MGA two-axis gimbal (MGA TAG) is a well-designed pointing system based on solar array drive systems flown on P59 and MCO. In both cases, the pointing system required equivalent or greater loads and had similar accuracy requirements. The design employs Techstar stepper motors and Vernitron rad-hard, 12-bit optical encoders. The motors are not used in the stepper mode but are under closed-loop control between feedback from the encoders and the control/drive electronics on the PDDU MAD card. The gimbal system moves very slowly due to the 160:1 harmonic drive reduction gear and has good torque margin for the application. Hardstops and softstops are used to limit the range of rotation.

Sixteen axes have been built to date. The motors and encoders used on the lander are out of the same lot as those used on P59 and MCO. The flight unit was successfully protoflight qualified although a bolt hole problem required rework that ended up causing ESD damage to one of the encoders. Following repair, the complete gimbal system went through a successful requalification program and series of system tests.

7. Harness Design and Deadfacing Approach

The harness design and implementation employs standard aerospace practices in most areas. The main power bus cables, which are a single-point failure, have added protection and inspection to avoid a catastrophic short. Ordnance cables are segregated from other harnesses and also have separation between prime and redundant signals. To save weight, the shielding method associated with the ordnance harness has an individual twisted shielded pair for each device but no overwrap. This approach is inconsistent with the preferred triax shielding approach but appears to have sufficient susceptibility margin to preclude accidental firing.

There are six signal/power connectors and two RF connectors associated with the cruise stage and backshell separation. The separation harness has 235 wires at the cruise interface and 271 wires at the backshell interface. The design uses scoop-proof connectors with the male pins on the pull-away side of the interface and is appropriately protected against exposed signals and the possibility of re-contact. Prime and redundant ordnance harnesses are separate from each other and the have individual separation connectors. All interfaces employ acceptable methods for deadfacing that limit current flow through the connector at the time of separation. They also use "toilet seat" dust cover/ESD flaps to completely cover the remaining connector interface.

An inspection of sample separation connectors showed them to be well made and to meet the scoop-proof criteria. The separation force required for pull away was impressive at room temperature and is understood to increase at cold temperatures. The issue of separation force is under investigation by the mechanical review team and was not pursued.

8. Verification and Environmental Simulation

The main objective of this review activity was to understand the test program for critical system elements at the component level and for key environments associated with entry and landed conditions. Overall, the test program was found to be comprehensive and consistent with appropriate electrical and environmental requirements developed for the system and flowed down to individual components.

One observation associated with the overall program is the fact that the system thermal–vacuum test activity was primarily interested in environmental simulation of the various mission phases and was not intended to provide confidence in the system reliability via thermal cycles. This approach increased the importance of testing at the component level to assure overall system reliability.

Areas of particular interest during the review were specialized environments such as the parachute mortar shock/load, the snatch load, the landing load, and operation in the Mars 6-torr CO_2 environment. These issues were addressed effectively in some cases, but there is a concern that there was too much analysis and not enough testing to be sure the individual components and the total system would work as expected.

The NiH battery is an example where no load simulation or testing was done. It was assumed (probably correctly) that the snatch and landing loads could be analyzed as a quasi-static case and then verified by the random vibration testing. Since the battery is a single-point failure for the system and did experience a shorting failure in it first random vibration test, it would seem that testing for all critical environments would be appropriate.

The UHF antenna and MGA have a similar concern in that their performance in the 6-torr Mars environment was analyzed but never tested at either the component or the system level. Given the mission criticality of both components and the fact that neither item was specifically designed for the Mars environment, an appropriate series of demonstration appears warranted.

Despite the omissions discussed above, the thermal vacuum test program was fairly comprehensive. The test effectively simulated every critical environment associated with cruise and landing. Therefore, with the exception of the UHF antenna and MGA, it is believed that the electrical system design, including telecom components, was verified to be compatible with the thermal and pressure environment expected during cruise, entry and on the surface of Mars.

The ATLO test program associated with verification of the pyro and propulsion functions was also found to be complete. LMA did a thorough job of end-to-end testing every wire and function at appropriate points in the test program. The final test occurred at the Cape and included a verification of all functions from a fire/no-fire perspective using a representative EDL profile. It is worth noting that a plugs-out test was performed but the telecom link employed a hard line to the GSE rather than antenna hats. Therefore, total ground isolation was not achieved during this test.

9. EMC Design and Test Program
The EMC design and test programs were found to be fundamentally sound. Appropriate practices were employed to achieve a 6-dB margin between emission sources and susceptible circuits. Test requirements were also flowed down appropriately to individual components.

10. Actel Design and Review Approach
Actel 1280 devices are used in many of the electrical components for critical logic functions. The designs were not reviewed but the overall approach to Actel design, simulation, test, and flight programming was explored. The EPS elements employ nine different designs, of which six are new and three are derived from an Air Force program. Designs associated with the C&DH were identified but not looked at in detail.

The design group is small and it is obvious that they are experienced as well as familiar with key rules associated with development of reliable Actel designs. Although majority voting is used, there are no specific design rules governing use of C vs. S modules, synchronous techniques, or percent of device utilization. Good tools are available, although the designs are realized using schematic capture techniques rather than VHDL (a plus and a minus). Circuit simulation is performed by the designer, but the design review process is not formalized to assure a standard level of design quality.

The chip- and part-level processing were very well done (although to an 883 rather than S equivalent level). Matsushita chips were selected and radiation tested at the die level (with JPL) and then packaged by Actel. Unprogrammed devices were then processed, including 168 hours of burn-in prior to programming. The programming activity is performed by a single individual using released and controlled software. All data associated with the release are retained and maintained to assure traceability.

Based on the review and the relatively low complexity of the designs, there are no major issues or concerns with the Actel development process. There is a minor issue with the fact that no screening is performed after device programming, but the process followed is fairly standard. There would be a concern in instances where extreme device performance is required. In such cases, a more formalized design and review approach would be appropriate.

11. Touchdown Sensor

The touchdown sensor design was reviewed from an electrical and functional perspective. The design uses an Optek OMH3040S Hall Effect Sensor mounted in close planar proximity to an SmCo magnet. Actuation of the sensor occurs when the foot mechanism translates the sensor and magnet relative to one another such that the magnetic field is reduced below the trigger level at the sensor.

The OMH3040U specification sheet indicates that the device is well suited to the application with sensitivity and hysteresis levels that are matched to the maximum magnetic field strength available from the SmCo magnet. The mechanical design itself appears good in most respects (and will probably be reliable) but does not make any attempt to capture the magnetic field or control the stray field through use of a yoke. As a result, the B-field can fluctuate when in proximity to other magnets or ferromagnetic materials and the circuit will also have variability in its trigger sensitivity.

The above issue results in a loss of margin, but would not result in false triggering of the sensor itself. However, the design does not have any electrical filtering or take specific precautions to mitigate the effects of EMI. Therefore, it certainly appears possible to induce a very fast electrical transient that would be sensed and potentially acted upon by the flight system.

12. Glass-Body Diode Problem

A glass body diode cracking problem was identified very late in the MCO/MPL development program. Surface-mounted glass diodes were found to be cracking in certain places where Aptek Type 5 polyurethane conformal coating material was used. This particular coating is harder than Uralane 5750 and also has a modulus transition temperature on the order of +10 degrees C. Therefore, the amount of stress applied to conformally coated parts was found to exceed acceptable limits under some conditions.

There were 101 diodes in the C&DH, 342 in the PDDU, and 512 in the PIU potentially affected by this problem. LMA did a good job of understanding the impact of a failure in each application. They were also able to understand the failure cause and develop a quantifiable method of inspection for determining which parts would need repair or replacement. A coating fillet under a part of less than or equal to 1/2D would not result in a crack. The C&DH, PDDU, and PIU units were removed prior to shipment of the lander to the Cape and inspected based on the on the 1/2D criteria described above.

Ten diodes were found to be cracked and were replaced between the three boxes. The remaining diodes in the components were individually inspected per the 1/2D criteria and 168 had their conformal coating removed and reapplied to the new criteria. Following inspection and rework, the three units were subjected to a one-axis vibration test and two thermal cycles at acceptance levels. They were then shipped to the Cape and reintegrated with the system. The entire system was then run through a comprehensive test where all functions were verified.

FINDINGS

This is a summary of the issues or other concerns that were discovered as part of the avionics review and evaluation effort. With the exception of item 13, most of the findings are minor but do identify design or test deficiencies where a failure or problem cannot be excluded. Item 13 is the sole key finding and identifies the ionization breakdown concern related to the UHF antenna and MGA. Neither was tested for proper operation in the Mars 6-torr environment. Therefore, it is an issue that should be precluded by an appropriate test.

1. The NiH main battery is a mixed CPV and IPV design and is a single-point failure for the system. The IPV cell is not a standard heritage item, but is a partially loaded CPV cell that was qualified by similarity to the CPV element.
2. Two CPV cells experienced shorts during vibration testing due to a manufacturing process problem. The problem was due to inadequate staking of insulators within the cell. Replacement of the entire battery lot was not possible due to time limitations, so an X-ray screening method was used to determine whether which batteries within the original lot were acceptable. Once selected, the cells were built up into the battery and successfully qualified.
3. The battery (and some other components) were not specifically tested and qualified for the parachute mortar shock/load, the parachute snatch load, or the landing load. Instead it was determined by analysis that the loads were acceptable. Qualification was performed via the random vibration test whose loads were considered sufficient to envelope the above cases.
4. Prime and redundant CCU operation is shut down prior to EDL in order to deadface the cruise solar array interface. Reactivation occurs after landing. This finding would not affect initial landed operations except in the event of a coincidental battery problem.
5. In addition to the battery, there are numerous other single-point failures associated with the power system wiring and distribution. These failure modes were effectively but not perfectly mitigated.
6. The MAD and associated MGA could not be operated during cruise. Therefore, first use occurred after landing on the surface of Mars.
7. The PDDU and PIU experienced late rework after system qualification to replace cracked diodes. Both units were successfully requalified and then reinstalled on the lander. The PIU was then removed for removal of PAL devices, then requalified and reinstalled for a second time. In both cases, the entire lander system successfully completed a comprehensive functional test.
8. The PIU test setup had a minimum threshold above the no-fire requirement for NSI devices. However, the combination of unverified parameters could not result in an accidental firing.
9. The PDDU uses 3/4-amp FM08-style fuses in numerous internal power supply fault protection locations. The 3/4-amp size is particularly susceptible to breakage and pulse damage due to its particular construction.
10. The MIMU unit requires a hermetic enclosure. The particular design uses a single O-ring seal system. The unit also does not include an internal pressure sensor. There is no evidence from flight data to suggest that the –A or –B units experienced a pressure loss problem.
11. The landing Radar system has a built-in test function that is unable to verify the Doppler section of the design. The four antennas and the T/R MUX device between the Radar output and antenna array also cannot be tested prior to first use.
12. The spoofing system used during ground Radar verification is relatively qualitative in nature and does not provide quantitative data regarding actual transmit power, receiver sensitivity, or absolute signal to noise ratio.
13. Neither the MGA nor the UHF antenna were tested for proper operation in the Mars landed 6-torr environment. Most of the ambient ground testing also bypassed the antennas resulting in limited system level verification for both items.
14. An ESD event during rework of the MGA damaged one of the two position encoders used for closed-loop control. The damaged unit but not the working unit was replaced. Based on

subsequent testing there is no evidence that the second part had latent damage. However, testing was very limited during system testing after integration.

15. The system level "plugs out" test used hard lines to the telecom system. As such, the ground connection to the system was not broken. As well, the MGA and UHF antenna were not verified as part of the setup.
16. The touchdown sensor design should have worked as expected from an electrical perspective. However, it has features and omissions that increase its noise sensitivity and reduce its performance margin.
17. The coaxial RF transfer switch is a potential single point failure for the X-band system. By definition, it can only be operated after loss of contact prior to EDL.
18. Both DST units experienced problems during testing (DST1 on Cassini) and required rework prior to flying on the lander. It is known that the DST1 unit was operating correctly, however, prior to loss of contact.
19. The pyro harness shielding used a single twisted-shielded pair for each output but did not include a second triax shield or over-wrap of the bundle. There is no evidence that this was a problem, but the susceptibility margins would have been reduced.

7.7 MPL Flight Software/Sequencing

INTRODUCTION

The MPL team at LMA presented their design and approach for several sequences. The team presented the logic for the various triggers for events during the EDL phase and for the early post-landed sequences. Several of these items had been discussed in previous Flight Software/Sequencing Review Team meetings. To illustrate problems with the software development processes, this report will focus on two of those sequences.

The first item deals with the logic presented for the uplink loss timer software. The second item deals with the logic in the thruster shutdown code upon sensing touchdown. The logic in both of these items had problems that could cause undesirable consequences.

7.7.1 Uplink Loss Timer Software Error

FAILURE MODE DESCRIPTION

The logic in the uplink loss timer software precludes switching from a failed uplink string to the backup uplink string, resulting in the loss of command capability to the spacecraft.

A set of logic facilitates switching hardware from a failed uplink hardware string to a redundant string. The logic is designed to switch if the spacecraft has not received a command from mission operations for a selected period of time. The time period that triggers the switch is a parameter in the software database; this parameter can be updated by commands from the mission operations system. The software records the time when a command is received and measures the elapsed time since that command was received. The software is designed to initiate a switch to the redundant uplink string when the time elapsed since the last received command is greater than the selected time period for switching defined in the software database. This logic was used during the cruise phase and during the landed phase of the mission. No problems occurred during the cruise phase.

For the landed mission operations, the values of the parameters in the logic are changed. There are also logic changes to the flight software for the command loss when the vehicle lands. At touchdown, the software saves the number of commands that have been received prior to the landing. Prior to storing the time of the last uplink and starting the countdown of the uplink loss timer, the logic in the software then searches for the time of a valid post-landed command. If this search indicates that no valid post-landed commands have been received, the logic skips the rest of the uplink loss timer software. The problem with this logic is as follows: the software can never take the action to switch to the redundant hardware string if the receive link fails during the EDL sequence. Because no commands are received on the failed receive string, the software logic will always skip around the rest of the command loss software and, consequently, will not switch to the redundant string. The result of this logic error is that a failed component in the uplink string of the lander during EDL would lead to a situation where the uplink loss logic could not switch to the redundant string.

A second error was caused by the selection of some database values. The configuration file parameter that controls the uplink component swap was set to 24 hours before the EDL sequence started. Consequently, a switch to the redundant string would occur if 24 hours elapsed without the receipt of a command. The software also resets this 24-hour timer (back to 24 hours) each time the spacecraft wakes up from a sleep mode. However, because the awake time never reaches 24 hours, the control timer never returns to zero and there would never be a string swap after landing. Therefore, the sequence had two sets of logic that would prevent the uplink loss software from switching to the redundant uplink string.

However, logic built into a sequence called "Sequence C" would in some cases provide a recovery path for the situations described above. Specifically, if no commands are received to change the sequence, Sequence C begins a few days after the landing. Sequence C commands the active uplink string to switch to the redundant string at a fixed time. Finally, Sequence C commands the spacecraft into the Safe Mode at the end of the multiple day sequence. Following these events, the spacecraft would then be restored to a configuration capable of receiving commands.

The logic for the landed uplink loss was poorly designed. However, as noted above, the mission could, in some cases, recover command capability through Sequence C. Therefore, the uplink loss software problem would not result in the total loss of the uplink capability unless a problem occurred with the loading or execution of Sequence C on board the spacecraft. An entry into safe mode after Sequence C started but before Sequence C commanded the uplink string swap, however, would cancel Sequence C and prevent the swap. It is not likely that the primary receive link failed during the EDL sequence. If this failure did occur, Sequence C execution would cause a switch to the backup uplink string (with the exception of the Uplink/Downlink Card in the Command and Data Handling Subsystem, which was not swapped by Sequence C).

DESIGN DESCRIPTION

The development of software follows the procedures outlined in the Software Management and Development Plan that was written for the Flight Systems Projects at LMA in Denver. The plan requires a software walkthrough process at each stage of flight software development; specifically, at the end of requirements definition, at the end of the design phase, at the end of the code phase, and, finally, when the test plan for unit testing has been prepared. A set of required attendees is established for each of these walkthroughs. The walkthroughs are intended to validate that:

1. The requirements are correct.
2. The software engineers understand the requirements.
3. The software design implements the requirements.
4. The code properly implements the design and provides the database for the code in the proper units.
5. The unit test properly demonstrates the functionality of the software unit and that all logic paths provide the desired response.

After successful completion of the unit test, the element of the software proceeds through further integration testing with the rest of the flight software. The total flight software package then undergoes rigorous sequence testing in the Systems Test Laboratory (STL) to demonstrate the full functionality using the actual flight software. Further testing of the software in the flight article lander is also done, to the extent that is practical. The STL test results are compared with the lander test results; the STL simulation is then upgraded to account for any differences. This process ensures the best fidelity simulation that the STL can provide for use during operations.

FINDINGS

1. The requirements for the uplink loss timer software were very similar to those defined for other planetary spacecraft missions. The walkthroughs were well attended. Minutes and action items were recorded.
2. The design of the uplink loss timer software introduced a failure mode that would not permit a switch to the backup string if the primary receive string failed during EDL. Design walkthroughs

focus primarily on the interface design of the software; therefore, the detailed design review occurs during code walkthrough. The logic problems were not found in the design walkthrough. Logic flow diagrams were not used during the walkthrough; it is difficult to find logic errors by walking through the code without logic flow diagrams to help the process.

3. The code walkthrough did not discover the design error in the uplink loss timer software (the logic that required a command to be received by the failed receive string before it could process the rest of the timer countdown and subsequently switch to the redundant string). Design and code walkthroughs do not evaluate flight data parameters; Product Integrity Engineers are responsible for their flight data parameters. Flight data parameter reviews were held with systems engineering, operations teams, and subsystems representatives prior to mission-critical events: pre-ATLO, pre-launch, and pre-EDL. A value corresponding to 24 hours should never be used for the flight data parameter in question in a landed mission phase.
4. The test walkthrough process did not present a test case that demonstrated the correct results in the presence of a failed receiver after landing. Apparently, the test cases tested the cruise-phase logic and did not include the extra logic that required a command to be received in the failed uplink string to initiate the landed uplink loss timer software. The actual landed sequence parameters that caused the failure to switch were not tested anywhere.
5. The actual software errors were not found in any of the software walkthroughs. These errors could have been found in the design and code walkthroughs if the right questions had been asked.
6. The software integration tests did not detect the problems in the uplink loss timer software. There were several tests that crossed the boundary between EDL and the landed mission phase. After the successful EDL landing, each test uplinked commands to configure the uplink loss fault case. That is not the proper logic for testing the ability of the lander software to switch to the redundant element should a failure have occurred during the EDL sequence.
7. The uplink loss timer software problems were not detected before launch or during the cruise phase of the flight. Instead, the problems were found after the landing, during the analysis of the suspected failures defined using a fault-tree analysis.

PROCESS ASSESSMENT

The software development process as defined in the Software Development and Management Plan is adequate and appropriate. However, the software did include a design error that was not detected in the software walkthrough process or discovered in subsequent testing of the software. The design error was discovered after a fault-tree analysis led to the examination of the code and the preparation of code descriptions for reviews by outside reviewers. There may be a clue here that suggests something is missing in the process (see Lessons Learned 4 below). The use of logic flow diagrams to illustrate the logic — instead of trying to understand the logic by reading the code — would provide more visibility for the walkthrough reviewers.

LESSONS LEARNED

1. Consider performing a fault-tree analysis prior to spacecraft test planning to define the test cases that are needed to drive out the logic paths that must be tested.
2. Review the flight software problems (and related mission operations software problems) that have occurred on Stardust, MCO, and MPL, as documented in Software Problem Reports, Problem/Failure Reports (P/FRs), and Incident/Surprise/Anomaly (ISA) Reports. Try to identify any process problems that have led to those problems. Correct the processes as a means to eliminating the problems on future missions. For example, try to understand why the two landed uplink loss errors were not found during the walkthrough process. One of these errors was obvious; the other required a detailed analysis of the interaction between two database parameters.

3. Use software flow diagrams and logic charts to aid in understanding the software design and in troubleshooting problem areas. These charts can also be used to identify the test cases that must be run to verify that the logic provides the desired actions.
4. Specifically for the database parameter-error problems:
   a) Conduct software testing with realistic database values and test conditions to demonstrate that uplink loss achieves the desired switch to the backup string when the primary string fails.
   b) Prepare a detailed plan to test the software during the transition from one mission phase to another (for example, from EDL to the landed phase). The testing must be done with the database parameters that will be in place at the beginning of the new phase.
   c) When changes are made to the database parameters that are involved in logic decisions, retest the logic must to verify that the desired actions are implemented.
   d) Ensure that the database is required to contain information describing the detailed derivation of every parameter value. As applicable, the database also needs to include constraint checking to ensure that only parameter values within an allowable range are used.
5. Software test teams need to assume that there is an error in the flight software. During testing, the teams must examine every requirement on the software to test whether they can identify a set of conditions that could "break" the software.

7.7.2 Premature Descent Engine Shutdown

FAILURE MODE DESCRIPTION

A spurious signal, generated when the landing legs are deployed at an altitude of about 1500 meters, can cause premature descent engine shutdown when the lander is 40 meters above the surface.

The three landing legs are deployed from their stowed condition to the landed position at an altitude of about 1500 meters while the lander is still attached to the parachute. Each leg is fitted with a Hall Effect magnetic sensor that generates a voltage when its leg contacts the surface of Mars. The descent engines are shut down by a command initiated by the flight software when the first landing leg senses touchdown. If the touchdown sensor in that leg fails to detect the touchdown, the second leg to touch down will trigger the engine shutdown. This logic is intended to prevent the lander from tipping over when it has a skewed attitude relative to the surface during touchdown. It is important to get the engine thrust terminated within 50 milliseconds after touchdown to avoid overturning the lander. The flight software is also required to protect against a premature touchdown signal or a failed sensor in any of the landing legs.

The touchdown sensors characteristically generate a false momentary signal at leg deployment. This behavior was understood and the flight software was required to ignore these events; however, the requirement did not specifically describe these events, and consequently, the software designers did not properly account for them. The resulting software design recorded the spurious signals generated at leg deployment as valid touchdown events. When the sensor data were enabled at an altitude of 40 meters, the engines would immediately shut down. The lander would free fall to the surface, impacting at a velocity of 22 meters per second (50 miles per hour), and be destroyed.

DESIGN DESCRIPTION

The design logic to implement the requirements is shown in the flow diagram in Figure 7-8.

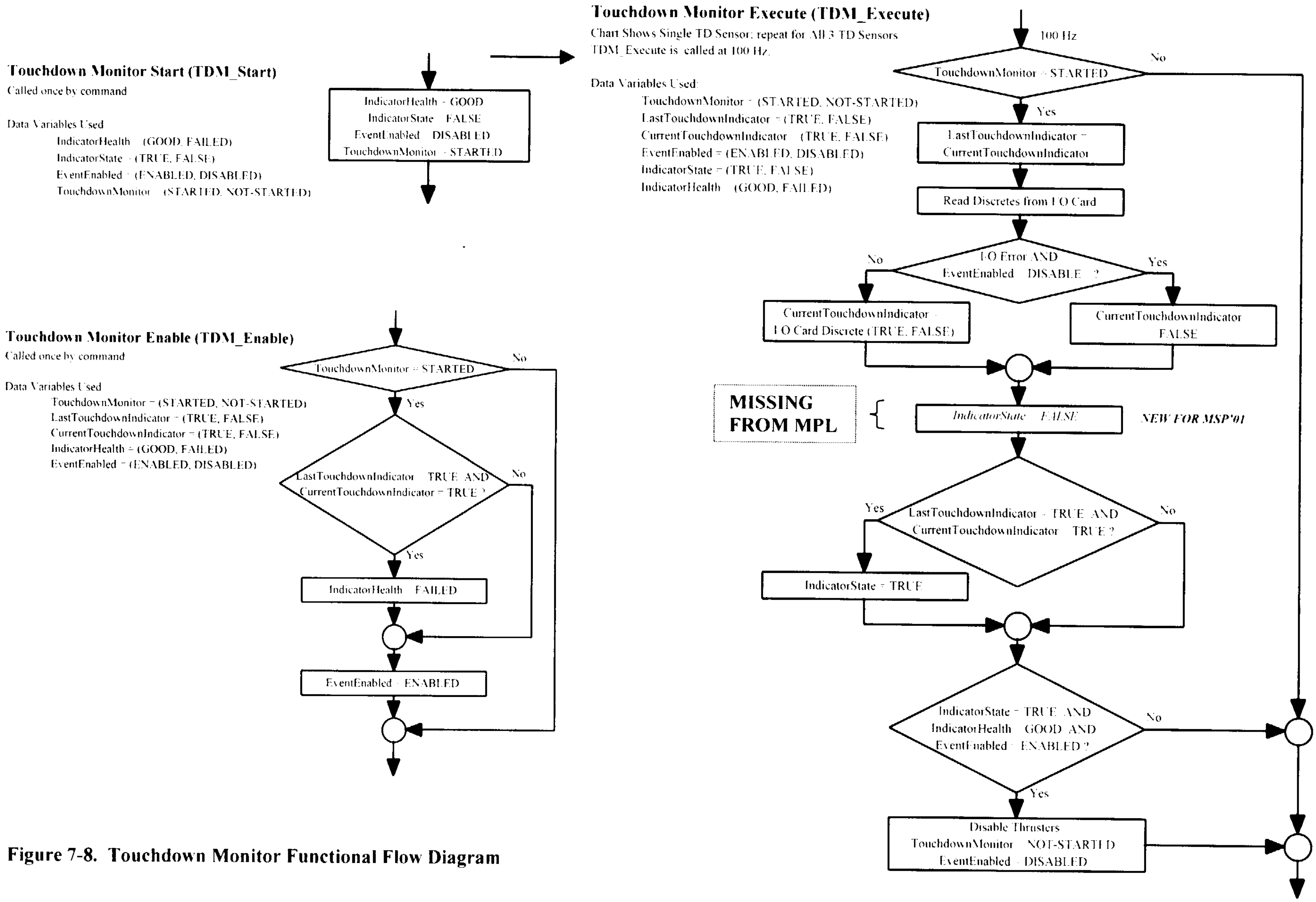

Touchdown Monitor Start (TDM_Start)
Called once by command
Data Variables Used
IndicatorHealth = (GOOD, FAILED)
IndicatorState = (TRUE, FALSE)
EventEnabled = (ENABLED, DISABLED)
TouchdownMonitor = (STARTED, NOT-STARTED)
IndicatorHealth = GOOD
IndicatorState = FALSE
EventEnabled = DISABLED
TouchdownMonitor = STARTED
Touchdown Monitor Enable (TDM_Enable)
Called once by command
Data Variables Used
TouchdownMonitor = (STARTED, NOT-STARTED)
LastTouchdownIndicator = (TRUE, FALSE)
CurrentTouchdownIndicator = (TRUE, FALSE)
IndicatorHealth = (GOOD, FAILED)
EventEnabled = (ENABLED, DISABLED)
TouchdownMonitor = STARTED
Yes
No
LastTouchdownIndicator = TRUE AND CurrentTouchdownIndicator = TRUE ?
Yes
No
IndicatorHealth = FAILED
EventEnabled = ENABLED
Touchdown Monitor Execute (TDM_Execute)
Chart Shows Single TD Sensor; repeat for All 3 TD Sensors
TDM_Execute is called at 100 Hz.
Data Variables Used:
TouchdownMonitor = (STARTED, NOT-STARTED)
LastTouchdownIndicator = (TRUE, FALSE)
CurrentTouchdownIndicator = (TRUE, FALSE)
EventEnabled = (ENABLED, DISABLED)
IndicatorState = (TRUE, FALSE)
IndicatorHealth = (GOOD, FAILED)
100 Hz
TouchdownMonitor = STARTED
No
Yes
LastTouchdownIndicator = CurrentTouchdownIndicator
Read Discretes from I/O Card
I/O Error AND EventEnabled = DISABLE ?
No
Yes
CurrentTouchdownIndicator = I/O Card Discrete (TRUE, FALSE)
CurrentTouchdownIndicator = FALSE
MISSING FROM MPL
IndicatorState = FALSE
NEW FOR MSP'01
LastTouchdownIndicator = TRUE AND CurrentTouchdownIndicator = TRUE ?
Yes
No
IndicatorState = TRUE
IndicatorState = TRUE AND IndicatorHealth = GOOD AND EventEnabled = ENABLED ?
No
Yes
Disable Thrusters
TouchdownMonitor = NOT-STARTED
EventEnabled = DISABLED

Figure 7-8. Touchdown Monitor Functional Flow Diagram

The logic uses six variables, defined as:

1. *Touchdown Monitor*. This parameter can have two conditions: Started or Not Started. This parameter is set to the Started state approximately 12 minutes before the Radar senses the 40-meter enable altitude.
2. *Last Touchdown Indicator*. This parameter is the reading of the state of the Hall Effect sensor as it is sampled at 10-millisecond intervals. "Last" means the state that it indicated during the previous 10-millisecond sample. This indicator has two conditions: True or False. True is a touchdown signal from the sensor. False is a non-touchdown indication.
3. *Current Touchdown Indicator*. This parameter has the same two conditions as the Last Touchdown Sensor reading. However, this parameter is sampled in the current 10-millisecond sampling interval.
4. *Event Enabled*. This is the engine shutdown enable gate parameter that is initially set at Disabled when the sequence begins and then is set to Enabled when the Radar senses 40 meters altitude.
5. *Indicator State*. This is the state of the landing leg touchdown indicator in one of the three landing legs. True means the Hall Effect sensor has been on for two consecutive 10-millisecond samples. False means that the sensor has not sensed two consecutive On sensor samples.
6. *Indicator Health*. This is the Hall Effect sensor health as determined by a sequence that is running just before the sequence represented in Figure 7-8. The health is set to Failed if two consecutive touchdown sensor readings are on before the touchdown event is enabled. Otherwise, this indicator reads Good.

The sequence starts with a command from the flight software (FSW OBJECT START) approximately 12 minutes before the Radar detects the 40-meter altitude. The sequence starts by initializing some parameters one time in the Touchdown Monitor Start (TDM_Start), shown in the upper left corner of Figure 7-8. Indicator Health is set to Good, Indicator State is set to False, Event Enabled is set to Disabled, and Touchdown Monitor is set to Started. The sequence then continues through the Touchdown Monitor Execute sequence shown on the right side of Figure 7-8. Because the Touchdown Monitor has already been set to Started, the logic sets the state of the Last Touchdown Indicator to the value stored in the Current Touchdown Indicator, which is the False state. The logic then reads the sensor status on the Input/Output (I/O) card at the 100-Hz rate, one leg at a time, approximately 6 minutes prior to entry. If there is an error indicated on the I/O card and the Radar has not yet sensed the 40-meter altitude (Event Enabled = Disable), the Current Touchdown Indicator is set to the False state. If there is no I/O error and the Radar has detected the 40-meter altitude (Event Enabled = Enabled), the Current Touchdown Indicator is set to the True or False reading it has read from the I/O card.

The next step on the diagram shows a line of code (Indicator State = False) that the Mars 2001 program added to correct the logic. That line was not included in the MPL code; therefore, we proceed to the next step. The logic asks if both the Last Touchdown Indicator and the Current Touchdown Indicator are in the True state. If they are, the Indicator State is set to True, which indicates that the sensor in that leg indicates that touchdown has occurred. If the answer is no, the Indicator State is not changed. The sequence then asks whether the Indicator State is true, whether the Indicator Health is Good, and whether the Event Enabled is Enabled. If the responses to those questions are yes, Descent Engine Thrust Termination is commanded. If any of those states are not satisfied, the logic returns to the beginning of the Touchdown Monitor Execute (TDM_Execute) and the process repeats.

When the Radar senses that the 40-meter altitude has been reached, the flight software commands the Touchdown Monitor Enable (TDM_Enable) to start (shown at the bottom left of Figure 7-8). The first step checks the state of the Touchdown Monitor, which has already been initialized to the Started state. The logic then continues to the next step, where it asks if the Last Touchdown Indicator and the Current Touchdown Indicator are both set to the True state. If that is so, the Indicator would have turned on erroneously before the 40-meter altitude was reached; therefore, the logic sets the Indicator Health to the Failed state. If the answer to the logic is no, the Indicator Health state is not changed from Good to Failed. The next step is to set Event Enabled to the Enable state, thereby indicating that the 40-meter altitude has been reached. The software then returns to the Touchdown Monitor Execute (TDM_Execute) sequence shown at the right side of Figure 7-8. The logic continues to repeat this sequence until any of the three touchdown sensors has two consecutive True readings. If the Indicator Health is Good (since the Event Enabled would now be Enabled), the Engine Thrust Termination command is issued. The Touchdown Monitor state is changed to Not Started and the monitor sequence is ended.

The problem with the logic is as follows: The landing leg deployments are complete at entry plus 4 minutes 13 seconds. If a touchdown sensor is stimulated by leg deployment dynamics long enough for the flight software to sense two consecutive On states from the sensor, the Indicator State is set to True. This means that the Hall Effect sensor in that leg has provided information that makes the flight software sense that touchdown has been signaled by that leg. If any of the three legs exhibit the dynamics to trigger the two consecutive sensor True states, the Touchdown Indicator state for that leg will be set to True for that sensor. When the transient dynamics have damped out, the sensor continues to be read by the flight software; however, the sensor will not provide an indication of True. At approximately entry plus 5 minutes 16 seconds, the lander altitude is at the 40-meter altitude gate. The flight software uses the previous and current sensor state to determine the touchdown sensor state. Any sensor that shows Touchdown (True) is marked as Failed on the Indicator Health and the sensor data are ignored for the rest of the timeline. However, the flight software does not reset the Indicator State to False; instead, the indicator remains as True. (*Note*: The Mars 2001 project has corrected this code and it does reset the Indicator State to False.) Because the dynamics that originally set the touchdown sensor to an On condition are no longer present at this time, the previously stimulated sensor now correctly reads "No Touchdown" and the Indicator Health is marked Good for that sensor.

As the logic proceeds to the next step, three conditions are checked. If the Indicator State is True, the Indicator Health is Good, and the Touchdown Event is Enabled, the command to terminate thrust of the descent engines will be issued. Since all three of these conditions are met when the spurious signal has occurred, the engines will shut down prematurely, shortly after the Radar has sensed the 40-meter altitude. The result is that the lander has a velocity of approximately 13 meters per second and is accelerating at the Martian gravity of 3/8 g. The lander strikes the Martian surface at approximately 20 meters per second. (*Note*: The correction provided by the 2001 flight software would prevent descent engine shutdown until the real touchdown occurs.)

Testing of the lander leg deployments showed some transients in the Hall Effect sensor output following the initiation of leg deployment. Many tests with an MPL EDU and with the actual MPL flight legs showed that the mean duration of the transient signal ranges from 5 to 33 milliseconds. There were six tests that had no transient, but there was reason to believe that there was a problem with the sensor or the landing leg during those tests. At the sensor-sampling rate of 10 milliseconds, getting two successive True indications and initiating a premature engine thrust termination would always happen for transients of 20 milliseconds or greater. For transients of less than 10 milliseconds, there would never be two successive True readings of the sensor and there would not be a premature thrust termination. For transients between 10 and 20 milliseconds, there was a possibility of two consecutive True readings, depending on the phasing of the sampling within the transient time period. A preponderance of all the leg deployment tests on the MPL EDU and on the MPL flight-article landing legs demonstrated touchdown sensor transients that would have resulted in premature descent engine thrust termination. The landing legs on the EDU had many tests; it was suspected that the transient time may no longer be representative of the actual MPL transient. The MPL flight legs were only being deployed for the third time during the actual EDL sequence. Therefore, a 2001 lander was used for two leg deployment tests of all three legs in a thermal–vacuum chamber with temperatures representative of what they would be in the Martian environment. The first test resulted in transient times of 12, 26.5, and 7.3 milliseconds on the three legs located at 0, 120, and 240 degrees, respectively. The second test resulted in transient times of 16, 12, and 25 milliseconds at those leg positions. An analysis of the data indicated that the first test would have resulted in a premature descent engine thrust termination from the transient on the leg at the 120-degree position. The second test would have resulted in a premature descent engine thrust termination from the transients on the leg at the 0-degree position and on the leg at the 240-degree position. These tests were much more representative of the MPL conditions during the terminal descent than were the EDL tests. The conclusion drawn from all the testing was that it was likely that premature descent engine thrust termination was experienced by MPL on 3 December 1999, assuming that the MPL was still healthy by the time terminal descent began. (References: Mars Polar Lander Touchdown Sensor Code Issue, January 28, 2000, LMA viewgraph presentation, H.H. Curtis; Appendix to that presentation: Touchdown Monitor FSW Description, G. Bollendonk; Mars Polar Lander Premature Descent Engine Termination Due to Touchdown (TD) Indication Conclusions, February 25, 2000, LMA viewgraph presentation, H.H. Curtis, R. Gehling, J. Bene, G. Bollendonk.)

The lack of telemetry during EDL made it impossible to determine if the landing leg deployment transients set the touchdown state to True during the leg deployment. Since there was no post-landed telemetry, there is no information regarding the time of the descent engine thrust termination.

PROCESS ASSESSMENT

The system-level requirements document that defined the requirements for the touchdown sensing had three requirements (defined in Change Summary XB0114) that are pertinent to understanding what happened in the software design, as follows:

1. The touchdown sensors shall be sampled at 100-Hz rate. The sampling process shall be initiated prior to lander entry to keep processor demand constant. However, the use of the touchdown sensor data shall not begin until 12 meters above the surface. (*Note*: The altitude was later changed from 12 meters to 40 meters above the surface.)
2. Each of the three touchdown sensors shall be tested automatically and independently prior to use of the touchdown sensor data in the onboard logic. The test shall consist of two (2) sequential sensor readings showing the expected sensor status. If a sensor appears failed, it shall not be considered in the descent-engine termination decision.
3. Touchdown determination shall be based on two sequential reads of a single sensor indicating touchdown.

The requirement to not use the sensor data until reaching the 40-meter altitude was put in place to protect against premature descent engine thrust termination in the event of failed sensors and possible transients. However, the requirement did not specifically state those failure modes. The software designers did not include in the design of the software a mechanism to protect against transients, nor did they think they had to test for transient conditions. The problem was compounded during the flowdown of the requirements to the Software Requirements Specification (SRS). All the requirements in the Change Summary were picked up in the SRS *except* for the following: "However, the use of the touchdown sensor data shall not begin until 12 meters [later changed to 40 meters] above the surface."

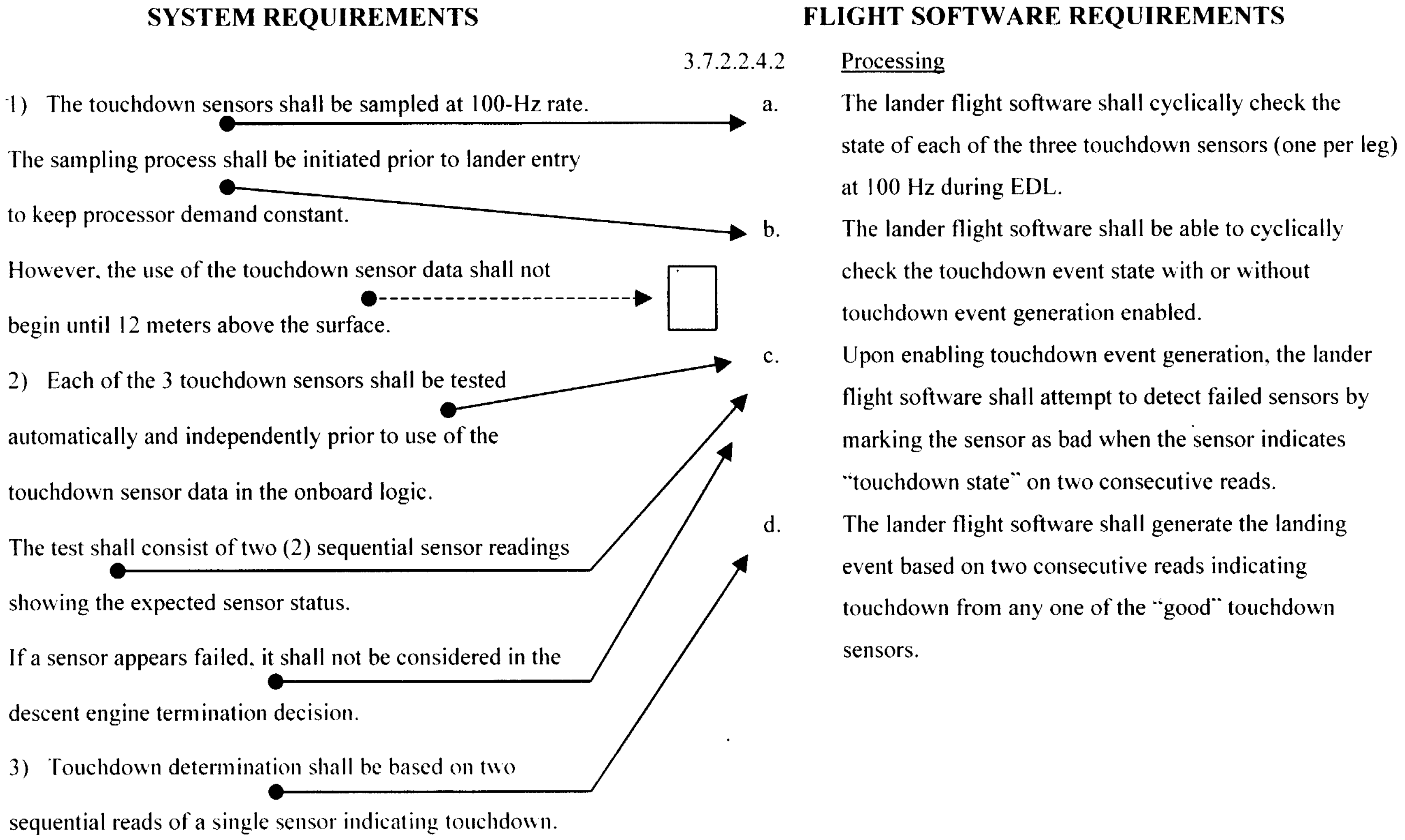
Figure 7-9 shows the flowdown from the system requirements from the Engineering Change Summary to the flight software requirements, as they were documented in the SRS (with the exception of the use of the touchdown sensor not beginning until 12 meters above the surface).

The omission of that requirement in the SRS may have led the software designers to allow the Indicator State to be set to True during the data processing prior to the Radar sensing of the 40-meter altitude. Because the requirement was not in the SRS, the software designers may not have seen the need to reset the state to False upon reaching the 40-meter altitude. Its omission in the SRS may also have led to the failure to test that requirement in the unit-level tests, and it was not included in the requirements to be verified by system testing. Therefore, the requirement was never tested at the unit-test level or at the system level. (Reference: Mars Polar Lander Touchdown Sensor Code Issue, February 11, 2000, LMA viewgraph presentation, H.H. Curtis.)

The requirement to keep processor demand constant by initiating the sampling process prior to entry was the result of lessons learned from other missions. It was intended to avoid transients in the CPU loading that had caused problems on other programs. This requirement led the software designers to start sampling the sensor data well before the 40-meter altitude had been obtained. In hindsight, it would have been better not to do any sampling of the touchdown sensors prior to the 40-meter altitude. The transients in the Hall Effect sensor due to landing leg deployment would have been over by then.

The software designers did test the sensors prior to their use at the 40-meter altitude with a routine that checked the sensors right after the Radar sensed the altitude. That routine labeled any sensor that was on for two consecutive samples to be labeled as a "bad" sensor and not used. The transient would not be present at that time in the EDL sequence, so the sensor that had the transient (and showed an indication of touchdown during the transient) would now pass the test as a healthy sensor. The sensor touchdown state that was set as True during the transient would still be in the True state, and since the enable was then present, all the conditions for descent engine thrust termination would be present. Because the software designers and systems engineers were not aware of the transient behavior from the Hall Effect sensors, the people participating in the walkthrough process did not catch the software problem.

The requirements for the touchdown sensing logic were not changed after the landing leg deployment tests established the likelihood of transient response of the Hall Effect sensors to the leg dynamic effects. This may have been the result of the mechanical design personnel not informing the systems and software personnel of the results in a timely manner. Perhaps, if the Systems Engineer was told, he or she may have thought that the problem was solved by the requirement not to use the touchdown sensor data until the 40-meter altitude had been reached. By that time, the transient would no longer be present. The combination of that requirement and the requirement to initiate the sampling process prior to entry to keep the processor demand constant put everything in place for the flight software to be vulnerable to a transient, triggering a premature engine shutdown. The systems and software personnel may not have informed the mechanical design personnel of the software design that was used to detect touchdown and to disable sensors that indicate a premature touchdown signal. If that is true, the mechanical design personnel would not have been sensitive to the problems that a transient would cause.



SYSTEM REQUIREMENTS

1) The touchdown sensors shall be sampled at 100-Hz rate.

The sampling process shall be initiated prior to lander entry to keep processor demand constant.

However, the use of the touchdown sensor data shall not begin until 12 meters above the surface.

2) Each of the 3 touchdown sensors shall be tested automatically and independently prior to use of the touchdown sensor data in the onboard logic.

The test shall consist of two (2) sequential sensor readings showing the expected sensor status.

If a sensor appears failed, it shall not be considered in the descent engine termination decision.

3) Touchdown determination shall be based on two sequential reads of a single sensor indicating touchdown.

FLIGHT SOFTWARE REQUIREMENTS

3.7.2.2.4.2 Processing

a. The lander flight software shall cyclically check the state of each of the three touchdown sensors (one per leg) at 100 Hz during EDL.

b. The lander flight software shall be able to cyclically check the touchdown event state with or without touchdown event generation enabled.

c. Upon enabling touchdown event generation, the lander flight software shall attempt to detect failed sensors by marking the sensor as bad when the sensor indicates "touchdown state" on two consecutive reads.

d. The lander flight software shall generate the landing event based on two consecutive reads indicating touchdown from any one of the "good" touchdown sensors.

Figure 7-9. MPL System Requirements Mapping to Flight Software Requirements

Even though the software walkthrough process is well defined and the walkthroughs are well attended, the existence of the Hall Effect sensor transient response during leg deployment was not known. (It should be noted that the Hall Effect sensor Product Integrity Engineer was not present at the walkthroughs.) Thus, it was not discussed during the walkthroughs, nor were suitable test cases defined to test the software with conditions representing the transient response of the system.

FINDINGS

1. Protection from transient signal behavior of the touchdown sensors was not specifically called out in the requirements. The requirement that specified that "the use of the touchdown sensor data shall not begin until 12 meters above the surface" was intended to eliminate any danger from sensor failure modes, including transients. However, that requirement was not included in the SRS in the requirements flowdown process, and it was not included in the requirements to be verified during system testing. The protection from transient signal behavior was not adequately captured in the system or subsystem requirement specifications, nor in the system-level test requirements. Therefore system, subsystem, and test teams did not verify transient signal immunity during software and system testing.
2. The software errors described were not found in any of the software walkthroughs prior to EDL. The missing requirement in the SRS was a contributor to the problem.
3. The walkthroughs apparently did not consider the impact of dynamic transient behavior from the Hall Effect sensors during landing leg deployment. A component test of the landing leg deployment was accomplished on 16 June 1997. That test provided an indication of the transient response from the Hall Effect sensors to the dynamics of the deployment. The importance of that transient was not recognized. The code walkthrough of the touchdown-sensing code was held on 30 June 1997 without consideration of the effects of that transient on the outcome of the sequence.
4. The walkthroughs did have the proper attendance at the meetings, although the Hall Effect sensor Product Integrity Engineer was not present at those walkthroughs. Because the sensor Product Integrity Engineer would probably have been aware of the presence of the Hall Effect sensor transient behavior during the leg deployments, he could have provided the software designers with that information during the walkthroughs.
5. Action items were properly recorded and later closed out.
6. The unit test cases did not provide a test that would have caught the logic errors in response to transients in the Hall Effect sensors. The software integration tests also did not detect the transient response problems in the software. The unit test cases were not intended to test for transients from the Hall Effect sensors. The unit test cases are intended to verify stated software requirements; the missing requirement in the SRS contributed to this problem. The intent of the requirement to not use any touchdown sensor data prior to the 40-meter altitude was to eliminate premature touchdown indications. If protection from deployment transients was a software requirement, a unit test would have caught this problem. A test to verify that sensor data prior to the 40-meter altitude was not used, but also could have caught this problem.
7. A system leg deployment test was performed on 4 June 1998 during spacecraft testing with the flight software touchdown code operating. Even though transients due to dynamic response of the Hall Effect sensors were probably present, they were not detected, nor was touchdown detected when technicians pushed up on the footpads to simulate touchdown. It was later discovered that the Hall Effect sensors were improperly wired because of an error in the wiring drawing, and the wiring error prevented the sensor response from being monitored. The legs were then rewired to correct the error. The technicians again pushed up on the footpads and the sensors indicated a touchdown had been sensed. However, the leg deployment test was not repeated after the wiring error was corrected. A rerun of that test with the proper wiring in place might have detected the software logic problem in the presence of the leg-rebound transient.

8. The software was tested for the failure of a Hall Effect sensor to a constant On condition. That test detected the errant condition of the sensor and marked it as a bad sensor. That sensor was then ignored in the touchdown sensing, as it should have been, and no premature engine-thrust termination occurred. A proper shutdown occurred when other sensors sensed the true touchdown event. That gave the software and systems engineers some confidence that the software was working properly, but the failure mode of an intermittent signal from the Hall Effect sensor was not tested. Therefore, the problem remained undetected in the design.
9. LMA MSP engineers presented the software issue described above to the Review Teams meeting at LMA in Denver. It was not detected in software walkthroughs or unit tests, nor was it found during the cruise phase of the flight. The touchdown sensor problem was found during a test run on the 2001 Lander when a test engineer pushed a button indicating a touchdown too early in the test. He released the button when he realized his error and was surprised when thrust termination occurred prematurely. That led to a failure analysis that uncovered the software problem.

LESSONS LEARNED

1. All the hardware inputs to the software-decision logic must be identified. The character of the inputs must be documented in a set of system-level requirements. The appropriate verifications must result from the requirements. Test planning needs to have a checklist that includes a requirement to test logic in the presence of transients or spurious signals.
2. Product Integrity Engineers must attend software walkthroughs when the software that interfaces with their equipment is being reviewed.
3. Examine the LMA software walkthrough process and integration and test process to look for clues that would indicate why the processes are not catching software logic errors. Consider using logic flow diagrams to provide visibility into the software design and review them at the design walkthrough. It gets more difficult to find these kinds of errors by inspecting the code, although it is still possible to find them at the code level.
4. Review the flight software problems (documented in Software Problem Reports, P/FRs, and ISAs) that have occurred on Stardust, MCO, and MPL. Try to identify the process problems that have led to those problems, and then correct the processes in an effort to eliminate a recurrence of these types of flight software problems.
5. Systems engineering must stay on top of test results from all areas and be aware of the possible impact of surprises or unusual test results. They must communicate their findings to other areas of the development project.
6. The engineers conducting development testing must accept the responsibility to make sure their test results are being communicated to the rest of the project disciplines, especially systems engineering. Systems engineering must review software requirements to make them consistent with the idiosyncrasies discovered during the test program.
7. When important tests are aborted or are known to be flawed due to configuration errors, they must be rerun after the configuration errors are fixed. If any software or hardware involved in a test are changed, the test must be rerun to demonstrate the correct functionality.
8. Software test teams need to examine every requirement on the software to see whether there is a set of conditions that could cause the software to fail.

Bibliography

LMA memorandum: from Thomas C. McCay to Shane Koskie, regarding Touchdown Sensor Miswire on the MPL in June 1998, February 14, 2000.

LMA report: LMSS-DO Investigation of Process Contributors to Mars Polar Lander Premature Thrust Termination Due to Touchdown Indication, March 5, 2000.

LMA viewgraph presentation: Functional Flow Chart, HHC-1.

LMA viewgraph presentation: Mars Polar Lander Premature Descent Engine Termination Due to Touchdown (TD) Indication Conclusions, February 25, 2000, H.H. Curtis, R. Gehling, J. Bene, and G. Bollendonk.

LMA viewgraph presentation: Mars Polar Lander Touchdown Sensor Code Issue, January 28, 2000, H. H. Curtis — Lander Systems Engineering, with an Appendix: Touchdown Monitor FSW Description, G. Bollendonk, MPL Flight Software.

LMA viewgraph presentation: Mars Polar Lander Touchdown Sensor Code Issue, February 11, 2000, H.H. Curtis – Lander Systems Engineering.

LMA viewgraph presentation: System Requirement Mapping to FSW, HHC31.

LMA viewgraph presentation: Timeline, HHC-3.

Mars Polar Lander Possible Premature Descent Engine Thrust Termination Process Investigation Report — Joseph Vellinga, MSP-00-5001, 02/10/00; via e-mail from J. Vellinga, 02/11/00.

Mars Surveyor Program (MSP) change summary: Lander Descent Velocity Change and Touchdown Sensor Change, UCN XB0114, September 18, 1996.

8 SUMMARY OF POTENTIAL DS2 FAILURE MODES

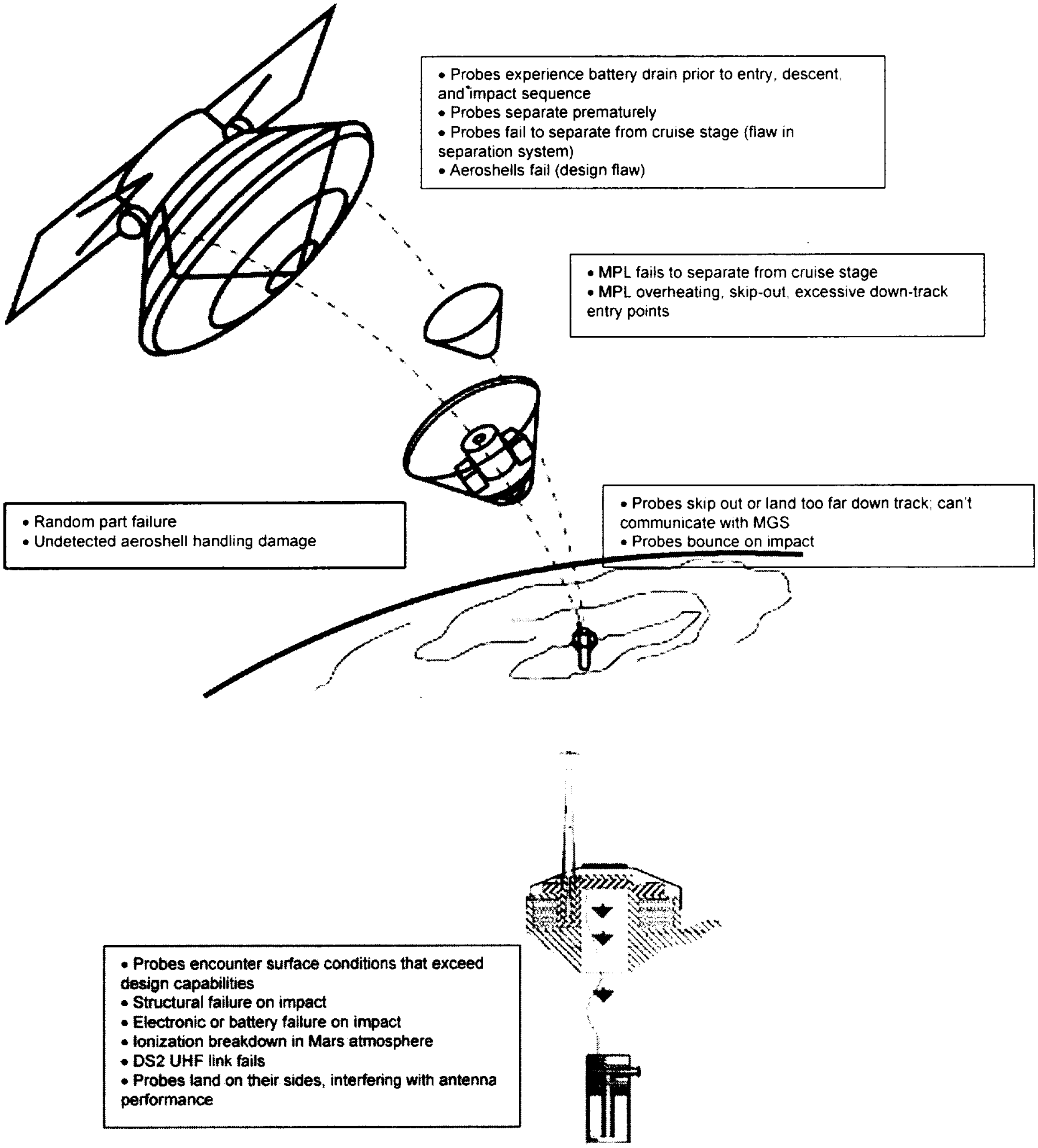
This section provides a summary description of the DS2 potential failure modes considered by the Board. It also provides a high-level assessment of the plausibility of each of the failure modes based on the Board's review of the relevant design, implementation, and test history, and what may be inferred from data obtained throughout the mission operations. References are made to Sections 9, which contains detailed descriptions of the failure modes summarized in this section, along with findings and Lessons Learned.

Failure modes are divided into two groups:

- Failure Modes Affecting Both Probes
- Failure Modes Affecting a Single Probe

The four DS2 potential failure modes identified by the Board as plausible are highlighted as *FLAG 1*, *FLAG 2*, *FLAG 3*, and *FLAG 4*.

Figure 8-1 illustrates the DS2 entry, descent, and impact (EDI) sequence and shows potential failure modes.



- Probes experience battery drain prior to entry, descent, and impact sequence
- Probes separate prematurely
- Probes fail to separate from cruise stage (flaw in separation system)
- Aeroshells fail (design flaw)

- MPL fails to separate from cruise stage
- MPL overheating, skip-out, excessive down-track entry points

- Random part failure
- Undetected aeroshell handling damage

- Probes skip out or land too far down track; can't communicate with MGS
- Probes bounce on impact

- Probes encounter surface conditions that exceed design capabilities
- Structural failure on impact
- Electronic or battery failure on impact
- Ionization breakdown in Mars atmosphere
- DS2 UHF link fails
- Probes land on their sides, interfering with antenna performance

Figure 8-1. DS2 Entry, Descent, and Impact Sequence with Potential Failure Modes

8.1 DS2 Failure Mode Assessments

8.1.1 Failure Modes Affecting Both Probes

Failure Mode	Assessment
Both probes separate prematurely.	IMPLAUSIBLE. This failure mode is implausible during the launch environment prior to spacecraft separation from the launch vehicle because the probes would have impacted and damaged the cruise stage solar panels. There is no evidence of this in flight. Additionally, no plausible failure mode for premature separation of the probes after spacecraft separation has been identified. See Section 9.2.1.
Both probes experience battery drain prior to EDL due to: —Sneak path electrical transient, e.g., at launch vehicle separation —EMI effect, e.g., from Range or launch vehicle emitted radiation —Plasma discharge, e.g., from pyro firings	PLAUSIBLE BUT UNSUPPORTED. There are several design deficiencies associated with the probe power switch circuit. The most critical of these could result in inadvertent turn-on of the probe and premature battery depletion. Inadvertent probe activation did occur during the final hardware assembly activity but was discovered before significant battery depletion. Several mitigation steps were subsequently implemented to minimize the chance for reoccurrence during processing or after integration with the MPL cruise stage. Although it is believed that these mitigation steps were successful, the actual circuit deficiency could not be corrected. See Section 9.3.
Both probes fail to separate from cruise stage due to systematic flaw in the probe separation system.	IMPLAUSIBLE. Judged not plausible based on a review of the design and test program. See Section 9.2.3.
Aeroshells fail on both probes due to systematic flaw in the aeroshell design.	IMPLAUSIBLE. Judged not plausible based on a review of the design and test program. See Section 9.2.4.
Both probes skip out or land too far down track to be able to communicate with MGS due to atmospheric model errors, e.g., density lower than design range.	IMPLAUSIBLE. The penetrator shape (the critical aerodynamic design factor) was selected to be identical to the Viking and Pathfinder designs to take advantage of these well-established databases. Some updates to the Mars atmosphere database were made based on MGS data, and the modeling approach has been independently verified by LaRC.
FLAG 1 Both probes bounce on impact due to unanticipated surface effects, e.g., lubrication effects of upper layer.	PLAUSIBLE. Probe impact on an ice surface was not a design requirement and not tested during development because this possibility was believed unlikely. This condition still seems unlikely, but cannot be ruled out. As another example, the MGS site survey suggests at least a few centimeters of soft material on top of whatever the underlying material may be. Since this soft material would support only a minimal shear force, it could act as a lubricant that would make penetration of any smooth hard underlying material less likely. See Section 9.1.2.
Both probes suffer structural failure at impact.	PLAUSIBLE BUT UNSUPPORTED. The probe aft-body, without the aeroshell, was empirically designed to withstand the impact tests. Due to lack of a suitable air gun, an impact test of the probe integrated with the aeroshell was never successfully conducted, preventing full characterization of the dynamic interaction between the aeroshell and the aft-body. The probe did survive the impact tests to which it was subjected. See Section 9.2.5.

Failure Mode	Assessment
FLAG 2 Both probes suffer electronic or battery failure at impact.	PLAUSIBLE. The DS2 project implemented a qualification program whose goal was to mitigate the potentially destructive effect of probe impact with the Mars surface. This program concentrated on qualification of the design approach, associated processes, and critical devices using engineering or otherwise representative hardware. Testing was performed on the hardware in an unpowered state with inspection and functional testing (where possible) performed pre- and post-test. Survival of a particular process method or hardware element constituted acceptable qualification. More than 50 impact tests were performed per the above described incremental build–test strategy. It was fundamentally successful as a method for qualifying the design and assembly approaches, but was incomplete with respect to qualifying several of the key subsystems and components. In particular, qualification of the battery and RF system is not considered adequate. There was no system-level impact test of a flight-like RF subsystem. It was qualified, mechanically and structurally, with brassboard and breadboard components in most cases. Many of these components were not electrically functional and, therefore, only limited pre-test and post-test DC continuity checks could be performed. The battery test program was reasonably thorough but also inadequate to assure qualification. During the program, an evolutionary series of failures were experienced as part of the design and development effort. However, it does appear that the incremental build–test effort led to an acceptable final design. The flight battery cell lot was delivered very late and could not be impact tested. Instead, the flight units were qualified by similarity to a preceding lot of identical cells. During qualification of the preceding lot, one of eight cells experienced physical damage but did not fail catastrophically. The small sample size and observed damage lead to a concern that the flight cell lot was not fully qualified. At a higher level, impact qualification of a complete flight-like probe was not attempted due to cost and schedule constraints, and due to the fact that it is technically challenging. Therefore, the impact qualification program is judged successful at verifying the general technology approach but not with respect to the integrated probe design. See Sections 9.2.6 and 9.3.
FLAG 3 Probes fail due to ionization breakdown in Mars atmosphere.	PLAUSIBLE. The DS2 antenna uses umbrella-like whiskers on its end to increase the effective electrical length it to 1/4 wavelength. This type of antenna has a relatively high electric field potential at the end of the sharp antenna tips. The voltage generated at these tips could potentially exceed the ionization breakdown limit for CO_2 in the 6-torr Mars environment. The probe antenna was not tested for this environment. Therefore, it is possible that the antenna could experience breakdown when operated under such conditions. If breakdown did occur, the antenna performance would be degraded such that the uplink margin could be reduced below the threshold for communication. Until a test is performed, this failure mode is considered plausible. See Section 9.3.

Failure Mode	Assessment
DS2 UHF link fails due to: —Beacon on MGS —DS2 transceiver —Incompatible protocol	PLAUSIBLE BUT UNSUPPORTED. Failure of any of the conditions listed would have precluded UHF communications between DS2 and MGS. The MGS to DS2 interface was simulated in a post-launch test with Stanford University in November 1996. Some of the 16 modes were verified during this test. The performance of the DS2 probes' Telecommunications Subsystem was tested in ATLO prior to delivery to KSC, but the probes could not be powered once installed on MPL until they were separated from the MPL cruise stage. A pre-launch test was performed between the flight spare telecommunications hardware and a CNES breadboard that verified the compatibility of the interface. See Section 9.4.1.

8.1.2 Failure Modes Affecting a Single Probe

Failure Mode	Assessment
Random part failure.	PLAUSIBLE BUT UNSUPPORTED. The probe design used commercial parts in the telecom system and in a number of other locations. Despite the lower inherent reliability of such parts, the extremely short probe operational time makes the chance of a random failure relatively small.
Undetected aeroshell handling damage.	PLAUSIBLE BUT UNSUPPORTED. The aeroshell material is extremely sensitive to fracture and even a very small scratch or other mechanical damage could have resulted in fracturing of the aeroshell during the launch environment. The acoustic acceptance test on the flight systems would have dramatically revealed any critical flaw existing in the aeroshell. This problem was well understood by the operations personnel, and, while plausible, is not considered likely given the extreme care in handling during ATLO.
FLAG 4 Probe lands on its side, interfering with antenna performance (e.g., anomalous surface).	PLAUSIBLE. The probe antenna was not designed, tested, or characterized for the condition where it is lying on its side and potentially in contact with the ground. Under such a condition, the radiation pattern would be affected. Therefore, it is possible that the link margin would drop below the threshold for communication.

9 DS2 DISCIPLINE AREA ASSESSMENTS

This section describes the detailed reviews conducted by the Board in specific technical discipline areas. Each of the technical discipline Review Teams focused on a list of postulated failure modes and attempted to ascertain whether or not the failure was plausible, based on precautions taken during the design phase and tests or verifications conducted during system validation.

Each of the following subsections describes the failure mode investigation results within each pertinent technical discipline area.

9.1 DS2 Environment and Impact Site

9.1.1 DS2 Environment and Delivery Corridor

Refer to Section 7.1, MPL Environment and Landing Site, for a description of environment and delivery issues affecting both MPL and DS2.

9.1.2 DS2 Landing Site Unsurvivable

FAILURE MODE DESCRIPTION

The DS2 probes were designed to withstand impact in a wide variety of soil conditions on Mars. However, identified failure modes included impact into an extremely soft surface thick enough to bury a probe and its antenna, or impact on rock or solid ice. Above a certain hardness, the soil behaves like a rock, and could cause a probe to fail if it bounced off the surface and came to rest in an orientation that prevented the probe antenna from communicating with MGS.

The DS2 probes must impact at no more than 30 degrees off the vertical axis to ensure penetration. It is projected that the impact angle resulting from a nominal entry would have been 20 degrees. Therefore, the probes might not be able to penetrate if the slope at point of impact is greater than 10 degrees.

FINDINGS

The DS2 project completed numerous impact tests in homogeneous dirt models, but seems to have conducted only limited testing in multilayered samples. Apart from this specific concern, the program appears to have been quite thorough.

No in-flight verification data from the probes themselves are available with respect to the failure modes. The remote-sensing data from the MGS orbiter indicate that the large-scale (100-meter footprint) slopes are all less than 10 degrees in the DS2 landing ellipse, although this does not preclude the possible existence of steeper locals slopes on the scale of the probes. Other MGS remote-sensing data also indicate that the surface of the landing site is covered with a material that has a low thermal inertia, typically indicative of a loosely packed material. The thickness of this material cannot be definitively ascertained, although the MGS data suggest that it uniformly covers most of the surface to a depth of at least 1 centimeter.

LESSONS LEARNED

The most common conditions to be encountered should be considered for test prior to any planned reflight.

Bibliography

DS2 Environment Specification and Landing Site Description — Sue Smrekar, January 13, 2000 viewgraph presentation to Environment and Landing Site Review Team at JPL, January 24, 2000.

Recommended Environments and Design ranges for the Mars Microprobe — Sue Smrekar and George Powell, Feb. 19, 1997, revised Aug. 12, 1997, Memorandum.

9.2 DS2 Mechanical Systems

This section summarizes the DS2 failure modes examinations and findings of the Mechanical Systems Review Team. The reviews were conducted with the DS2 project and technical staff at JPL on 26 January 2000. Materials handed out at this meeting, as well as other materials gathered via e-mail, are listed in the Bibliography.

9.2.1 DS2 Premature Separation

FAILURE MODE DESCRIPTION

This failure results in early deployment and loss of a probe. The following sub-failures could lead to this condition:

a) Structural failure of the probe separation joint during launch environment. This failure includes the loss of separation joint pin engagement in flexure due to late modification to pin end without subsequent testing and verification.

b) Longitudinal deflection of cruise stage separation joint and plunger relative to strut mounted separation device of 0.5 inch minimum. The probe separation initiation plunger, which rests against the MPL aeroshell ring, must move 0.5 inch to actuate probe release.

INTRODUCTION

The Mechanical Systems Review Team met with JPL DS2 mechanical systems engineers on 26 January 2000 to review this failure mode. DS2 engineers presented the material. There were no follow-up actions.

FINDINGS

The configuration of the probe structural support system is a straightforward truss assembly. The three-point attachment between the probe and support structure is insensitive to deformations occurring in the truss. The general design is acceptable.

The launch vehicle design loads were conservative and verified by coupled loads analysis. The NASTRAN finite-element model (FEM) was constructed for the aeroshell and support structure to determine member loads and deflections. The aeroshell/support structure system fundamental frequency was 60 Hz. In general, the structural system was well designed and analyzed.

The aeroshell/support structure system was qualification tested with cold temperature –65 degrees C, 43 g's quasi-static load, 15 grms random vibration, acoustic acceptance level plus 7 db, and pyrotechnic shock. This is a full complement of environmental tests and establishes high confidence in the structural integrity of the system.

Modifications to the three separation joint pins would not have compromised the integrity of the separation joint. These modifications were performed in a controlled manner, fully documented, and with full Quality Assurance participation.

Deflections of the cruise stage interface ring in the amount necessary to actuate a premature probe release would not be possible without catastrophic structural failure of the cruise stage.

Premature release of the probes would damage the MPL solar panels, and damage to solar panels would likely result in an electrical power deficiency. There was no evidence of this during cruise.

Flaws in the DS2 aeroshell that could cause premature separation would have been detected during acoustic tests performed on the flight probes. Flaws in the silicon carbide heatshield would produce a catastrophic failure of the aeroshell when subjected to the acoustic environment. After testing, there is high confidence in the integrity of the aeroshell. Specialized handling equipment and procedures were developed and implemented to ensure against handling damage to the probes.

Several other possible failure modes were presented and reviewed. They included ejection pin failure, slippage of ejection pin assembly, insufficient slack in the cable cutter lanyard, and buckling of the internal elements of the plunger mechanism. The design features and test verification program for these elements were satisfactory.

PROCESS ASSESSMENT

The design of the structural and separation system, margins, and test qualification program were excellent.

9.2.2 DS2 Fails to Separate from Cruise Stage Due to Failure of Cruise Stage Separation from Aeroshell/Lander

FAILURE MODE DESCRIPTION

For this failure to occur, the cruise stage to aeroshell separation distance would have to be less than the 0.5 inch required to initiate probe release. The failure modes for MPL cruise stage separation that are applicable to DS2 failure to separate are:

a) Separation nut fails to release bolt.
b) Separation connector/ESD cover and/or other drag forces/energy exceeds separation spring forces/energy.
c) Cold welding of aluminum-to-aluminum surfaces.
d) Mechanical hang-up between separating hardware.

INTRODUCTION

The Mechanical Systems Review Team examined the failure of cruise stage separation from the aeroshell/lander with LMA on 19 January 2000. The report on that examination can be found under Section 7.2.1, Lander/Aeroshell Fails to Separate from Cruise Stage. Cruise stage separation failure mode descriptions and findings that are applicable to DS2 failure to separate can be found in the same section. Excerpts from that examination as they relate to the DS2 failure to separate failure mode are shown below.

FINDINGS

See Section 7.2.1 for complete text.

A failure of one separation spring would not prevent the required 0.5-inch separation and therefore is not applicable. MPL ATLO system-level separation tests and analyses verified cruise stage separation.

A failure of one of the six cruise stage separation nuts to release is unlikely. Release nut qualification tests and MPL ATLO system-level separation tests verified release nut function. Given that one of the release nuts failed to release its bolt, there is enough structural compliance to allow push-off springs to open the separating rings by the amount necessary to release at least one probe.

ITT Canon connector pull forces have been test qualified. The separation joint energy margin = 1.4. MPL ATLO cruise stage separation tests verified that the connectors pulled properly.

There is no credible failure of the cruise stage to separate due to cold welding of interface materials, and there is no credible mechanical hang-up scenario that would prevent cruise stage separation.

A full system, quasi-static separation test verification, with flight hardware, was performed during MPL ATLO testing. The actuation of the DS2 separation plungers was verified in the test.

PROCESS ASSESSMENT

The design, analysis, and test verification process for the cruise stage separation joint was adequate.

9.2.3 DS2 Fails to Separate After Cruise Stage/Aeroshell Separation

FAILURE MODE DESCRIPTION

This failure mode can be caused by the following sub-failures:

a) Separation initiation plunger does not stroke (stuck plunger).

b) Guillotine does not actuate, or fails to sever restraint ligament.

c) Separation pins do not retract from probe flexures. This item includes failure modes introduced by late modification to the engagement end of pin without subsequent testing and verification.

INTRODUCTION

The Mechanical Systems Review Team met with JPL DS2 mechanical systems engineers on 26 January 2000 to review this failure mode. There were no follow-up actions.

FINDINGS

It was procedurally and physically verified that the "remove before flight" safety pins used to prevent accidental actuation of the separation initiation plunger were removed.

Modifications to the three separation joint pins would not have compromised the integrity of the separation joint or prevented probe separation. These modifications were performed in a controlled manner, fully documented, and with Quality Assurance participation.

The designs of the separation initiation plunger, guillotine, separation pins and associated retraction and push-off springs, were examined and found to be acceptable. Functional margins and qualification tests were adequate. Aeroshell/support structure environmental qualification tests verified system-level structural and separation mechanisms integrity. System-level qualification ambient and cold separation tests verified separation function.

PROCESS ASSESSMENT

The separation joint design, margins, and test verifications were very satisfactory.

9.2.4 DS2 Aeroshell Failure/Fracture at Entry Max-G

FAILURE MODE DESCRIPTION

This failure during entry could cause a probe not to survive entry/impact. This item includes failure of the adhesive bond holding the parts together and fracture of SiC at the probe attachment lugs.

INTRODUCTION

The Mechanical Systems Review Team met with JPL DS2 mechanical systems engineers on 26 January 2000 to review this failure mode. There were no follow-up actions.

FINDINGS

The DS2 aeroshell components are the SiC heatshield structure and thermal protection system (TPS), SiC backshell structure and TPS, and interface and penetrator bushings. The thin-wall SiC shells have high stiffness, high temperature capability, and extreme resistance to thermal stress and shock. They are brittle and fracture completely upon impact. Three titanium (kinematic) mounts transmit the load from penetrator to aeroshell.

A JPL FEM analysis of the SiC structure, using a conservative 39 g's launch acceleration, produced 5600 psi maximum stress. The same analysis, using the entry decelerations of 12 g's, produced 1700 psi maximum stress. The launch environment is the loads and stress defining case. The aeroshell has been designed for 60 g's. The strength margins of the aeroshell are large.

The aeroshells were analyzed by NASA Lewis Research Center using Ceramics Analysis and Reliability Evaluation of Structures (CARES). Coupon tests provided data for analysis. X&Y&Z load cases at 60 g's indicated that the probability of aeroshell failure is less than 0.5 percent.

Launch venting analysis was performed at JPL.

The aeroshell was structurally qualified by two-axis quasi-static, acoustics, pyro shock, and thermal cycle tests. The qualification aeroshell went through system-level acoustics test at LMA, and system-level thermal–vacuum and separation testing at JPL. Acceptance test of flight aeroshells was system-level acoustics.

Coefficient of thermal expansion (CTE) mismatch analysis was done for all bond joints between SiC and Ti, SiC and Epoxy 9394. Data for thermal analysis were provided by NASA LaRC. The bond line between heatshield and backshell is 2.5 millimeters wide around the entire perimeter of the shell. Maximum bond line stress at heatshield/backshell interface is 1 ksi at launch and negligible at entry. Bond lines get hot *after* peak deceleration pulse. Bond line margins at max g and at high temperature are very high.

Flaws in the aeroshell that could cause failure of the aeroshell during entry would have been detected during flight acoustics test. Critical flaws in the SiC heatshield and backshell would have produced catastrophic failure of the aeroshell during the test. Specialized handling equipment and procedures were developed and implemented to insure against subsequent handling damage to the probes.

PROCESS ASSESSMENT

The design of the aeroshell and its structural margins, including bond lines, was acceptable. The analyses and test program used to verify the design was also acceptable.

9.2.5 DS2 Structural Failure at Impact

FAILURE MODE DESCRIPTION

These failure modes result in the probes' inability to communicate:

a) Aeroshell causes damage to probe structure at impact.
b) Antenna mast bending propagates to structure/electronics failure at impact.

INTRODUCTION

The Mechanical Systems Review Team met with JPL DS2 mechanical systems engineers on 26 January 2000 to review this failure mode. There were no follow-up actions.

FINDINGS

It is commonly understood that impact analyses at very high g levels are not reliable. Therefore, the design process is empirical and impact testing is the only reliable verification method.

The kinetic energy of the backshell, dissipated on the probe aft-body cover and antenna at impact, was assumed to be the worst-case scenario for this failure mode. Development impact tests of the aft-body cover against a flat plate aeroshell simulator produced significant structural damage to an early prototype design. Material and design changes to the cover were implemented and shown to survive the impact tests. These tests only approximated the actual dynamic interaction between the aeroshell and the aft-body. Due to a test apparatus limitation, no impact tests of a flight-configuration aeroshell with probe attached were performed. The probe aft-body design was qualified by a series of impact tests. It was not established how conservatively the tests represented the flight impact dynamics.

No detailed analysis was done of the aft-body to antenna interaction. Both FEM analysis and hand calculations were used for the antenna structure, but neither provided confident results because the loads were not well understood. Several antenna masts were slightly bent during impact testing, but no analytic models could be made to match the empirical damage. Damage to the antenna was limited to bending of the mast above the base. There has been no evidence of antenna base/aft-body deformations. The base fixity stiffness of the aft-body is high. The antenna structure design was proven empirically by several impact tests.

Analysis shows that impact between the aeroshell and the antenna tip occurs at greatly reduced relative speed due to the short distance between them. A special impact drop test was performed on the antenna to qualify aeroshell/antenna interaction. The test demonstrated that the aeroshell would not damage the antenna or whiskers.

PROCESS ASSESSMENT

The probe structure and antenna have been empirically designed to withstand the impact tests to which they were subjected. The structure and antenna integrity has been verified by these same tests. Within the limits of the impact tests, the probe structure and antenna demonstrated their survivability. However, the verification process is less than complete, due to the absence of a combined aeroshell–probe impact test. The flight configuration was not impact tested.

LESSONS LEARNED

For future missions, perform impact tests with the probe integrated with the aeroshell to demonstrate acceptable dynamic interaction between them.

9.2.6 DS2 Telecom Subsystem Fails at Impact

FAILURE MODE DESCRIPTION

In this potential failure mode, the RF subsystem does not survive impact with the surface within the limits of the design.

INTRODUCTION

The Mechanical Systems Review Team met with the JPL DS2 engineering staff to examine this failure mode on 26 January 2000. There were no follow-up actions.

FINDINGS

1. The probe design did not allow for post-environmental system functional testing without destructive disassembly of the aeroshell and probe; therefore, there was no verification of flight readiness after acoustic test.
2. All system-level impact testing was conducted at the probe level without the aeroshell. There were no impact tests of the combined aeroshell and probe. Tests were conducted with soil requirement conditions #3 through #5, representing the harder surface class of properties.
3. The interaction of the aeroshell and probe aft-body at impact was tested by firing the aft-body into a flat plate of aeroshell material. This test was only an approximation of the actual dynamic interaction. These development tests resulted in an empirical approach to the aft-body design.
4. RF system development impact tests were limited to brassboard and breadboard components and subassemblies. Post-test visual inspections of component mounting integrity and electrical connections were conducted. These development tests provided the component mounting and configuration requirements that were implemented in the flight RF design. Since many of the RF components were not electrically functional, only limited DC pre-test and post-test checks were possible. These development tests did not represent complete qualification of the RF subsystem; they qualified the subsystem structurally, but not functionally.
5. No system-level impact tests were conducted with a flight-equivalent RF subsystem. Design changes emerging late in the program resulted in its unavailability for system testing. The DS2 project's position is that the RF Subsystem was qualified by similarity to other electrical components that satisfactorily survived system impact tests, and were verified as functionally acceptable. Subsystems that were tested at the system level include tunable diode laser (TDL) assembly, power switch, aft sensor board, and pressure sensor electronics. Other electrical parts were tested for performance before and after impact, with special attention paid to components known to be affected by high g loads. Nonetheless, the absence of a flight-equivalent RF Subsystem impact test precluded verification of its functional design and survivability.
6. The DS2 project thought there was no alternative to accepting the absence of a flight-like RF Subsystem impact test, short of missing the MPL launch opportunity. The rationale for proceeding to launch was presented and accepted at two peer reviews and presented at three project-level reviews: Risk Assessment, Mission Readiness, and Delta Mission Readiness. The project had "proceed to launch" concurrence from JPL and NASA upper management (Reference: DS2 Comments to Casani Report Version 3b, Sarah Gavit, 2/15/00; also Deep Space 2 Mission: Status — letter from Ed Stone, JPL Director, to Edward Weiler, January 4, 1999 (describes state of readiness for launch on January 3, 1999).
7. The flight spare RF Subsystem, which was planned to be available for post-Mars impact diagnostics, could now be used for impact testing.

PROCESS ASSESSMENT

The absence of functional test access to the probes after integration with their aeroshells precluded verification of the flight RF Subsystem readiness following completion of system acoustic environmental tests. Since there was no system-level qualification impact test of a flight-like RF subsystem, verification of the RF Subsystem is incomplete.

LESSONS LEARNED

1. Conduct an RF flight spare system impact test to demonstrate survivability. Describe criteria for a successful test.
2. Include the aeroshell with the probe for future qualification impact tests. The impact tests performed on this program only approximate the interaction between these two elements (refer to Section 9.2.5, DS2 Structural Failure at Impact).
3. For future probes, include electrical test access features that will allow verification of flight readiness at the fully integrated system level.

SUMMARY

The mechanical systems designs and design process was excellent. With the exception of the incompleteness of system-level impact testing, the test verification process for the mechanical systems was fully satisfactory and well executed. The design review process was effectively implemented. The technical leadership and ownership of this activity was evident.

Bibliography

Deep Space 2 Mission: Status — letter from Ed Stone, JPL Director, to Edward Weiler, January 4, 1999 (describes state of readiness for launch on January 3, 1999).

DS2 Comments to Casani Report Version 3b, by Sarah Gavit, 2/15/00.

DS2 Failure Review handout package, Umbilical/Electronics Packaging Design and Verification, by Saverio D'Agostino, 13 January 2000, 20 pages.

DS2 Mechanical Systems Failure Modes handout package, by Tom Rivellini, January 26, 2000, 189 pages.

New Millennium DS2 Failure Review handout package, by Tom Rivellini, January 13, 2000, 86 pages.

9.3 DS2 Avionics

INTRODUCTION

Meetings were held with the DS2 team on 26 January 2000 to review the DS2 system avionics and potential failure modes. The Avionics Review Team addressed the key avionics system elements from a design and test perspective, although there was insufficient time to cover all items in great depth.

SYSTEM DESIGN

The DS2 system is divided between aft-body and penetrator elements with a flexible polyimide tether electrically linking them together. All power and signal communication between the two bodies is performed via this tether. The penetrator is a round-nose penetrator containing the science instrumentation together with a small three-sided prism structure holding the science-related power and control electronics. The aft-body contains the batteries, power switch, and telecom hardware, together with a sensor ASIC.

With respect to the inability of the DS2 probes to communicate, the aft-body contains all of the hardware associated with the critical power and communication functions. With the exception of a power bus short in the umbilical, there is no evident single failure or common mode in the penetrator that would preclude proper operation of the telecom system. Therefore, efforts have focused on the power and telecom functional elements, together with the tether. The aeroshell configuration with respect to EMI and ESD sensitivity was also examined.

PROCESS ASSESSMENT

a) Batteries. The cell development effort was well done in most respects, especially given the difficulty in packaging and testing the devices to meet the extreme impact requirements. The team worked closely with the battery vendor, Yardney, and appears to have done all the right things from a design and quality perspective to get a good product. As would be expected, there were many test failures of diverse nature during the development process. That process went through two major design modifications and seven impact validation tests leading to the final flight design. For the most part, it appears that the final design is adequate to meet the environmental and energy requirements associated with the DS2 mission. However, no impact testing was performed on the flight cell lots. Therefore, the flight batteries are currently qualified only by similarity to a lot that experienced one performance degradation (non-catastrophic internal damage) out of eight devices.

Assembly of the cells into an aft-body battery pack appears to be a robust process that should survive impact. Each cell is epoxied into a cylindrical Torlon sleeve and has the wire terminations fully encapsulated with low-temperature Solithane polyurethane. The completed cell is then epoxied into a bored-out hole in the magnesium aft-body (four cells per battery; two complete batteries) and the motherboard is mounted on top of it. This is a very nice scheme, since the wire leads are kept short and can be fully staked at the point where they emerge through the motherboard. From a power perspective, the flight lot of cells was well characterized through a series of realistic storage and operational scenarios. The available energy is strongly dependent on cell temperature but testing has shown that a flight battery pair could be expected to have at least 2.4 amp-hours of energy (under very worst-case conditions) when operated through the planned mission profile. Assuming the batteries survived, the energy available meets the mission requirement with substantial margin.

b) Power Switch. The power switch design was originally developed by Boeing and uses a p-channel and n-channel MOSFET in combination with a bias network to produce a regenerative latch effect.

The design by its nature is optimized to assure turn-on and does not effectively guard against inadvertent activation. It is also dependent on having a load connected that will draw enough current to assure that the p-channel switch leakage will not reach the turn-on threshold for the n-channel latch (the circuit could actually self-activate if there is no external load). The design also does not account for the worst-case specification leakage for the p-channel switch, which can be as high as 250 microamps. Testing of prototype hardware and other sample devices shows that the device leakage is extremely low and not an issue.

A second design weakness for the power switch is that wires for the switch arm function are isolated with 100-kohm resistors. By virtue of this relatively high impedance, the wires can appear to be floating from an EMI perspective and could act as a pickup antenna for EMI. However, the RC time constant of the filter circuit on the gate of the power switch is 10 milliseconds. Therefore, the circuit should be immune to all but the strongest RF signals.

c) Aft-body to Penetrator Tether. The tether design is well thought out and looks as though it will function as intended. The test program also appears adequate, with the exception that most of the failed test specimens were only qualitatively analyzed. When failures occurred, the samples were looked at visually and measured with a standard ohmmeter. The failed specimen was not evaluated with more powerful material analysis tools, nor were tests performed at higher, more representative test voltages (standard ohmmeters only apply 0.2 volt to the circuit). However, the tether appears tough enough and the test program was thorough enough that a tether failure is considered extremely unlikely for both probes.

d) Telecom System. The original telecom system was abandoned late in the probe development flow due to technical problems. As an obvious risk area, the replacement telecom system design was reviewed in fair detail as part of this assessment to determine both its suitability for the planned mission and state of readiness at the time of delivery. In particular, the antenna design, uplink and downlink margins, and the development/test program were evaluated. Some effort has also been spent on the detailed electrical design.

Based on discussions with the engineers, it was clear that the telecom effort was in skilled hands and was (eventually) well supported by Laboratory resources. The design, which is based on cellular telephone technology, appears to be sound. The majority of the active parts were plastic commercial types with no radiation pedigree, although it was pointed out that the project accepted plastic parts for all the DS2 subsystems. There was also no consideration given to the radiation hardness of the specific parts. Again, this approach was based on a radiation effects review (IOM 507-B-DBI-97, D, Bergens, Results of DS2 Microprobe Radiation Effects Review) showing that rad-hard parts were not necessary. A subsequent review initiated by the Board (SSM-514-C-001-00, S. McClure, 24 February 2000) concurs with the original assessment.

The flight telecom units were tested as an integrated system with some environmental testing exceptions. Specifically, the telecom system was not tested at Mars pressure, nor was it impact tested as a complete system. Flight unit subassemblies (e.g., the daughter boards, digital boards) were all tested and characterized individually over the thermal qualification range prior to integration as a system into the flight probes. While the flight units were not environmentally tested as an integrated system, the telecom flight spare unit was fully tested and characterized over the thermal qualification range (also not at Mars pressure).

e) Aeroshell. The design was reviewed and an assembled aeroshell used for EMI testing was inspected, as was a cracked reject that was not assembled. The Review Team also checked the resistance of the SiC material and the glue joints. Altogether, the design appears quite good from a mechanical perspective, although there was no attention paid to EMC, ESD, and grounding with respect to making the complete shell an effective electrostatic shield. Only one out of the three sample glue joints associated with the probe mounting pads was conductive. Therefore, it is possible that the probe was electrically floating when attached to the inside of the aeroshell body.

Based on the sample hardware, it appears that the circumferential joint between the two hemispheres is uneven enough to assure a partially conductive connection between the mating halves. However, depending on the quality of the epoxy joint, it is likely that the shielding effectiveness would be compromised. This is borne out by preliminary measurements performed in the EMC lab showing a measured attenuation of approximately 12 dB. This is not an unreasonable result for a poorly bonded shield. A well-bonded shield would be expected to provide 40 to 60 dB of attenuation.

f) Test Program. The test program was limited by time and budget plus the fact that a flight-ready probe, as designed, could not be fully tested once integrated. Therefore, the elements of each probe were tested fairly completely on an individual basis, but the complete probes did not get an end-to-end series of environmental tests under fully simulated flight conditions. Beyond the lack of a complete system test, there are four principal concerns: 1) The flight battery lot was impact qualified by similarity to another lot that was not flown (other qualifications tests were performed); 2) Impact testing of electronic modules was done in a power-off condition rather than under a powered condition; 3) The probe RF system was not tested for proper operation as a complete system in the 6-torr Mars environment.

g) Documentation and Data Review. The project records are in relatively good shape and the project team should be commended for their efforts to maintain configuration control despite extreme schedule and cost pressure.

FINDINGS

1. The battery cell design is considered fundamentally rugged enough to survive impact. However, the test program was incomplete since there was no impact testing of the flight cell lot. As well, the sample size of the impact test lot was too small to statistically assure qualification of the design. Therefore, a catastrophic battery failure at probe impact is considered plausible but unsupported.
2. The power switch design is marginal and the switch can inadvertently turn on due to a handling error, an ESD event, or EMI. Great care was taken during the ground processing of the probes to mitigate this deficiency and there is no direct evidence suggesting that the probes experienced a premature turn-on. Due to the extreme sensitivity of the circuit, however, early inadvertent turn-on is considered a plausible but unsupported failure mode.
3. The worst-case leakage current specification for the power switch MOSFETs is high enough that, in principle, it is possible for the batteries to be discharged during the long storage and cruise interval. Testing of a prototype circuit and some representative parts demonstrated leakages low enough to make this scenario unlikely.
4. The probe mounting and associated aeroshell assembly methods were not designed or controlled to achieve good probe grounding and effective EMI shielding. Though probably not catastrophic, the resulting shield performance is not predictable and cannot be counted on to remain consistent through the series of probe test and operational environments. One possible result would be ESD or EMI sensitivity sufficient to inadvertently activate the power switch as discussed above. This is considered unlikely, however.
5. The power lines in the aft-body–to–penetrator tether were not fused or current limited. The design of the tether also did not specifically preclude the possibility of an electrical power short. Test

program results indicate that a short is unlikely, but testing was insufficient to guarantee that a short could not occur and/or would not be catastrophic in the event of occurrence. It is unlikely that a failure of both probes can be explained by this finding.

6. The flight telecom subsystem was not qualified as part of the flight probe system test. However, sufficient testing at lower levels in combination with testing of the spare hardware makes a problem unlikely.
7. While an analysis was performed, the associated high E-Field at the antenna tips could result in breakdown of the CO_2 at the 6-torr Mars atmospheric pressure. This is considered a plausible failure mode until a test is performed to preclude its possibility.
8. The antenna test activity did not quantify pattern and gain performance for the off-nominal condition where the probe is lying on its side (the probes did not have a requirement to function under this condition). Therefore, inadequate link margin is plausible for this case. The link calculations themselves appear correct, so a probe that did not skip or bounce would not be affected by this finding.
9. The parts selected for the telecom system (and the rest of the probe system) are mostly commercial types since there was no requirement to do otherwise. A part failure is plausible, but the short lifetime of the probe makes a malfunction of both probes highly unlikely.
10. The overall probe test program did not perform any impact testing of a fully integrated and powered system. Therefore, the probes were flown (with JPL management's knowledge) without being fully qualified for the expected environments. A failure due to inadequate qualification is considered plausible.

9.4 DS2 Communications

9.4.1 UHF Link Fails

FAILURE MODE DESCRIPTION

In this potential failure mode, the DS2 probes are unable to communicate with MGS. This could be caused by a failure of the MGS or DS2 telecommunications hardware or an incompatible interface between MGS and DS2.

Thermal tests of the telecommunications system were limited to the following:

- Engineering units — All subassemblies were tested over the temperature range.
- Flight spare — Tested as a system over the temperature range (post-launch).
- Flight units — Only the digital board and aftsensor assemblies were tested over the temperature range.

During thermal tests of the telecommunications system after launch, a software error was detected for which the oscillator frequency was not compensated as a function of temperature. Further tests revealed that this error had a minimal impact on link performance (<1 db).

There were no tests of the telecommunications system at Mars pressures.

There were no airlink tests of the flight units to verify link performance. Tests were performed on the flight units using uncalibrated antennas to verify the presence of a signal only. Link-performance tests were performed on engineering units only.

A pre-launch compatibility test of the CNES MGS MR flight spare and the DS2 telecommunications flight spare was performed as an end-to-end telecommunications qualification test. (*Note*: At project start, it was acknowledged that a system end-to-end test with MGS was not possible because MGS was to be launched before the DS2 telecom system was fabricated).

An in-flight test was conducted between Stanford University and MGS to verify the Mars Relay (MR) operational modes in November 1996. During this test, it was determined that there was a wiring error that resulted in the wrong operational modes being selected. This required a software change to make the operational mode commands consistent with the hardware configuration. A follow up in-flight test with MGS was not performed to verify the MR responses to the new commands. The MR receiver was verified as part of the November 1996 Stanford University test but it was not verified after that time.

The MGS MR downlink modes for MGS-to-DS2 communications were verified after the Mars anomaly in December 1999 using the Stanford University 46-meter antenna (several unsuccessful attempts had been made earlier in cruise).

There was no capability to power the DS2 probes from the time they were attached to the MPL cruise stage at KSC, until after separation from the MPL cruise stage.

PROCESS ASSESSMENT

An end-to-end link compatibility test was never performed with the MGS spacecraft and the DS2 probes. This was an accepted risk at DS2 project start, as it was known that the MGS spacecraft would be launched before the DS2 telecom system would be built. While in-flight MGS tests verified the MR for commanding the DS2 probes, these tests were unable to verify MR receive functions for DS2. End-to-end tests performed between the MR flight spare at CNES and the DS2 flight spare were performed with a hardline connection, thus link margins were not verified.

LESSONS LEARNED
Perform pre-launch link compatibility tests.

Bibliography

DS2 Electronic Subsystem Review — Handout, DS2 Briefing 01/13/00.

DS2 Impact Shock and Random Vibration Qualification, IOM 5053-99-001, dated January 15, 1999.

DS2 Impact Testing of Telecom hardware — via Saverio D'Agostino e-mail 01/14/00.

DS2 Integration and Test System Test Program Overview — Handout, DS2 Briefing 01/13/00.

DS2 Software (Flight, Test and Operations) — Handout, DS2 Briefing 01/13/00.

DS2 Telecom POR Circuit — via Eric Archer e-mail 01/28/00.

DS2 Telecom Questions on AMC Failure Modes — via Robert Nowicki e-mail 01/27/00.

DS2 Telecom Questions on Response to MGS — via Christopher Morse e-mail 01/27/00.

Environmental Specifications and Landing Site Description — Handout, DS2 Briefing 01/13/00.

Mars Microprobe Project (DS2) Mission Assurance Plan and Specification, D-14323, dated March 1997.

Mission Assurance — Handout, DS2 Briefing 01/13/00.

Possible Failure Modes — Handout, DS2 Briefing 01/13/00.

Operational Process & Validation — Handout, DS2 Briefing 01/13/00.

Structural Test Program Overview — Handout, DS2 Briefing 01/13/00.

System and Mission Design Overview — Handout, DS2 Briefing 01/13/00.

Telecommunications Subsystem — Handout, DS2 Briefing 01/13/00.

Umbilical/Electronics Packaging Design and Verification — Handout, DS2 Briefing 01/13/00.

Appendix 1

Bibliography

AACS Algorithm: Entry Navigation Kalman Filter, Report Rev. 2, dated 3/11/98, presented on 01/26/00 at LMA.

AACS Algorithm: GyroCompass — Handout, LMA Meeting 01/31/00.

AACS Algorithm: Radar Commanding, Report Rev. 4, dated 5/25/99, presented on 01/26/00 at LMA.

AAIA-98-3665, Test and Modeling of the Mars '98 Descent Propulsion System Waterhammer — T. Martin, L. Rockwell, C. Parish, LMA, 7/13-15/98, Joint Propulsion Conference & Exhibit at Cleveland, Ohio.

AAS Algorithm: Radar Processing, Report Rev. 4, dated 06/23/99, presented on 01/26/00 at LMA.

Additional Information of MPL Prop Peer Review Process — via Lad Curtis, 2/24/00, e-mail from Greg McAllister on 2/22/00 regarding Propellant Isolation AI from Prop CDE, electronic format.

Additional Information on MPL Tank Outlet Temperature — via Lad Curtis, 2/21/00, e-mail from Kevin Miller on 2/18/00 regarding MSP '98, Memorandum to Greg McAllister, Tim Martin on 9/16/99, MSP '98 MPL Fuel Tank Status.

Additional Information on MPL CM Offset Calculations From Flight TCM Data — Lad Curtis, 3/7/00, e-mail responding to Questions on MPL CM Offset Calculations from Flight TCM Data, H. Curtis, J. Wynn.

Additional Information on Propulsion: Zero-G Fuel Transfer Considerations — Lad Curtis, 2/17/00, e-mail of report from Tim Martin regarding Consideration of MPL Zero-G Fuel Transfer During Design and Development.

Ambiguity on MPL System FMECA Status — via Lad Curtis, 03/14/00, e-mail from Robert Menke.

Analysis of MGS/MOC Observations of the Mars Polar Lander (MPL) Landing Zone, Michael Malin, February 24, 2000, HTML Publication.

Analysis of MGS/MOC Observations of the Mars Polar Lander (MPL) Landing Zone — Supplementary Data, Michael Malin, March 7, 2000, HTML Publication.

ATLO Leg Deployment — via Lad Curtis e-mail of 02/15/00; memo from Thomas McCaa to Shane Roskie of 02/14/00 re Touchdown Sensor Miswire on MPL in June 1998.

B3. ACS Lander Hardware Description — Kent Hoilman, 01/25/00, viewgraph presentation at LMA.

Battery power capability — via Kyle Martin e-mail 02/07/00.

Brace Concerns — Handout, LMA Meeting 01/31/00.

C&DH CDR Peer Review, D-14523, dated 12 November 1996.

C&DH Failure (Reply to Postulated C&DH Failure) — via Lad Curtis e-mail of 02/15/00; information re potential failure modes in Avionics section of Board report; topics: processor resets during EDL, CMIC errors after landing (add EDAC to CMIC), EEPROM errors after landing; info from Jerry Henderson.

CFD Analysis of Mars '01 Lander Near-Ground Environments — Joe Bomba, Pete Huseman, 2/24/00.

CG Offset Effect on Landed Location — Bill Willcockson and Jason Wynn, 01/25/00, viewgraph presentation at LMA.

CG Offset Effect on Landed Location — Willcockson and Wynn, January 26, 2000, viewgraph presentation to Environment and Landing Site Review Team at LMA, February 1, 2000.

CMIC_map — Handout, LMA Meeting 01/31/00.

Collection of Action Item Responses from the Dynamics and Control Review Team meeting on 01/25–26/00 at LMA.

Comm/C&DH/FSW/Seq MPL FRB Action Item List — Kyle Martin to Richard Brace e-mail of 02/04/00; cover message includes Scott Toro-Allen e-mail to Kyle Martin of 02/04/00, response to Comm FRB Action Item #5.

Comments on Entry and Descent Separation Analyses and Test Report — forwarded from Frank Locatell via e-mail of 01/17/00; memo from Jeff Bene dated 01/11/00 re document VR022 of 12/10/98.

Corona Analyses for MPL UHF Antenna — via Lad Curtis e-mail of 02/18/00; Scott Toro-Allen e-mail to Lad Curtis of 02/18/00 incorporating message from Mike Pearce to Bill Wallace of 03/26/97.

Cruise Stage Separation Analysis — via Lad Curtis e-mail of 02/15/00; info from Jeff Bene.

Deep Space 2 Mission: Status — letter from Ed Stone, JPL Director, to Edward Weiler, January 4, 1999 (describes state of readiness for launch on January 3, 1999).

Detection of a Candidate Signal from the Mars Polar Lander — via Richard L. Horttor, 02/17/00, original memo from George Resch to Richard Cook, Mars UHF Signal and Analysis.

Diplexer and bandpass filter plating — via Kyle Martin e-mail 02/04/00.

DS2 Comments to Casani Report Version 3b, by Sarah Gavit, 2/15/00.

DS2 Electronic Subsystem Review — Handout, DS2 Briefing 01/13/00.

DS2 Environment Specification and Landing Site Description — Sue Smrekar, January 13, 2000 viewgraph presentation to Environment and Landing Site Review Team at JPL, January 24, 2000.

DS2 Failure Review handout package, Umbilical/Electronics Packaging Design and Verification, by Saverio D'Agostino, 13 January 2000, 20 pages.

DS2 Impact Shock and Random Vibration Qualification, IOM 5053-99-001, dated January 15, 1999.

DS2 Impact Testing of Telecom hardware — via Saverio D'Agostino e-mail 01/14/00.

DS2 Integration and Test System Test Program Overview — Handout, DS2 Briefing 01/13/00.

DS2 Mechanical Systems Failure Modes handout package, by Tom Rivellini, January 26, 2000, 189 pages.

DS2 Software (Flight, Test and Operations) — Handout, DS2 Briefing 01/13/00.

DS2 Telecom POR Circuit — via Eric Archer e-mail 01/28/00.

DS2 Telecom Questions on AMC Failure Modes — via Robert Nowicki e-mail 01/27/00.

DS2 Telecom Questions on Response to MGS — via Christopher Morse e-mail 01/27/00.

DST Environmental Comparison MSP98 vs. Cassini — Handout, LMA Meeting 02/01/00.

DST Fault Protection — Lad Curtis e-mail 02/08/00.

DST Fault Protection — Lad Curtis e-mail of 02/14/00; and Rev. 1, Lad Curtis e-mail of 2/14/00.

EDL Backup Timers (Justification for No EDL Backup Timers) — via Lad Curtis e-mail of 02/16/00; re fault-tolerance section of Board report; info from Bill Willcockson.

EDL Critical Events Review — Steve Jolly, 01/05/00 viewgraph presentation to Board at LMA.

EDL Electrical States — Handout, LMA Meeting 02/01/00.

EDL Fault Tree — Lad Curtis, 01/05/00 viewgraph presentation to Board at LMA.

EDL Propellant Tank Modeling and Analysis, LMA IOM FSMO-00-007, J. Wynn to Jim Chapel, Bill Willcockson, Tim Martin, 3/8/00.

Effect of Recent CG Shift Estimates on Touchdown Location — via Lad Curtis e-mail of 01/26/00, memo from Bill Willcockson to Milt Hetrick of 01/26/00; cover e-mail message from Curtis discusses center-of-mass displacement at entry as result of center-of-mass shift during cruise due to fuel migration along axis of prop tanks.

Entry and Descent Separation Analyses and Tests, LMA document VR022, Lowell Cogburn, 10 December 1998.

Entry Systems — Bill Willcockson, 01/25/00, viewgraph presentation at LMA.

Entry, Descent and Landing (EDL) Overview — John Cuseo, 01/25/00, viewgraph presentation at LMA.

Environmental Specifications and Landing Site Description — Handout, DS2 Briefing 01/13/00.

Fault Protection enable/disable states — via Kyle Martin e-mail 02/07/00 with the following attachments: EDL FP State Changes; MSP_11.pdf Section 11 Component-Level Fault Protection; MSP_12.pdf Section 12 Performance-Level Fault Protection; MSP_13.pdf Section 13 System-Level Fault Protection

Fault-tree Analyses — Lad Curtis e-mail of 02/08/00 to Pete Burr re FTA, Failure Mode Effects and Criticality Analyses (FMECAs), Redundancy Verification Analyses (RVAs), and Worst-Case Analyses (WCAs) for MSP '98.

FBC#2 — via Philip Garrison e-mail, 1/13/00, from John McNamee e-mail on 12/23/99.

Feed System Transient Pressure Effects on Operational Thruster Performance For a Pulse Modulated Controlled Multiple Thruster Planetary Lander, Report #D99-41717 — 12/23/99, Timothy Martin, William J. Bailey, Kelly R. Scheimbert, LMA.

Flight Software Changes and Problem Reports — via Lad Curtis, e-mail of 01/28/00, file name = FSW Changes Accounting Prelim 011700 from Greg Bollendonk.

FSW Action Item Closure — Kyle Martin e-mail of 02/07/00 to Richard Brace re fault protection enable/disable states. Attachments: Lander EDL Fault Protection State Changes; Section 11–Component-Level Fault Protection; Section 12–Performance-Level Fault Protection; Section 13–System-Level Fault Protection.

FSW Overview — Handout, LMA Meeting 01/01/00.

Fuel Tank Outlet — via Lad Curtis e-mail of 02/28/00; Kevin Miller e-mail to Frank Locatell of 02/28/00; presentation to Jeff Leising et al. of 02/24/00, MPL Fuel Tank Outlet Discussion by K. Miller and G. McAllister.

Fuel Tank Outlet — via Marilyn Morgan, 2/29/00, e-mail from Lad Curtis on 2/28/00, and Kevin Miller on 2/28/00, attachment: MPL Fuel Tank Outlet Discussion, 2/24/00.

Heatshield Review — Ron Turner, February 1, 2000, viewgraph presentation to Environment and Landing Site Review Team at LMA, February 1, 2000.

Heatshield Structure Pinhole Arc Jet Testing — Jan Thornton, February 1st, 2000, viewgraph presentation to Environment and Landing Site Review Team at LMA, February 1, 2000.

Hot Descent Engine Valve Issue — via Lad Curtis, e-mail of 02/09/00, viewgraph presentation documenting testing performed at LMA.

How Long Will the Lander Live? — via Lad Curtis e-mail of 02/08/00; Adrian Adamson response to Comm Review Team query pertaining to possible UHF signal from MPL.

IMU Descent Vibration Environment — Kent Hoilman and Jim Chapel, 01/25/00, graph presented at LMA.

In-Flight Verification of Telecom, C&DH and Flight Software — Handout 6, LMA Meeting 01/31/00.

Integrated Propulsion and GN&C System Modeling and Results; Flowtran Propulsion Modeling — Tim Martin, 01/26/00, model presented at LMA.

JPL FRB Question: Entry Center-of-Mass Requirement — Lad Curtis, 1/13/00, e-mail reporting on center-of-mass requirement for entry on 1/12/00.

Justification for Non-Standard Disk-Gap-Band (DGB) Parachute on Mars Pathfinder Project, document ME-2589-Rpt Rev. A.

Lander Configuration After EDL — Handout, LMA Meeting 01/31/00.

Lander EDL Fault Protection State Changes — Gregory Bollendonk, via Lad Curtis e-mail, 02/04/00; e-mail response to action item from Comm Review Team.

Lander Entry State File (LESF) — Tom Kelecy, 01/25/00, viewgraph presentation at LMA.

Lander Propulsion Loading Data — via Lad Curtis, e-mail of 01/14/00: Tank Center of Gravity Calculations: MPL Lander Flight Propellant Load (memo VR-192 from J. Greg McAllister to Lad Curtis of 01/16/00); MSP Lander Verification Report VR006, paragraphs 3.3.7.7 and 3.3.7.11 (no date).

Lander/Backshell Recontact Analysis, MPL/DS2 Mishap Investigation — Spencer (JPL), Desai, and Queen (LaRC), February 1, 2000, viewgraph presentation to Environment and Landing Site Review Team at LMA, February 1, 2000

Latest Revision of MPL FRB Section 7.5 on Propulsion and Thermal — Carl S. Guernsey, 2/28/00, e-mail

Leg Test Status — forwarded from Frank Locatell on 02/08/00; e-mail from Jeff Bene of 02/08/00. Also note re Framotome lanyard testing.

Legs Sensor — Lad Curtis e-mail of 02/24/00 to John Casani et al., message discusses TD sensor transient and how observation was documented.

Lessons Learned Report from Mars Polar Lander Descent Engine Cold Catalyst Bed/Cold Inlet Manifold Issues — Milt Hetrick, Kevin Miller, LMA, 11/24/99, memo to Bill Meersman, Larry Talafuse, Lad Curtis, Al Herzl.

L-GN&C Subsystem Test/Verification — Tom Kelecy, 01/25/00, viewgraph presentation at LMA.

LMA Comments on Board Report, draft #3b — via Lad Curtis e-mail of 02/15/00.

LMA Comments on Board Report, draft #3b, propulsion section only — via Lad Curtis e-mail of 02/15/00.

LMA Comments on Board Report, draft #6 — via Lad Curtis e-mail of 02/23/00.

LMA Comments on Board Report, draft #7a — via Lad Curtis e-mail of 03/03/00.

LMA memorandum: from Thomas C. McCay to Shane Koskie, regarding Touchdown Sensor Miswire on the MPL in June 1998, February 14, 2000.

LMA MPL Investigations Since Landing Day — Lad Curtis, 01/05/00 viewgraph presentation to Board at LMA.

LMA report: LMSS-DO Investigation of Process Contributors to Mars Polar Lander Premature Thrust Termination Due to Touchdown Indication, March 5, 2000.

LMA viewgraph presentation: Functional Flow Chart, HHC-1.

LMA viewgraph presentation: Mars Polar Lander Premature Descent Engine Termination Due to Touchdown (TD) Indication Conclusions, February 25, 2000, H.H. Curtis, R. Gehling, J.Bene, and G. Bollendonk.

LMA viewgraph presentation: Mars Polar Lander Touchdown Sensor Code Issue, January 28, 2000, H. H. Curtis — Lander Systems Engineering, with an Appendix: Touchdown Monitor FSW Description, G. Bollendonk, MPL Flight Software.

LMA viewgraph presentation: Mars Polar Lander Touchdown Sensor Code Issue, February 11, 2000, H.H. Curtis – Lander Systems Engineering.

LMA viewgraph presentation: System Requirement Mapping to FSW, HHC31.

LMA viewgraph presentation: Timeline, HHC-3.

Mars '01 Heritage Changes, Lesson Learned, and Enhancements from MSP '98 — via Lad Curtis, e-mail of 01/12/00, viewgraph presentation at JPL on 12/15/99.

Mars Climate Orbiter and Mars Polar Lander: Spacecraft Development and Operations Summary — Ed Euler, 01/05/00 viewgraph presentation to Board at LMA.

Mars Global Surveyor Mars Relay Flight Test Final Report, D-14423, John L. Callas, dated 1997 March 14.

Mars Microprobe Project (DS2) Mission Assurance Plan and Specification, D-14323, dated March 1997.

Mars Polar Lander Angle of Attack with Maximum Propellant Shift — Bill Willcockson, 01/10/00 memo to Ed Euler (via Lad Curtis e-mail of 01/13/00).

Mars Polar Lander Descent Thruster MR-107N Thermal Analysis Verification Test Report (MSOP-00-0003) — Kevin Miller e-mail message of 02/16/00 (hard copies sent); report by Jon R. White, February 2000. (File name = final-desc-eng3.doc).

Mars Polar Lander Descent Engine Plume Issues Summary — via Lad Curtis, e-mail of 03/14/00, presentation by H.H. Curtis, 03/14/00.

Mars Polar Lander EDL Attitude Determination — Tom Kelecy, 01/25/00, viewgraph presentation at LMA.

Mars Polar Lander EDL Inertial Navigator — Tom Kelecy, 01/25/00, viewgraph presentation at LMA.

Mars Polar Lander EDL Success Rates with Large CG Offsets — via Lad Curtis e-mail of 02/17/00; Bill Willcockson memo to Duncan MacPherson and Charles Whetsel.

Mars Polar Lander Entry Design States vs. Reconstruction, Pre-Entry Lateral Miss — via Lad Curtis e-mail of 02/17/00; memo from Bill Willcockson to Richard Cook et al. of 02/14/00.

Mars Polar Lander Large Aero Effects on EDL — Bill Willcockson, 01/10/00 memo to Ed Euler (via Lad Curtis e-mail of 01/13/00).

Mars Polar Lander Possible Premature Descent Engine Thrust Termination Process Investigation Report — Joseph Vellinga, MSP-00-5001, 02/10/00; via e-mail from J. Vellinga, 02/11/00.

Mars Polar Lander Premature Descent Engine Termination Due to Touchdown (TD) Indication Conclusions, LMA charts, H. H. Curtis, R. Gehling, J. Bene, G. Bollendonk, February 25, 2000.

Mars Polar Lander Premature Descent Engine Thrust Termination: Quantitative Definition of Likelihood — H.H. Curtis, J. Bene, R. Gehling, presentation, March 10, 2000; via e-mail from Lad Curtis, 03/13/00.

Mars Polar Lander Propulsion System Schematic — John Cuseo, 01/25/00, viewgraph presentation at LMA.

Mars Polar Lander Spacecraft Overview — Lad Curtis, 01/05/00 viewgraph presentation to Board at LMA.

Mars Polar Lander Surface Power Constraints — Handout, LMA Meeting 01/31/00.

Mars Polar Lander Touchdown Sensor Code Issue — Handout, LMA Meeting 01/31/00.

Mars Polar Lander Touchdown Sensor Code Issue — Lad Curtis, 01/27/00, viewgraph presentations to Board Review Teams at LMA (via Lad Curtis e-mail of 01/27/00).

Mars Polar Lander Touchdown Sensor Code Issue, LMA charts, H. Curtis, January 20, 2000.

Mars Polar Lander, Cold Descent Engine Issue Close-out — H.H. Curtis, 11/22/99.

Mars Surveyor Program (MSP) change summary: Lander Descent Velocity Change and Touchdown Sensor Change, UCN XB0114, September 18, 1996.

Mars Surveyor Program '98 Fault Protection Description Document, D-14512, dated 5 January 1998.

Mars Surveyor Program Landing Radar Overview of Flight Tests and GN&C Interfaces — John Cuseo and Bradley Haack, Report AAS 98-067, presented on 01/25/00 at LMA.

Mechanical Failure Review Splinter — Action Item Review handout package, February 3, 2000.

Mechanical Failure Review Splinter handout package, January 18–19, 2000.

Mechanical Systems Failure Review Team: Action Item Review — Jeff Bene via Frank Locatell, viewgraph presentation of 02/03/00.

Microwave component plating — via Kyle Martin e-mail 02/04/00.

Mission Assurance — Handout, DS2 Briefing 01/13/00.

MOC Photoclinometry — Mike Malin, 1/24/2000, viewgraph presentation to Environment and Landing Site Review Team at JPL, January 24, 2000.

More Info on Flow Split, LMA e-mail, T. Martin to J. Leising, 2/25/00.

More Rebuttal — Timothy Martin, 2/18/00, e-mail regarding section 4.0 of the draft MPL failure review board findings.

MPL 6-DOF EDL Touchdown Scatter, ± 2mm c.g. Dispersion Along Tank Axis — via Lad Curtis e-mail of 02/17/00; attached "flash memo #1," Bill Willcockson to Sam Thurman et al. of 02/15/00.

MPL ACS Working Group Actions — via Lad Curtis e-mail of 02/03/00: (1) Thomas Kelecy to Jim Chapel e-mail of 02/02/00 re: analysis to address action item #7; (2) Jim Chapel to Garry Burdick e-mail of 01/28/00 re: discussion of action items #1–10.

MPL Area Analysis of Pulse Widths [from MGS MOLA] — Maria Zuber to Casani, Whetsel, Murray, and MacPherson, February 6, 2000, e-mail correspondence.

MPL Avionics, report of the Avionics Review Team, Battel Engineering, document #BE/093/00/020, 02/03/00.

MPL Backshell Recontact Analysis — Bill Willcockson, 01/10/00 memo to Ed Euler (via Lad Curtis e-mail of 01/13/00).

MPL Center-of-Mass Analysis Status — Lad Curtis, 02/01/00 e-mail message reporting on CM analysis.

MPL Center-of-Mass Bound for TCM-4 and TCM-5 — Jason Wynn, 2/15/00, e-mail regarding center-of-mass offset via spacecraft rate of telemetry.

MPL Center-of-Mass Estimation Using TCM Telemetry Data — Jason Wynn, 2/17/00, GN&C PDO Technical Memo MSP AC-00-0381 to MacPherson, Whetsel, Burdick, Macala, Curtis, Euler, Chapel, Willcokson, Cwynar, Spath.

MPL Center-of-Mass Bound for TCM-4 and TCM-5 — via Jason Wynn e-mail of 02/15/00.

MPL Center-of-Mass Estimation Using Flight Dynamics Telemetry Data (file called MPL CG Uncert), and MPL Entry Body and Terminal Descent Mass Properties; Mechanical Coordination vs. ACS Coordinates (file name CG Offset, no cover slide) — via Lad Curtis e-mail of 02/10/00, viewgraphs from Kim Barnstable. (Re-sent via Jeff Bene with more information re: dry center-of-mass analysis in cover e-mail, 02/13/00).

MPL CM Offset Updates and Additions — Lad Curtis e-mail of 03/01/00 to Duane Dipprey et al.; update to Jason Wynn's memo re reconstruction of CM offset from flight TCM data; attachments: memo Jason Wynn to Duncan MacPherson et al. (MPL Center-of-Mass Estimation Using TCM Telemetry Data, 02/24/00, MSP-AC-00-0381 Rev A); presentation Lad Curtis (CM Offset Summary – Rev B, 02/29/00).

MPL Cruise Stage Separation Interim Report —Ed Euler, 01/03/00, memo SCR01-00 from Shane Roskie and LMA MPL team to Ed Euler.

MPL Descent Engine Termination: Correction — Lad Curtis e-mail of 02/25/00; notes that test date shown as 06-Jun-97 on pp. 8–9 of 02/25/00 presentation should be 16-Jun-97. Page 11 line item correctly identifies test date as 6/16/97.

MPL EDL Propellant Shift Analyses, Rev. A — Timothy Martin, 3/08/00, memo FSMO-00-008 to G. McAllister, M. Hetrick, J. Wynn.

MPL Entry Center-of-Mass Requirement — Lad Curtis, 01/13/00 e-mail message re: CM requirement for entry.

MPL Entry Risk Status Report — MacPherson et alia, November 19, 1999, viewgraph presentation to JPL MPL EDL Red Team.

MPL Flight Reconstruction of Center-of-Mass Offset Using all TCM Data — via e-mail from Lad Curtis of 02/17/00 to Duane Dipprey et al.; memo from Jason Wynn re estimation of center of mass using TCM flight telemetry data (MSP-AC-00-0381).

MPL Framotome Separation Connector Pull Test Results — via Lad Curtis e-mail of 02/24/00; Jeff Bene e-mail of 02/23/00 re tests.

MPL Fuel Tank Outlet Discussion — K. Miller, G. McAllister, 2/24/00.

MPL Lander to Backshell Clearance — Bill Willcockson, February 1, 2000, viewgraph presentation to Environment and Landing Site Review Team at LMA, February 1, 2000.

MPL Landing Estimates — Phil Knocke, January 13, 2000, viewgraph presentation to Environment and Landing Site Review Team at LMA, February 1, 2000.

MPL Maneuver Overview — Phil Knocke, January 13, 2000, viewgraph presentation to Environment and Landing Site Review Team at LMA, February 1, 2000.

MPL Mission Safety and Success Team Final Report — Charles Whetsel, December 1, 1999, IOM 3130-CWW-001.

MPL Premature Descent Engine Termination Conclusions — via Lad Curtis e-mail of 02/25/00; presentation for briefing to JPL MPL FRB on 02/25/00.

MPL Prop Line Temperature — via Lad Curtis e-mail of 02/15/00; info from Kevin Johnson to Milt Hedrick and Lad Curtis.

MPL Propulsion Peer Review Process — via Lad Curtis e-mail of 02/24/00; Greg McAllister e-mail to Lad Curtis of 02/22/00 with attachments: MSP Lander Propellant Differential Draining Analysis (memo from Timothy Martin to D. Doub et al., 01/17/97, MSP-PR-97-0122); MSP Lander Propellant Transfer Analysis Update – Rev. A (memo from Timothy Martin to D. Doub et al., 10/24/97, MSP-PR-97-0214 Rev A); Lander Prop CDR Action Item Summary (no date); Review Board Report: MSP '98 Propulsion Subsystem CDR Peer Review of 2–3 October 1996 (final report 10/29/96).

MPL Questions — Richard Cowley, 2/16/00, e-mail regarding hydrazine freezing and missing data period.

MPL Radar Lock on Heatshield — Lad Curtis e-mail of 02/17/00 to Garry Burdick et al.

MPL Small Forces Issues — Stu Spath, January 19th, 2000, viewgraph presentation to Environment and Landing Site Review Team at LMA, February 1, 2000.

MPL software changes and problem reports — via Lad Curtis e-mail 01/28/00.

MPL Tank Diaphragm Test ROM — Milt Hetrick e-mail of 02/07/00 to Jeff Leising.

MPL Tank Diaphragm Test ROM — Milt Hetrick, 2/7/00, e-mail regarding a ROM estimate of the test cost to obtain the necessary data on the MPL tank diaphragm.

MPL Tank Outlet Temperature: Additional Information — via Lad Curtis e-mail of 02/21/00; Kevin Miller e-mail of 02/18/00 has info and also refers to attachment to ISA #Z54100, a memo from Jon White re MSP '98 fuel tank status, 09/16/99.

MPL Telecom Fault Protection Enables/Disables — Handout, LMA Meeting 02/01/00.

MPL Telecom Screen Shots (Telemetry Data) — Handout, LMA Meeting 02/01/00.

MPL Throttle Engine Issue — via Lad Curtis, e-mail of 03/14/00; presentation Mars Polar Lander Pulse Modulated vs. Throttled Descent Engine Issue, Milt Hetrick and H.H. Curtis, 03/14/00.

MPL Uplink Log and Summaries — Kyle Martin, e-mail of 02/02/00: MPL Uplink Log; MPL Uplink Summary–EDL Uplinks; MPL Uplink Summary–Landed Prep Uplinks; MPL File Interchange System (FIS) Access Information.

MPL Uplink logs — via Kyle Martin e-mail 02/02/00 including the following files: MPL Uplink Logs — via Kyle Martin e-mail 02/02/00, including: MPL UL Log.xls MPL Uplink Log; MPL edl_uplink_sum.xls MPL Uplink Summary — EDL Uplinks; MPL landed_prep_uplink_sum.xls MPL Uplink Summary — Landed Prep Uplinks; MPL FIS Access.doc MPL FIS Access Information.

MPL Uplink Loss Response Timer — Change control package, LMA Meeting 01/31/00.

MPL Zero-G Fuel Transfer During Design and Development — via Lad Curtis e-mail of 02/17/00; info from Tim Martin.

MPL/DS2 Aero Environment Splinter, Entry Body Mass Properties — Kim Barnstable, February 1st, 2000, viewgraph presentation to Environment and Landing Site Review Team at LMA, February 1, 2000.

MPL/DS2 Review — Environment Review Team Session #1 Agenda — Charles Whetsel, January 24, 2000.

MPL/DS2 Review — Environment Review Team Session #2 Agenda — Charles Whetsel, February 1, 2000.

MPS Landing Radar Overview — John Cuseo and Dave Cwynar, 01/25/00, viewgraph presentation at LMA.

MSP Landed STV Test Profile — Handout, LMA Meeting 02/01/00.

MSP Lander Flight Propellant Load — J. Greg McAllister, 3/9/00, memo to L. Curtis, K. Barnstable, J. Lenada, C. Cooley.

MSP Lander Propellant Differential Draining Analysis — Timothy Martin, 1/17/97, memo to D. Doub, G. McAllister, P. Sutton.

MSP Lander Propellant Transfer Analysis Update - Rev A — Timothy Martin, 10/24/97, memo to D. Doub, G. McAllister, P. Sutton, W. Willcockson, L. Curtis.

MSP Lander Verification Report VR006, circa Dec 97.

MSP Telecom Subsystem CDR Peer Review, D-14526, dated 13 November 1996.

MSP'98 Propulsion Subsystem CDR Peer Review — 10/29/96, CDR Peer Review on 10/23/96, LMA.

MSP99-4070, Mars Polar Lander, Descent Thruster MR-107N, Cold Start Verification Test Report — 11/97, Tim Fischer, Kevin Johnson, LMA Propulsion PDO.

NASA Administrator's Weekly Topics: Fault-tree Analysis, 20 January 2000.

New Millennium DS2 Failure Review handout package, by Tom Rivellini, January 13, 2000, 86 pages.

Operational Process & Validation — Handout, DS2 Briefing 01/13/00.

Parachute Lengths — Milt Hetrick, 2/14/00, e-mail regarding the distance from the center-of-pressure of the chute to the MPL.

Parachute Propellant Transfer, LMA e-mail, M. Hetrick to J. Leising, 3/10/00.

Parachute System — Lad Curtis, 01/12/00 e-mail message describing telecon with Leff Lavell.

Plumes — Milt Hetrick, 3/8/00, e-mail.

Possible Failure Modes — Handout, DS2 Briefing 01/13/00.

Post-Landing Loss of Signal Fault Tree — Handout, LMA meeting 01/31/00.

Post-Landing Loss of Signal Fault Tree — Steve Jolly, 01/05/00 viewgraph presentation to Board at LMA.

Power & Pyro: Answers to Questions — Lad Curtis e-mail of 02/11/00 re: coaxial switches, system design changes for MSP '01, Radar tests. Includes viewgraph presentation to MPIAT on 01/20/00 re: comparison of MSP '98 with MSP '01 (file name = 15MSP01).

Presentation — MPL Aeroshell Environments and TPS Design, — Willcockson, Edquist, and Thornton, February 1, 2000, viewgraph presentation to Environment and Landing Site Review Team at LMA, February 1, 2000.

Propulsion EDL Timeline — via Lad Curtis e-mail of 02/11/00, Greg McAllister.

Radar Test Review — John Cuseo and Brad Haack, 01/25/00, viewgraph presentation at LMA.

Re: Actions from 1/24 MPL/DS2 Landing Site Splinter, Ken Herkenhoff to Charles Whetsel, March 7, 2000, Email Correspondence.

Re: MPL Landing Site... [Absence of Terracing] — Tom Duxburry to Charles Whetsel, February 11, 2000, Email correspondence.

Recommended Environments and Design ranges for the Mars Microprobe — Sue Smrekar and George Powell, Feb. 19, 1997, revised Aug. 12, 1997, Memorandum.

Reply to Inadequate Thermal Margin and Deviation from Accepted Design Practice — Lad Curtis, 3/6/00, e-mail with attachment regarding Temperature Margin Management on Wetted Propulsion Components and MPL by Kevin Miller, 3/6/00.

Report on the Loss of the Mars Climate Orbiter Mission – JPL Special Review Board, JPL internal document, JPL D-18441, November 11, 1999.

Results of July 18–19, 1996 MR Compatibility Test at Lockheed Martin Astronautics, Denver , Colorado, Release July 25, 1996.

Results of May 31, 1996 MR Compatibility Test at Lockheed Martin Astronautics, Denver, Colorado, Release July 2, 1996.

Review of Temperature Margins for Deployment Mechanisms and Separation Devices — via Frank Locatell, 11/22/99 viewgraph presentation to JPL Red Team by Locatell and Kevin Miller (LMA thermal engineer).

RF Switch Materials — via Kyle Martin e-mail of 02/10/00, response from Teledyne re: possible cold welding.

RF Switch Materials — via Kyle Martin e-mail of 02/10/00, response from Teledyne re: possible cold welding.

Sequence C — Sequence of Events, Generated December 1 03:20:20, 1999.

Slosh Model — Philip Good, 01/26/00, report presented at LMA.

Software Development Story to MPIAT — Lad Curtis e-mail of 02/23/00 to John Casani and Al Schallenmuller; also John McNamee responded to same topic.

Standards Document Problem/Failure Reporting System, Guidelines and Procedures, JPL internal document, JPL D-8091, August 1998.

SOL 0 and Landed Init Timeline — Handout, LMA 01/31/00.

SOL 0 to SOL 33 Timeline — Handout, LMA 5/6 January 2000.

Spider Architecture — Handout, LMA Meeting 01/31/00.

Status of Center of Mass Action Items — Glenn A. Macala, 2/28/00, e-mail regarding further update.

STL Sequence Runs — Handout, LMA Meeting 01/31/00.

Structural Test Program Overview — Handout, DS2 Briefing 01/13/00

STV REA Thermocouple Locations — November 1997.

Surface Dust Disturbance and Deposition During Mars '01 Landing — Carl Guernsey, 4/25/99, memo to Eric Suggs.

Surveyor PDS Analysis — via fax Jim Chapel to Bill Ely and Joe Protola, 01/24/00, presented at LMA.

System and Mission Design Overview — Handout, DS2 Briefing 01/13/00.

Tank Diaphragm Testing - Centaur Tank — Milt Hetrick, 2/15/00, e-mail regarding update on Centaur water hammer testing.

Tank Diaphragm Testing Quick Look Data — via Lad Curtis, e-mail of 03/14/00, presentation by Propulsion PDO and EPL, 03/10/00.

Tank Diaphragm Quick Look Data, Rev. A — LMA presentation, M. Hetrick et al., March 15, 2000.

Tank Line Temperature — via e-mail from Lad Curtis of 02/17/00; responses to queries from Richard Cowley and Jeff Leising. Attachment: TCM and SAM burns. Follow-up e-mail from Kevin Miller of 02/17/00 referring to documentation in ISA #Z54100 closed 11/20/99.

TCM-5 Line Temp Trace — via Lad Curtis e-mail of 02/16/00; Greg McAllister e-mail to Richard Cowley of 02/15; flight data from EDL -1 hr (approx): "MPL Final Contact Data Surrounding Pressurization."

TCM-5 Rationale - Cross-track Capability — Phil Knocke, February 1, 2000, viewgraph presentation to Environment and Landing Site Review Team at LMA, February 1, 2000.

TD Sensor PIE and Involvement, 25 February 2000, e-mail message from Lad Curtis.

Telecom Action Items from 02/01/00 — via Kyle Martin e-mail of 02/10/00, memo from William Adams and Scott Toro-Allen on remaining action items (includes responses re: what are view angles of all antennas?; if 10 dB down on UHF signal seen at Stanford, what does that mean for comm with other antennas?; is there some off-nominal landing orientation that precludes X-band and UHF comm?).

Telecom Overview — Handout, LMA Meeting 01/31/00.

Telecommunications Subsystem — Handout, DS2 Briefing 01/13/00.

Terminal Descent Phase Overview — John Cuseo, 01/25/00, viewgraph presentation at LMA.

Testing of the MPL 1/2" Pyro Valves in Propellants — via Lad Curtis e-mail of 1/10/00 from George E. Cain e-mail on 1/7/00.

Testing of the MPL 1/2" Pyro Valves in Propellants — via Lad Curtis 01/10/00, memo from George Cain to Lad Curtis of 01/07/00.

The Extent of the Post-Launch MGS Mars Relay Mode Confirmation, John Callas e-mail, 03/09/00.

Throttled Thrusters — Milt Hetrick, 3/8/00, e-mail.

Touchdown Sensor Comments — Lad Curtis e-mail of 02/10/00 re: possible new leg deploy tests; sensor miswiring at ATLO test.

Touchdown Sensor Flow Chart — via e-mail from Lad Curtis of 02/17/00; functional flow chart for TD sensor code.

Touchdown Sensor Leg Deploy Testing — via Lad Curtis 02/09/00, Russ Gehling viewgraph presentation to MPIAT on 02/09/00 (no cover slide on presentation).

Touchdown Sensor PIE and Involvement — Lad Curtis e-mail of 02/25/00 to John Casani et al., re issues surrounding cause of premature descent engine termination.

Touchdown Sensor Tests — via Lad Curtis e-mail of 02/09/00; presentation to MPIAT on 02/09/00 (no cover slide on presentation).

Touchdown Sensor Tests — via Lad Curtis e-mail of 02/17/00; Jeff Bene e-mail of 02/09/00 to Wes Menard re status and charts from Russ Gehling.

Umbilical/Electronics Packaging Design and Verification — Handout, DS2 Briefing 01/13/00.

Why No Downlink Capability During EDL for MPL? — John McNamee to Ed Stone et al., via e-mail, 12/08/99.

Appendix 2

Review Team Members and Consultants

Environment and Landing Site

Charles Whetsel (Review Team Leader)
Arden Albee
Bobby Braun
Pete Burr
Mike Carr
John Casani
Tom Duxburry
Ken Herkenhoff
Randy Kirk
Duncan MacPherson
Michael Malin
Wes Menard
David Paige
Tim Parker
Sue Smrekar
Dave Spencer
Ash Vasavada
Maria Zuber
Richard Zurek

Mechanical Systems

Wes Menard (Review Team Leader)
Frank Locatell (Deputy Team Leader)
Keith English
Jeffrey Lavell
Donald Lewis
Chia-Yen Peng
Don Sevilla
John Vasebinder

Dynamics and Control

Garry Burdick (Review Team Leader)
Douglas Bernard
Robert Bunker
Edward Kopf, Jr. (Ted)
Glenn Macala
Richard Rose (TRW, ret.)
Alejandro San Martin (Miguel)
Joseph Savino
Charles Whetsel

Communications/Command and Data Handling
Richard Brace (Review Team Leader)
James Donaldson
Mark Schaefer
Julie L. Webster

UHF Subteam
Richard Horttor. Lead
Jim Border
John Callas
Phil Knocke
Steve Lowe
George Resch

Propulsion and Thermal
Jeff Leising (Review Team Leader)
Ron Carlson (Section 353 Propulsion Lead)
Duane Dipprey
Phil Garrison
Carl Guernsey
Hartwell Long
Barry Nakazono
Tim O'Donnell
Morgan Parker
Ron Reeve (Thermal)
Bob Sackheim

Avionics
Steven Battel (Review Team Leader)
Richard Brace
Garry Burdick
Joe Savino

Flight Software/Sequencing
Al Schallenmuller (Review Team Leader)
Richard Brace
Garry Burdick
Glenn Reeves
Charles Whetsel