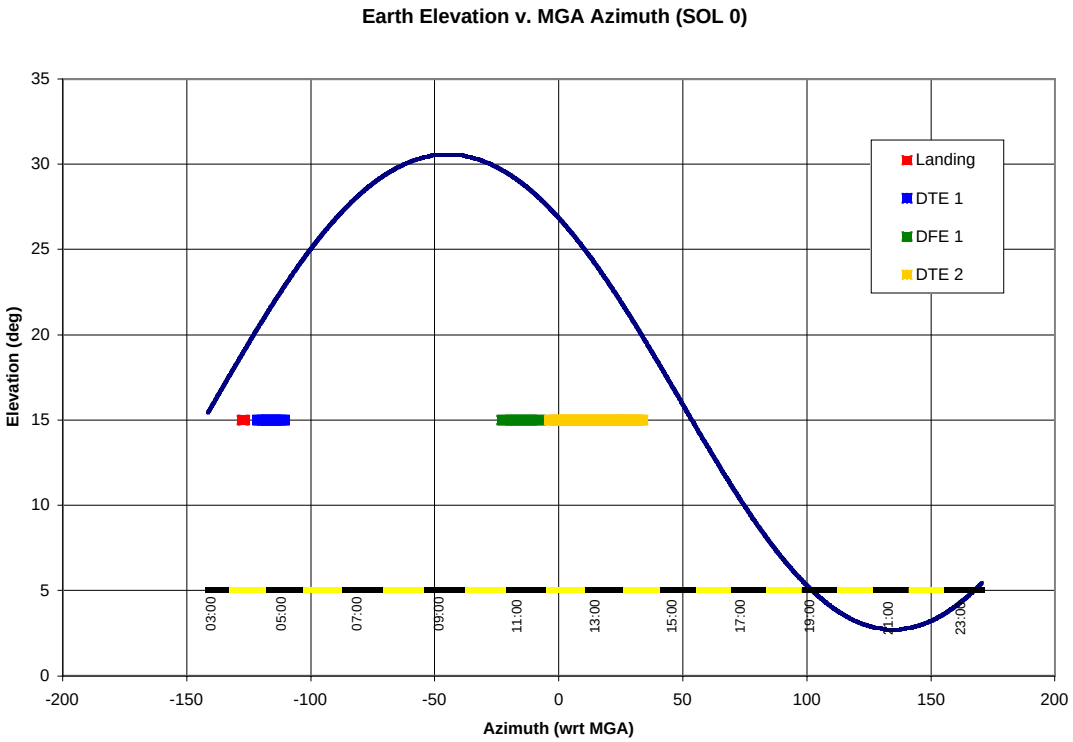


**Figure 7-5. Earth Geometry for the Nominal Landing Orientation and Site on Sol 0**

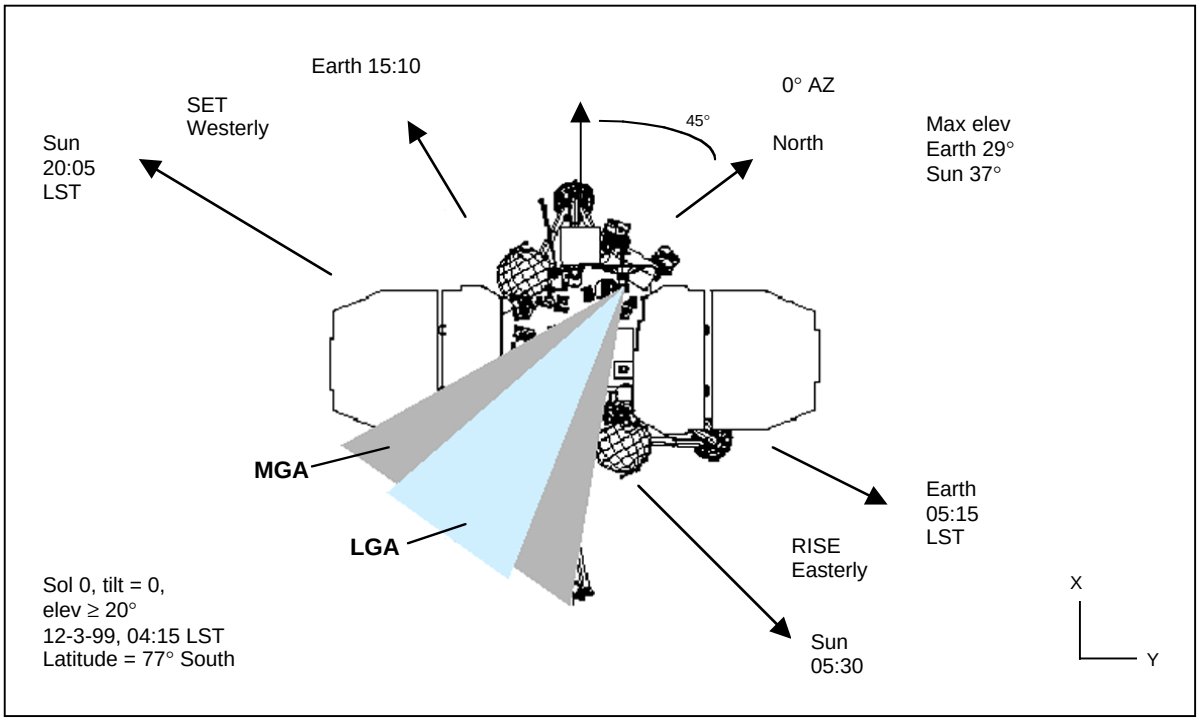


**Figure 7-6. Command-Blind Zones in Azimuth for MGA (125 bps) and LGA (7.8125 bps)**

*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 $2.8 \times 10^{-5}$.

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

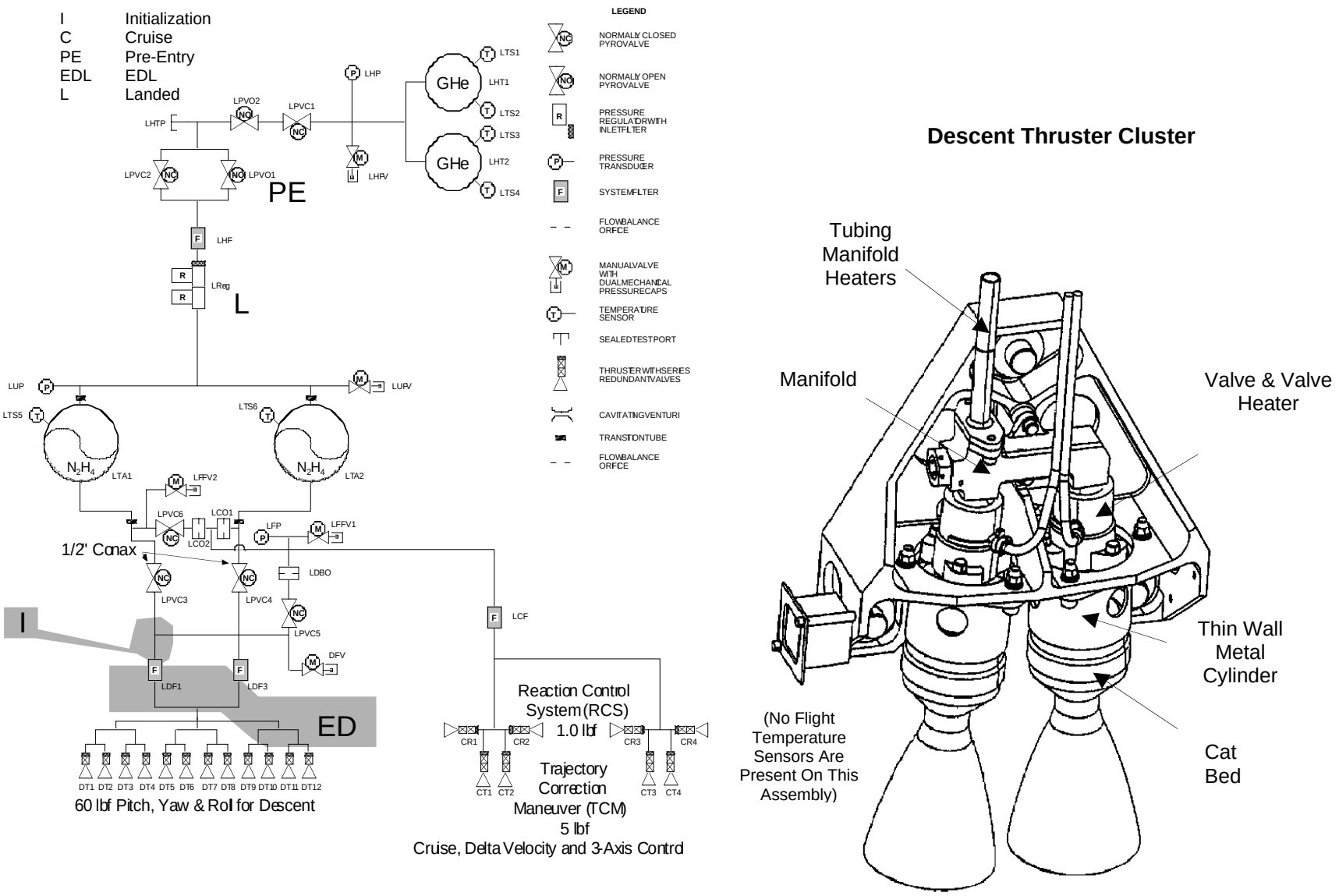


**Figure 7-7. MPL Propulsion Subsystem Schematic**

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.

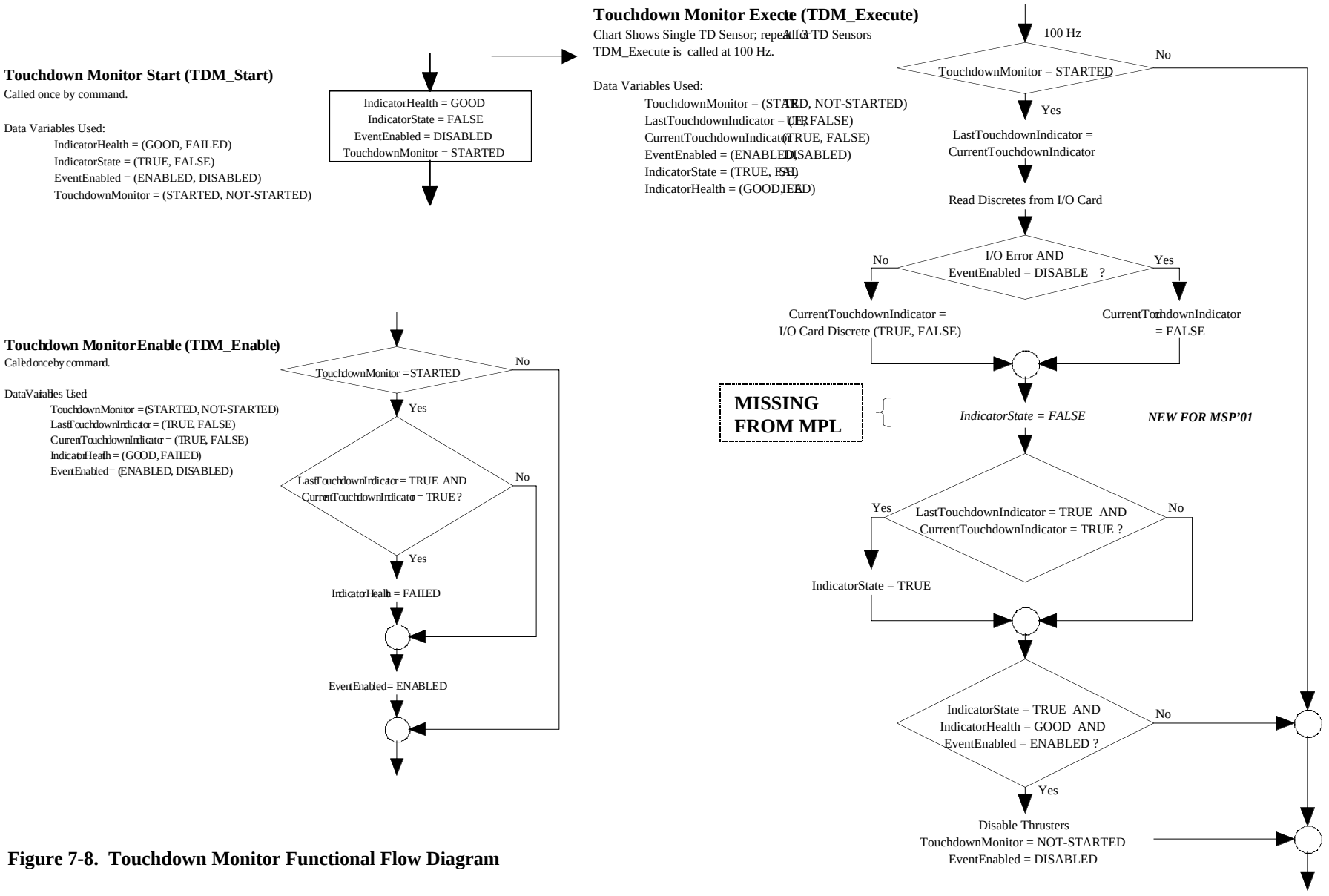


**Figure 7-8. Touchdown Monitor Functional Flow Diagram**

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.

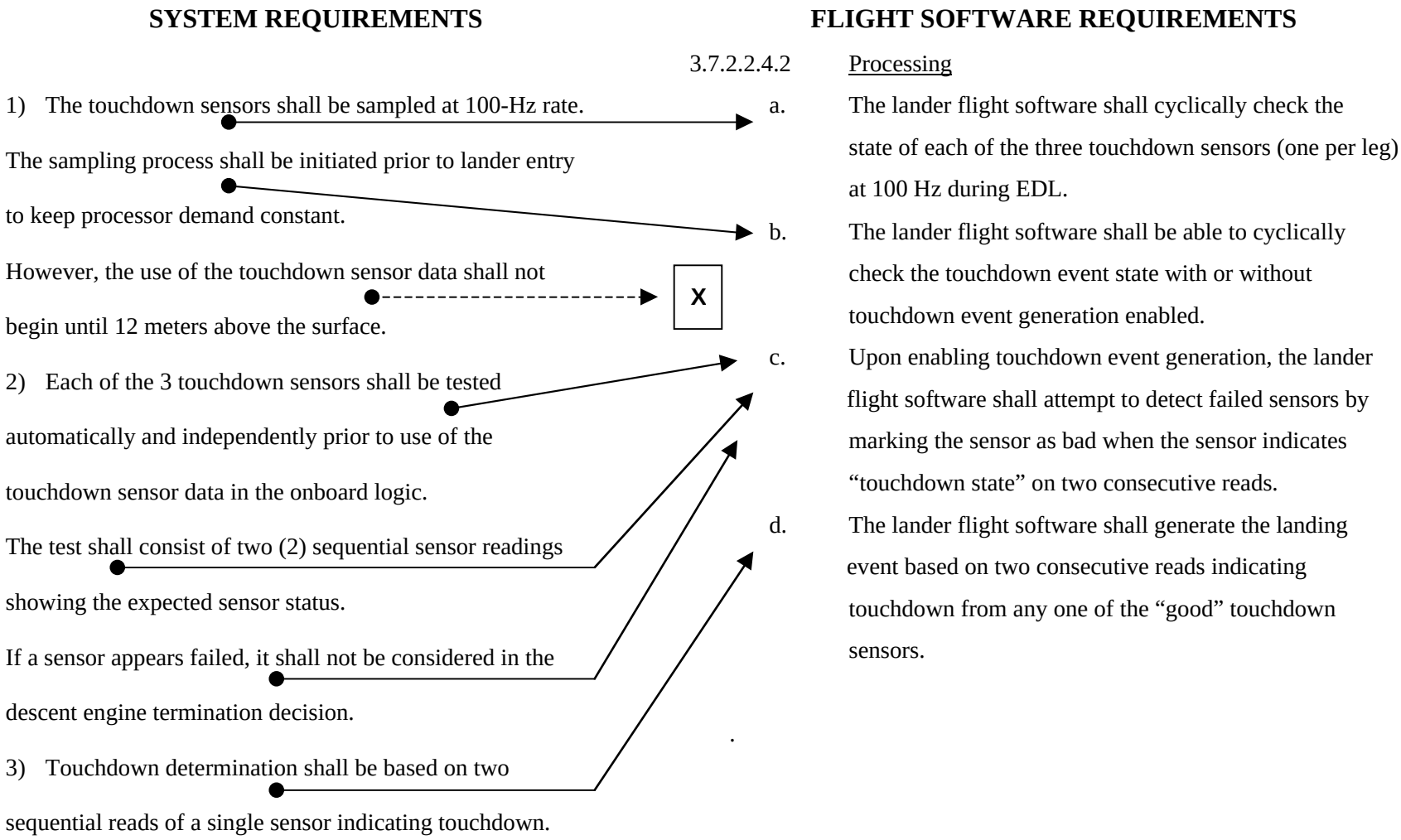


**Figure 7-9. MPL System Requirements Mapping to Flight Software Requirements**

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.