



**AAS 01-074**

**THE FAILURES OF THE MARS CLIMATE ORBITER AND MARS  
POLAR LANDER: A PERSPECTIVE FROM THE PEOPLE  
INVOLVED**

**Edward A. Euler and Steven D. Jolly**  
**Lockheed Martin Astronautics Operations Denver, CO**  
**H. H. 'Lad' Curtis**  
**ITN Energy Systems Littleton, CO**

---

**24th ANNUAL AAS GUIDANCE AND CONTROL CONFERENCE**

---

January 31 - February 4, 2001  
Breckenridge, Colorado

Sponsored by  
Rocky Mountain Section



AAS Publications Office, P.O. Box 28130 - San Diego, California 92198

# **THE FAILURES OF THE MARS CLIMATE ORBITER AND MARS POLAR LANDER: A PERSPECTIVE FROM THE PEOPLE INVOLVED**

**Edward A. Euler and Steven D. Jolly**

**Lockheed Martin Astronautics Operations Denver, CO**

**H. H. 'Lad' Curtis**

**ITN Energy Systems Littleton, CO**

The failures of the Mars Climate Orbiter and Mars Polar Lander were the subject of numerous failure review boards composed of senior personnel not closely associated with the projects. The causes and corrective actions were well documented, however, these reports did not capture inner workings of the projects and the subtle things that happened that eventually led to the failures. This paper will present the story from the perspective of the people intimately involved with the design, development, and operation of the vehicles. In the case of the MCO, it is a story about how a number of seemingly unrelated events and actions finally led to the large navigation error and how that error could remain undetected by a group of competent and dedicated engineers and managers. In the case of the MPL, it is a story of how a flight software code error was made, why it was made, and why it went undetected through a very rigorous test program. It is hoped that these examples will lead not only to a further sense of awareness, but to emphasize once again that there are some inviolate principles that should never be compromised in the development of one-of-a-kind single flight missions.

## **INTRODUCTION**

In 1994, NASA established the Mars Surveyor Program (MSP), dedicated to the long term exploration of Mars at each minimum energy Earth-Mars transfer opportunity (every 26 months). The program was to consist of orbiting vehicles for global reconnaissance and surface vehicles for in situ scientific investigations at various sites around the planet. At the start of the program, both the Mars Pathfinder (MPF) project (part of the Discovery program) and the Mars Global Surveyor (MGS) project were well into development and scheduled for launch during the 1996 launch opportunity.

MGS was the first mission in the Mars Surveyor Program. The next two missions were to be a lander (later named the Mars Polar Lander, MPL) and another orbiter (which became the Mars Climate Orbiter, MCO) scheduled for launch during the 1998 opportunity. At this time, NASA had fully embraced the "Faster, Better, Cheaper" philosophy and imposed some demanding requirements on the Mars Surveyor '98 project: a 37 month Phase C/D development schedule, spacecraft launch masses consistent with launch on Med-Light class launch vehicles, and a financial cap of about \$184M covering development of the space vehicles, scientific payloads, and the ground operations system (excluding launch vehicle costs). A separate project was established, called the Mars Surveyor Operations Project (MSOP) to perform the operations for MGS and all of the succeeding missions under the Mars Surveyor umbrella. This project also had a cost cap for conduct of all mission operations.

In February 1995, the Jet Propulsion Laboratory (JPL), which was managing the MSP'98 project for NASA, selected Lockheed Martin Astronautics in Denver as the spacecraft contractor for the MSP project. In addition to the NASA requirements mentioned earlier, the system design selected required the MPL to perform a direct entry into the Mars atmosphere and execute a soft landing near the South Pole of Mars, since this was a unique opportunity to land during the southern summer when the south polar cap receded to minimum area. The MCO science payload included a wide field camera and an infrared radiometer originally flown on the Mars Observer mission. In order to achieve the desired 400 km near-circular polar orbit within launch mass constraints of the "Med-lite" launch vehicle, the MCO was designed to propulsively capture to a loose orbit around Mars, then use the aerobrake technique (also used for MGS) to slowly reduce the orbit apoapsis to the required value.

The combined set of cost, schedule, and technical requirements were extremely challenging for a new interplanetary mission. The project had to rely heavily on design heritage from previous missions (MGS, MPF, Viking) and keep project teams at all participating organizations to absolute minimum size. The dependence on heritage design and operations eventually became a contributing factor in the loss of the MCO.

During the development time period for the two MSP'98 vehicles, the name of the game was to be very creative in management and technical planning to reduce each step in the development process to the mandatory elements and eliminate all direct non-value added activities. Take some risk, but manage it carefully. The project worked to this philosophy and did not at any time feel the risk had become unacceptable. Many of the decisions made early in the project were later criticized by the various failure review teams as too risky, but at the time, they were consistent with the "FBC" philosophy and reviewed and accepted by NASA review boards external to the project.

After the failure of the MCO, failure review boards were commissioned by JPL (Ref.1), and by NASA (Ref.2). With the additional failure of the MPL, again JPL commissioned a special review board to establish a most probable cause (Ref 3.) and NASA established the Mars Program Independent Review Team (MPIAT) chaired by A. T. Young (Ref. 4) that reviewed the entire Mars Surveyor Project history and led to a significant restructuring of the Mars exploration program. The intent of this paper is not to question or disagree with the findings of the various boards (they were fair and accurate), but to explain the environment and circumstances that existed from the viewpoint of the personnel intimately involved. The 300 or so talented JPL, Lockheed Martin, payload supplier, scientists, and subcontractor personnel dedicated a substantial portion of their lives to make this project a success. They deserved a better fate.

## **PART I: THE MARS CLIMATE ORBITER**

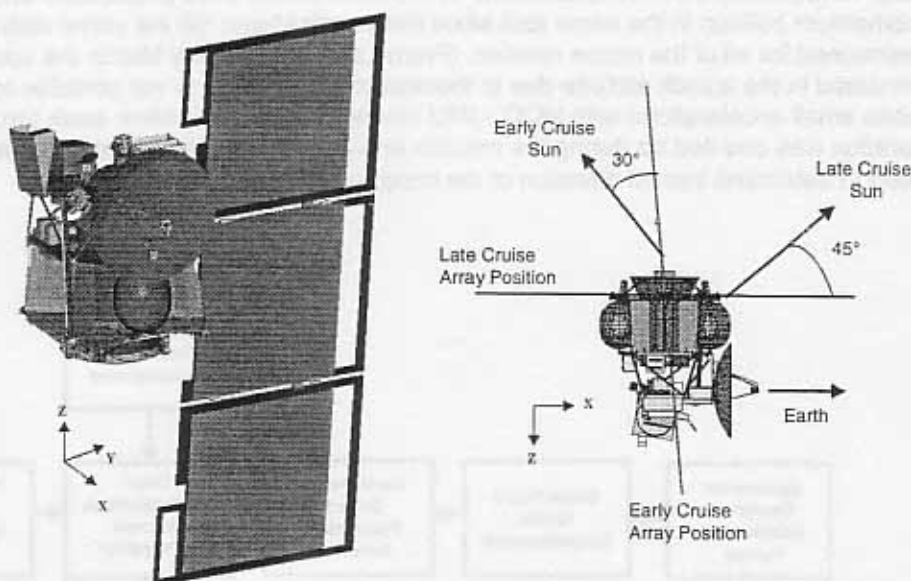
### **Mars Climate Orbiter Mission Overview**

The objective of the Mars Climate Orbiter (MCO) mission was to deliver an infrared radiometer (Pressure Modulated Infrared Radiometer, PMIRR) and a multispectral camera assembly (Mars Color Imager, MARCI) into a low, near-circular, Sun-synchronous orbit around Mars. The PMIRR was to collect data on the Martian climate and atmospheric/surface processes that will provide the basis for an atmospheric circulation model of Mars. The MARCI was to perform surface and atmospheric imaging with both wide and medium angle staring array cameras with "pushframe" color filter arrays (IFOV of 7.2 km and 40 m respectively). MCO was designed to provide relay link support for the playback of MPL landed science data following aerobraking and attainment of the mapping orbit. The Orbiter was compatible with the Delta II 7425 launch vehicle, and was launched on a Type II transfer trajectory on December 11, 1998. MCO performed four Trajectory Correction Maneuvers (TCMs) during its 9 month cruise phase. Mars Orbit Insertion (MOI) occurred on September 23, 1999, and was to be followed by 66 days of aerobraking to achieve the final mapping orbit. Mapping would then have been conducted for a full Martian year. Lander science relay support was also to be initiated with the mapping phase, and continue for a total of

5 Earth years in order to support follow-on Lander missions. The mapping orbit was chosen to meet planetary protection requirements.

The Attitude Control System (ACS) employed three-axis control for cruise, orbital acquisition, and orbital mission phases, facilitating TCM control, MOI control, inertial slewing, and nadir pointing. An analog sun sensor provided  $2\pi$  steradian sun-sensing for use in sun acquisition, search, and safe modes, an Inertial Measurement Unit (IMU) provided rate and attitude update information in all modes. A star camera initialized and updated the Kalman filter attitude estimates in the inertial hold/slew, cruise, and mapping modes, and reaction wheels (RW) provided fine attitude control and slewing capability.

The Rocket Engine Modules (REMs) were used for attitude control during the TCMs, MOI, and the aeropass, and for dumping accumulated angular momentum. The REMs consisted of four 22-N aft-facing thrusters and four 0.9-N roll thrusters. The 22-N thrusters were on-pulsed at 10 Hz to provide yaw and pitch control (about the orbiter X and Y axes respectively) during the 500-N main engine burn for MOI. The 22 N thrusters are also used to impart  $\Delta V$ s for all four TCMs, and are off-pulsed at 10 Hz to provide pitch and yaw control. The 0.9-N thrusters are pulsed at 10 Hz to provide roll control (about the orbiter Z axis). Because the 0.9-N and the 22-N thrusters both have small minimum impulse bits, any of the thrusters could be used to dump momentum from the 4-N-m-s RWs.



**Figure 1. MCO Cruise Configuration**

The orbiter cruise configuration is shown in Figure 1. The solar array (SA) is deployed, while the high gain antenna (HGA) remains stowed until after mapping orbit is achieved. During cruise the orbiter was flown with the SA offpointed from the sunline by approximately  $60^\circ$ , the inner gimbal is set at approximately  $-41^\circ$ , outer gimbal is set to  $0^\circ$ . During the first 15-20 days following Launch, the spacecraft body was rotated about the Y axis by  $14^\circ$  to shade the Star Cameras. The Orbiter essentially cruised in an orientation very similar to the safe mode orientation so when in safe mode the only difference was that the solar array is placed normal to the sun line. During late cruise the HGA was pointed at the Earth and the solar array offpoint was fixed at  $45^\circ$ . The SA was articulated into a passive restraint for TCMs and MOI in order to maximize control



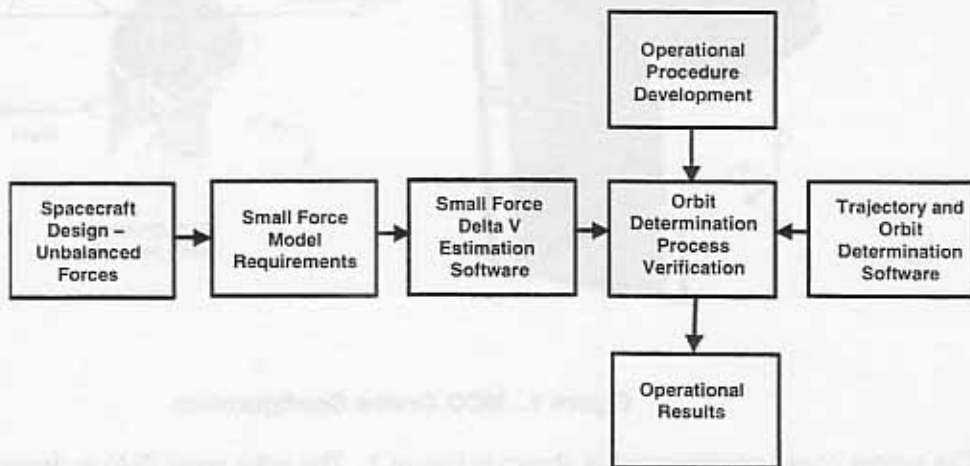
and minimize cross track errors. This position of the array while restrained was similar to launch where the array was against the spacecraft body (but panels open).

### ACS Spacecraft Performance Summary from Launch to MOI

Twelve housekeeping-type sequences with durations of approximately 3-4 weeks each were uplinked and executed during Cruise. Minimal ACS commanding was contained in these sequences as the spacecraft maintained Earth Point mode for all of cruise. The total fuel usage for the mission, up until the start of MOI, was 8.3 kg out of the 189 kg loaded at Launch. Usage for desats was close to pre-Launch predicts with an average of 7 grams/day, and overall usage well under the budget primarily due to a small TCM-1. Controller performance overall was excellent, with no in-flight modifications needed. Minimal solar array movements were executed during the mission, with large motions performed only to stow the array for TCMs. A fixed position was used for the majority of the Cruise phase. Autonomous reaction wheel desaturation frequency occurred every 10-20 hours, with the shortest mean time between desats being in mid-Cruise. Desats were accomplished in all 3 axes simultaneously.

### Orbit Determination Process and the Angular Momentum Desaturation Files

The orbit determination process must be able to account for all accelerations experienced by the spacecraft, especially those unbalanced forces imparted during autonomous momentum desaturations during the cruise phase of the mission (see Figure 2). MCO performed these reaction wheel desaturations approximately once every 17 hours, primarily due to asymmetric solar wind pressure on the spacecraft. The desaturations were predictable and were triggered by momentum buildup in the same axis since from early March '98 the same attitude was essentially maintained for all of the cruise mission. (From Launch until early March the spacecraft had remained in the launch attitude due to thermal constraints.) It is not possible to directly measure these small accelerations with MCO's IMU accelerometers, therefore each thruster pulse and duration was counted up during the mission and the thruster alignment and spacecraft attitude used to determine inertial direction of the imparted  $\Delta V$ .

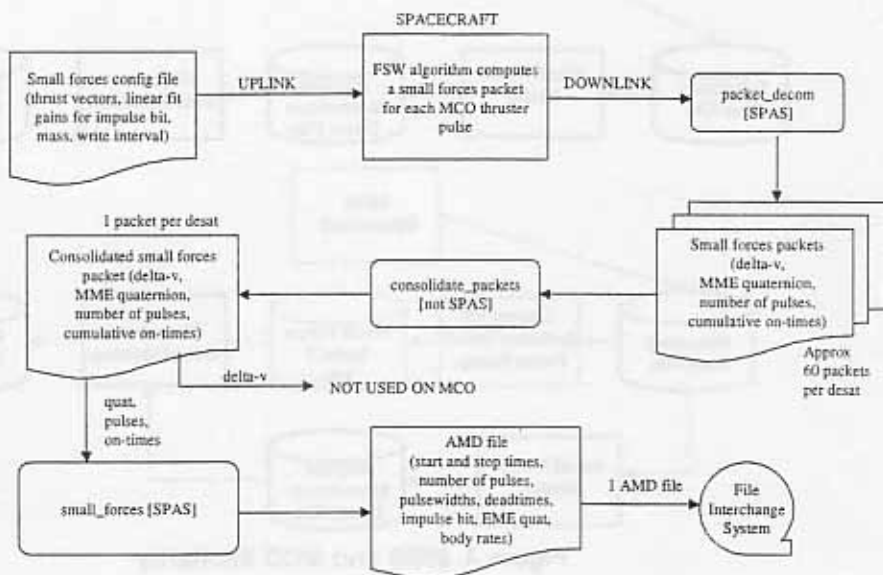


**Figure 2. Unbalanced Forces and Orbit Determination**

Onboard the spacecraft, the flight software small forces algorithm would compute a small forces telemetry packet for each MCO RCS thruster pulse (reference Figure 3). Except during TCMs,

approximately sixty packets per desat event (one per pulse) were generated and downlinked to the ground. Each packet contained the inertial delta-V vector, the number of pulses, and the cumulative on-times.

The next step was to use a ground data system software entity - the Spacecraft Performance Analysis Software (SPAS) "small\_forces" - to produce Angular Momentum Desaturation (AMD) files which would be placed on a file server for the Navigation team access. The SPAS tool would take the quaternion, number of pulses, and the on-times from the flight data. Even though the MCO spacecraft software did calculate the predicted delta-V from each pulse in the correct units, the SPAS software would not use this data but instead performed its own calculations. This was the same way that Mars Global Surveyor (MGS) small forces are calculated (reference Figure 4), as the purpose was to use Mars Observer (MO)/MGS heritage software.



**Figure 3. AMD Process Flow**

Prior to April 16, 1999, there was 1 AMD file produced for every downlinked spacecraft small forces packet. Because of the sheer number of packets involved with every desat, the Flight and Navigation teams agreed to consolidate the packets into 1 AMD file per Desat event. This wasn't accomplished until about 4 months into the cruise phase where another ground routine consolidated the small forces packets into 1 packet per desat - still containing delta V, inertial delta-V vector, number of pulses, and cumulative on-times, before handing over to the SPAS tool.

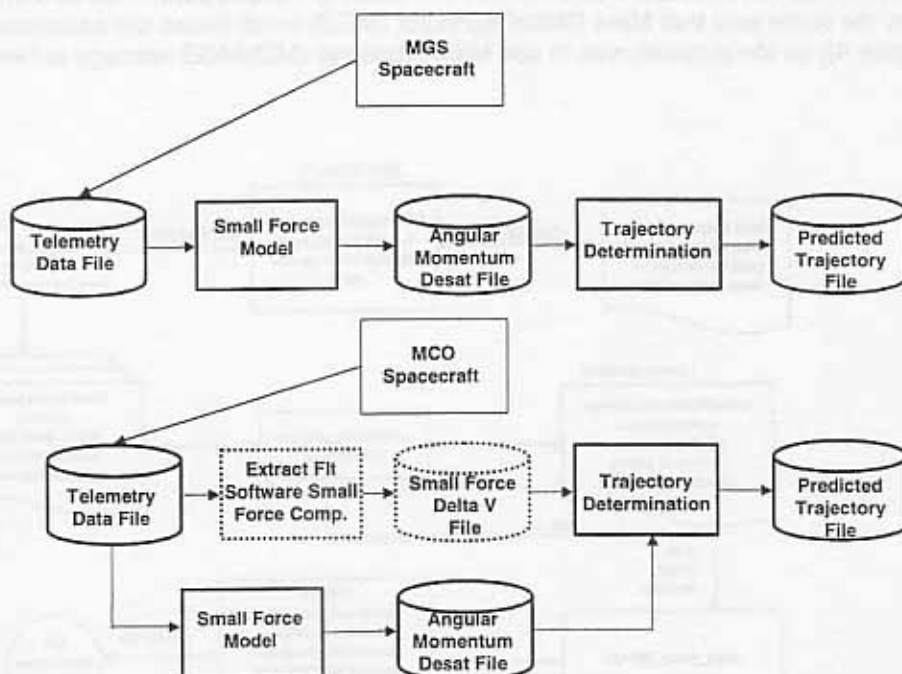
### Flaw in the Spacecraft Performance and Analysis Software

The AMD files that the SPAS entity generated are required to conform to an MGS-heritage Software Interface Specification (SIS) which specifies the exact file contents (format and units). An error was contained in the impulse-bit (I-bit) calculation portion of the software: it did not convert the I-bit from lbf-sec to N-sec, which were the units specified in the SIS.

The equations used to make the I-bit calculation are vendor supplied and in English units (in the case of this vendor). Although starting from MGS-heritage software, the coded MGS thruster equation had to be changed because of the different size RCS thruster that MCO employed (same vendor). As luck would have it, the 4.45 conversion factor, although correctly included in the MGS equation by the previous development team, was not immediately identifiable by

inspection (being buried in the equation) or commented in the code in an obvious way that the MCO team recognized it. Thus, although the SIS required SI units, the new thruster equation was inserted in place of the MGS equation - without the conversion factor.

Requirements walkthroughs and subsequent code walkthroughs failed to expose the flaw, and in the formal S/W acceptance testing the "truth" AMD file (computed manually) used for comparison contained the same error as the acceptance test output file. Similarly, informal interface testing with the Navigation team did not test the truth of the file but concentrated on making sure it could be moved across on the file server.



**Figure 4. MGS and MCO Similarity**

As will be discussed later in the paper (lessons learned section), the best chance to find and arrest this problem existed at the early levels of development. But the team also failed to recognize the importance of this SPAS software and the same attention given to flight software (FSW) was not accomplished. Technical management accepted the "just like MGS" argument and did not focus on the details of this software. (There were other notable format issues that plagued this process of AMD file generation, issues that ultimately served to obscure the real problems and distract the Flight and Navigation teams, but they are not as pertinent to this discussion and are therefore not covered in detail).

In summary, the large errors in the predicted small forces were inconsistent with the model used in the orbit estimation process. This, in turn, led to an error in the state at closest approach to Mars. Unfortunately, the error was in the only direction (toward the planet) that could lead to catastrophic consequences.

The next section will enumerate the chronology leading up to the loss of MCO and illustrate the frustration the Flight Team experienced in ultimately failing to uncover this fatal flaw. This is not done by way of defense, but rather to understand the context in which this failure occurred and to drive out a few more valuable lessons that should be learned from MCO's unfortunate fate.

## Chronology and Context of MCO Loss

### **Launch**

The Mars Climate Orbiter (MCO) was successfully launched on December 11, 1998 from CCAFS onboard a Delta 7425. Rate damping following third stage separation was very minor, only 19.4 seconds, indicating very low rates. Solar array deployment was nominal. The Star Camera acquired attitude on the second try (which was expected with the Earth likely being in the FOV on the first attempt). Telemetry was first acquired at 19:45:08 UTC following a nominal separation from the Delta upper stage. All systems functioned nominally during ascent and acquisition, with the exception of a few short Star Camera outages. The accuracy of the interplanetary injection provided by the launch vehicle was excellent as can be seen from Table 1.

Orbit Parameter	Actual	Targeted	Error	3 $\sigma$ accuracy
Perigee Radius (nmi)	3544.3	3543.9	+0.4	+2.3
C3 (km <sup>2</sup> /sec <sup>2</sup> )	10.92	10.89	+0.03	+0.22
DLA (deg)	15.62	15.46	+0.16	+0.53
RLA (deg)	-142.16	-142.25	+0.09	+1.16

**Table 1. MCO Launch Injection Performance**

### **Trajectory Correction Maneuver 1**

The Mars Climate Orbiter conducted a successful TCM1 on Dec. 21, 1998. The TCM magnitude was small (19 m/s) due to the excellent injection and basically removed the trajectory bias that was put in to assure third stage flyby of Mars. The post-TCM evaluation by the Flight Team and Navigation confirmed an actual 19.174 m/s  $\Delta V$  against a desired 19.210 m/s and pointing errors of only 9.8 mrad (RSS of x and y component).

TCM 1 was unaffected by the small forces anomaly due to the small number of desats since launch, the different radiometric observation angles associated with early cruise, as well as the fact that the AMD files were not being used at this time by the Navigation team.

Because of the format issues associated with the AMD files and the sheer number of files, which Navigation and the Flight Team agreed to reduce by consolidating, the Navigation Team basically used estimates of the small forces affect on trajectory by relying on e-mail communication from the Flight Team. So, for the design of both TCM 1 (Dec. 21, 1998) and TCM 2 (March 3, 1999), the flawed data was not used.

### **Trajectory Correction Maneuver 2**

TCM 2 was successfully executed on 99-063 at 14:44:00 UTC. The articulation of the solar array, and the subsequent slews, and the burn, were all nominal. The integrated attitude error yielded a 36.5 mrad overall pointing error, against a requirement of less than 100 mrad. The delta V of TCM 2 was designed to be 0.8586 m/s. MCO's four 5lb TCM thrusters burned for 8.4 sec, producing a spacecraft measured delta V of 0.8577 m/s. Navigation's quick-look analysis of the effective burn indicated an actual delta V of 0.917 m/s. However, the quick look burn reconstruction did indicate execution well within the 1 sigma B-plane error ellipse.

### **Trajectory Correction Maneuver 3 (MOI- 59 days)**

TCM 3 was the turning point for the Flight Team in that observable data began to show that something was amiss in the design and execution of the maneuver. Up to this point the Navigation team had been using estimates of the small forces delta-V as discussed before – without the flawed SPAS-generated data. But finally all the format issues had been resolved, the packet consolidation S/W tested and in place, and on or about April 19, 1999 the SPAS data was available for the Navigation Team. In fact, the Flight Team ran all the previous small forces



packets through the system and delivered them to the file server. So the design of this burn used the flawed data.

The Mars Climate Orbiter spacecraft successfully performed TCM 3 on July 27, 1999 which was 59 days from MOI. During TCM 3 the spacecraft performed a measured 3.298 m/s burn lasting 36.6 sec. against a prediction of 37.4 sec. The performance requirement on magnitude for this TCM was  $\pm 0.76$  m/s. The target delta V was 3.33 m/s. (In retrospect, this would be a larger than expected TCM for this point in the trajectory, another tell-tale sign that something was wrong.) All execution errors were well within expectations.

However, following the slew to the earth-point communications attitude, the spacecraft did experience a safe mode entry while commanding the solar array two-axis gimbal to articulate the array out of its passive restraint. In addition, the quick look data following the burn, using several hours of tracking was much worse than results from the previous two TCM's - but was attributed to too short a time of tracking and was expected to improve. The data indicated the actual trajectory was well outside the 1 sigma target ellipse, and in fact, was "below" the Mars horizon. So even at this early time before MOI, the orbit determination (OD) process was indicating solutions biased toward a low altitude at closest approach.

Unfortunately, the anomaly that resulted in the safe mode entry completely distracted the small MCO flight team, including scarce ACS personnel resources, and because of the flurry of activity associated with the safe mode entry and the potential threat to MOI and Aerobraking, the Flight Team and Navigation Team failed to ascertain the importance of this "symptom". For the next 6 weeks the spacecraft team was engaged in troubleshooting the anomaly and replanning MOI and Aerobraking in case the spacecraft were to suffer again the same anomaly. No less than 3 flight troubleshooting exercises were performed, preceded by heavy test laboratory preparation and data review. The final passive restraint exercise was successfully executed on Friday, September 3 as planned. Using this data the team was able to map a trajectory into and out of the restraint to hopefully avoid the anomalous condition, and was now ready for TCM 4 and MOI.

#### ***Trajectory Correction Maneuver 4 (MOI – 8 days)***

TCM 4 was successfully completed on September 15, 1999. A 1.3742 m/s delta V was recorded by the spacecraft's IMU against a target of 1.3711 m/s. All spacecraft indications were nominal. Overall pointing error (RSS of x and y) was 27.2 mrad, well within requirements.

The solar array articulation was nominal. The revised restrain/unrestrain trajectory was used, along with the new gain values that were demonstrated in the recent flight verifications. The team felt they were a "go" for MOI and Aerobraking. (Mitigation strategies were still in place onboard the spacecraft, to prevent mission loss in case the array got stuck in, or near the passive restraint.)

But initial Navigation tracking (based on only 2 hours) indicated an underburn, showing only 1.33 m/s. This initial trajectory estimate showed that MCO may be out of its 3 sigma burn target ellipse. This would correspond to a post-MOI periapsis (P2) altitude of 137 km periapsis instead of the target of 210 km. MOI periapsis altitude (P1) was 16 km higher. However, over the next 24 hours, the NAV team reported that the solution showed that the periapsis altitude was 172 km. Daily telecons continued between the Navigation team and the Spacecraft team as they monitored the situation. It was agreed that if TCM5 was necessary, the decision to execute it would be made on Sunday, September 20 (1430 MDT). But to make the decision to execute, required that the TCM5 products be fully tested and reviewed. So the team decided to design the TCM5 using the same burn attitude as did TCM4. The magnitude was changed to 0.23 m/s (corresponding to about a 30-50 km increase in periapsis altitude), and the epoch updated for a Monday, September 20 execution. All products were fully tested in the STL on Friday night, with the full data review to follow on Saturday.

The Navigation and Flight Team continued to monitor the predicted periapsis altitude for MOI resulting from TCM4. Because of the observation geometry from Earth to the spacecraft's velocity vector it was taking longer to confirm the resulting trajectory and make sure it was high enough to insure that periapsis would be outside the Martian atmosphere.

### ***Trajectory Correction Maneuver 5 and Post-MOI Options Developed and Tested***

#### **MOI - 6 days: Friday, September 17, 1999**

It was reported that tracking solutions were beginning to cluster, the post-MOI P2 mean had climbed to 164 km with the 3 sigma low at about 140. Late in the day as plans were firmed up for how to test TCM5 and the resulting MOI which follows, the Flight Team began to raise the possibility of reducing risk to MOI by not performing TCM5, but instead preparing plans for post-MOI that would alleviate MCO from going into Safe mode during its first post-MOI periapsis passage (referred to as P2 since P1 is MOI) if it were to encounter aerodynamic torques. A Safe Mode entry could occur as these torques could saturate the reaction wheels. These discussions were held because the data indicated that a TCM5 was not strictly required. (Obviously, in hindsight the team was making decisions with bad data.) But two options were created that could be individually selected in part or whole:

- a. Develop on-board sequence that manages the actuator selection from Wheels to Thrusters during the post-MOI periapsis passages; and
- b. Develop a 40 km raise orbit trim maneuver (OTM) for first apoapsis (A1) execution, following MOI.

Finally, a decision was made to hold a Saturday morning special telecon with management and the MCO standing review board to outline the TCM 5 risks and options. It was expected that 24 more hours of Nav tracking would give more confidence in the decision to be made the following morning.

#### **MOI - 5 days: Saturday, September 18, 1999**

The latest solutions were reported as 173 +/- 18 km (P1, 3 sigma). TCM5 was outlined and discussed but the decision was to proceed with options for post-MOI as described above (both options a & b). The team was to proceed with TCM5 until results from the 12 Noon Navigation team meeting could be assessed. Following the Noon meeting, at 2:30 PM the solutions were reported from range measurements to indicate a mean of 161 km and a tight variance of no lower than 150 km (3 sigma low), but solutions using doppler data were reported to be all over the map. The worst single solution for the doppler data was 140 km and was felt by the Flight Team to be survivable with margin. (The data did not indicate as of yet the true altitude of periapsis, but the data was indicative of a problem of some kind.) TCM5 was then called off and the Flight Team was refocused on building and testing the post-MOI options a and b discussed in the telecon.

#### **MOI -2 days: Tuesday, September 21, 1999**

The decision criteria for using the post-MOI options was presented and approved at the 9AM Mission Design Meeting. At that time it was agreed that MCO should perform the OTM (option b) for sure at the first Apoapsis (A1) so that the Flight Team would not have to execute the actuator management sequence (option a), although both would be on the shelf. On this date the best solutions were indicated to be 161 +/- 11 KM. By the time that Thursday, September 23 arrived, the predictions were still about 150KM.

### ***Mars Orbit Injection: September 23, 1999***

The final flight products for the Mars Climate Orbiter were successfully uplinked on Friday, September 17 and the injection sequence was initiated. The sequence remained in a holding pattern (as planned) until 17:00:44 UTC (ERT) on 9/22/99 when, as planned, it issued a series of commands to disable most of the spacecraft's fault protection. The remainder of the countdown to 9/23/99 went smoothly with zero alarms.

All telemetry and ground data indicate that the on board Master Sequence and MOI Block were executing properly at Mars occultation. As expected, the spacecraft switched off telemetry

modulation and swapped to the MGA with carrier-only shortly after the Solar Array had reached its standoff position. At the time of telemetry stop, all subsystems were nominal and there were zero alarms.

During the countdown to MOI ignition, the Flight Team received word from the JPL that navigation solutions were now showing a post-MOI periapsis of only 110 km against the prediction earlier that day of 150 km. The Flight Team immediately began altering the existing post-MOI apoapsis Orbital Trim Maneuver (OTM-1) to double the firing time so an orbit raise of the post-MOI periapsis of +80 km could be achieved. (This burn would be loaded following MOI and executed at the first apoapsis.)

While the DSN was reacquiring the carrier following the planned switch of antennas, the spacecraft was finishing the stowing of the solar array and preparing to slew to its burn attitude. Once the DSN had acquired the carrier, the AGC strength of -146 to -152 dB indicated that the spacecraft was still in its pre-MOI attitude, as it should be. Right on time, at 08:49:46 UTC (ERT), the slew began to the burn attitude and the Flight Team observed the AGC-level decrease, as predicted, to -168 to -174 dB.

At 08:55:48 UTC (ERT) the ME fuel and oxidizer leg pyros were successfully fired and filled the propellant lines up to the Main Engine Valves. At 110 sec before engine ignition the pressurization pyros were apparently successfully fired and pressurized the Fuel and Oxidizer tanks. At 09:00:46 UTC (ERT) the Main Engine was ignited on time and JPL reported that the doppler residual indicated the burn was taking place. All indications were that the spacecraft was in control and holding the burn attitude while the main engine was firing.

At 09:05:02 UTC (ERT), 39 seconds earlier than predicted, the spacecraft carrier dropped out completely as apparently Mars occultation had begun. Occultation was expected to end at 09:26:25 (using the actual occultation time) as reported by JPL. Unfortunately, the signal never appeared again. While the Flight Team continued to build the post-MOI burn predict during the occultation period, the navigation solutions continued to drop until finally reaching 57 +/- 1 km for MOI (P1) and 40 km for post-MOI periapsis (P2).

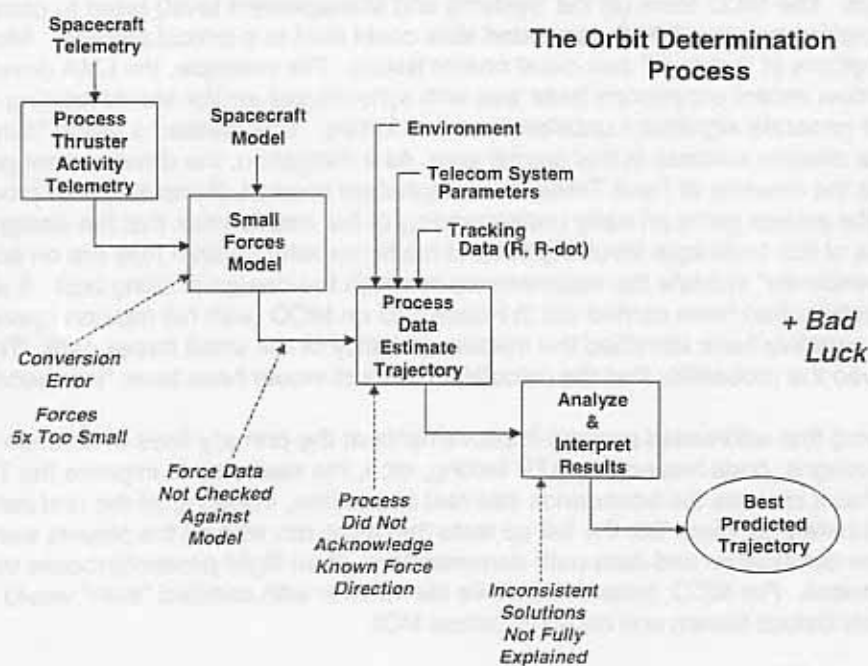
It was now apparent that the navigation predictions prior to approaching Mars apparently had an error of about 100 km at MOI closest-approach from where the spacecraft actually was, at closest-approach. As the spacecraft began to more strongly experience the Martian gravity, the Navigation team was able to calculate more accurately the MOI closest-approach distance. The most confident calculations were the last ones before occultation, resulting in the estimated 57 km altitude.

Thermal subsystem predictions show that the spacecraft would most likely have exceeded critical temperature limits at about 98 km. Attitude control authority would be exceeded at about 85 km altitude. It is believed that the spacecraft was lost as it approached periapsis following occultation. The MCO was approximately half way through the MOI burn when aerodynamic torques and heating caused the loss of control and possible break-up of the vehicle. It seems probable that the solar array broke off first and burned up in the atmosphere with some metallic parts getting to the surface of Mars. If the body of the MCO stayed together, the aerodynamic drag coupled with the partial MOI burn provides just about enough deceleration to capture into Mars orbit, so it is difficult to predict whether the MCO was captured or skipped out of the atmosphere to continue on an interplanetary trajectory. If captured, the body would plunge deep into the atmosphere on the next periapsis pass, eventually breaking up with some small pieces reaching the surface. Another possible outcome is that the aerodynamic effects during the MOI would cause catastrophic rupture of the propellant tanks, creating many small pieces, which again would burn up with some debris reaching the surface.



In summary, it seems probable that some debris did get to the surface of Mars, but it would have been exposed to very high temperatures to destroy any biological organisms. (The sterilization requirement is for surfaces to reach greater than 500 °C for more than 0.5 sec.)

The Flight Team instigated the emergency Loss-of-Signal procedure shortly after occultation was ended. The ACE's were unsuccessful in reacquiring MCO after radiating 40 command files between 04:05:34 MDT on 99-266 and 06:00:00 on 99-267. Twenty-nine of the forty radiations were related to the LOS procedure, and eleven were a last ditch attempt to uplink and execute a large periapsis-raise maneuver before the predicted second periapsis passage, a passage in which the spacecraft would enter and surely not survive (40 km). Various sweep patterns and doppler adjustments were used. Finally, as the predicted time of the second periapse passage approached, the flight team transmitted a large periapsis-raise maneuver sequence "in-the-blind," as it was believed the spacecraft would surely not survive a second periapsis passage due to the low (40 km) altitude being predicted. Search efforts continued into the following day (Friday, Sep. 24). The search for MCO was discontinued at approximately 04:00 UTC on Saturday, Sep. 25.



**Figure 5. Anatomy of MCO's Loss**

### MCO Lessons Learned

The lessons learned from the perspective of the Flight Team fall into two general categories: Spacecraft Generic; and Deep Space Mission-Specific. Figure 5 serves as a roadmap for the critical error that led to catastrophic loss of the mission.

#### Spacecraft Generic Summary

1. The Obvious: do it right the first time
2. Mission Critical Understanding (end to end)/ Identification of Mission Criticality
3. Test-Like-You-Fly (TLYF) Extension Into Mission Operations
4. Unhealthy Flight Team Distractions Due to In-flight Anomalies



### **Deep Space Mission-Specific Summary**

5. Emergency Backup Maneuvers for Target Encounter
6. Independent NAV Data Type

Each are now discussed:

1. The obvious lesson is not to make mistakes in the first place (in this case the units error), but it is difficult to implement an error-free design and development, especially in an FBC environment. Nevertheless, additional training and oversight is necessary for projects like Mars '98 that to meet cost constraints, relied on "one deep" personnel in various areas. The probability of catching errors as they are missed in the first line of defense decreases as it goes undetected to the next levels. TLYF can never be used to obviate us of our first responsibility – to do it right first. Following standard company procedures, this error would not have been made. Interface specification requirements were not met, and went untested.

2. During Phase C/D the development team (involving appropriate membership of Flight Operations) needs to understand all the command and data paths associated with mission success. The MCO team (at the Systems and Management level) failed to correctly understand or recognize how the SPAS-generated data could lead to a critical problem. More often than not, assumptions of "heritage" can cloud crucial issues. For example, the LMA development/ flight team most recent experience base was with symmetrical and/or slowly rotating spacecraft that did not generate significant unbalanced small forces. This created a group "mind set" that worked against mission success in this crucial area. As a mitigation, the development process should include the creation of Fault Trees or an equivalent product. Because in the process of deriving them the project gains an early understanding of the mission risk that the design poses. In fact, the use of this technique involving subject matter experts (even if they are on project) serves to "independently" validate the requirements to which the design is being built. It is believed that if such activity had been carried out in Phase C/D on MCO (with full mission operations support) it would certainly have identified the mission criticality of the small forces data. That would have improved the probability that the calculation outputs would have been "independently" checked.

3. Having first addressed prudent improvements at the primary lines of defense (requirements walkthroughs, code inspection, ATP testing, etc.), the next step is improve the TLYF approach such that it crosses the boundaries into real operations, involving all the real participants. Unfortunately for Mars '98, the full up tests that were run with all the players were more focused on crew certification and data path demonstration, than flight product/process validation and data correctness. For MCO, tests that involve file transfer with certified "truth" would have caught the anomaly before launch and certainly before MOI.

4. The post -TCM 3 safe mode entry on what had been to-date a well behaved spacecraft, certainly contributed to the inability of the Flight Team to recognize the obvious. Combined with a general misunderstanding of how the Navigation process was using SPAS data and sparse personnel in the ACS area not consumed by the other anomaly – this was an overwhelmed team. In addition to increasing subsystem staffing levels, the recommendation is to always include senior systems personnel with extensive flight experience that keep a "sideways glance" (out of the critical loop of the anomaly of the moment) on all data and information on the health of the spacecraft. They need to have a Sherlock Holmes approach and a bulldog's disposition to pursue strange indications while the rest of team is distracted. Similarly, the discipline of documenting all concerns on problem reports is paramount for spacecraft teams in flight operations – to make sure nothing "falls through the cracks". This was not rigorously applied on Mars '98.

5. For missions like MCO which have encounters with planetary bodies, either for flybys, landing, or orbiting, the Flight Team should employ an onboard emergency suite of maneuvers that can be selected with minimum uplink, at nearly any time prior to encounter – even two hours out. In fact,

as was the case for MPL following the MCO loss, the maneuvers should be designed to allow the Flight Team the luxury of trajectory knowledge “truth” afforded by the gravitational pull of the encounter body (assuming it is massive enough to give enough warning). Had we developed that capability for MCO, we might have been able to execute a burn prior to MOI in the last minutes that would have saved the mission. (It should be pointed out, however, that for MCO the as-designed TCM5 burn had insufficient magnitude to save the spacecraft, and the burn vector would not have been optimum. Some have pointed to the calling off of TCM5 as the last chance to save the mission. But the data available then said that one only needed a 30+ km raise to get back to 180-210 KM, when the truth was that we needed a > 40 km guaranteed periapsis raise to even reach predicted spacecraft survivability limits.)

6. An obvious improvement for future spacecraft with planetary body encounters is to employ independent navigation data types – such as optical or other radiometric types that connect the spacecraft state with the target body. This would provide independent solutions for orbit prediction.

## PART II: THE MARS POLAR LANDER

### Background

On December 3, 1999 at 1:20 p.m. MST Mars Polar Lander (MPL), Figure 6, sent its last transmission to Earth and turned away to orient for entry into the Martian atmosphere. That was the last confirmed signal from the spacecraft. After several months of attempts to contact the Lander the mission was declared a loss. What happened to the spacecraft? There is no certain cause of the loss of the vehicle and no hint of any anomalies prior to the last transmission. Post-mission failure boards identified six plausible failure modes including landing in hazardous terrain consisting of a steep slope near the predicted touchdown site (see Table 2). Although it will probably never be known absolutely what caused the failure of the only soft-lander since the Viking missions of the late 1970's there did emerge a most-probable cause of the failure.

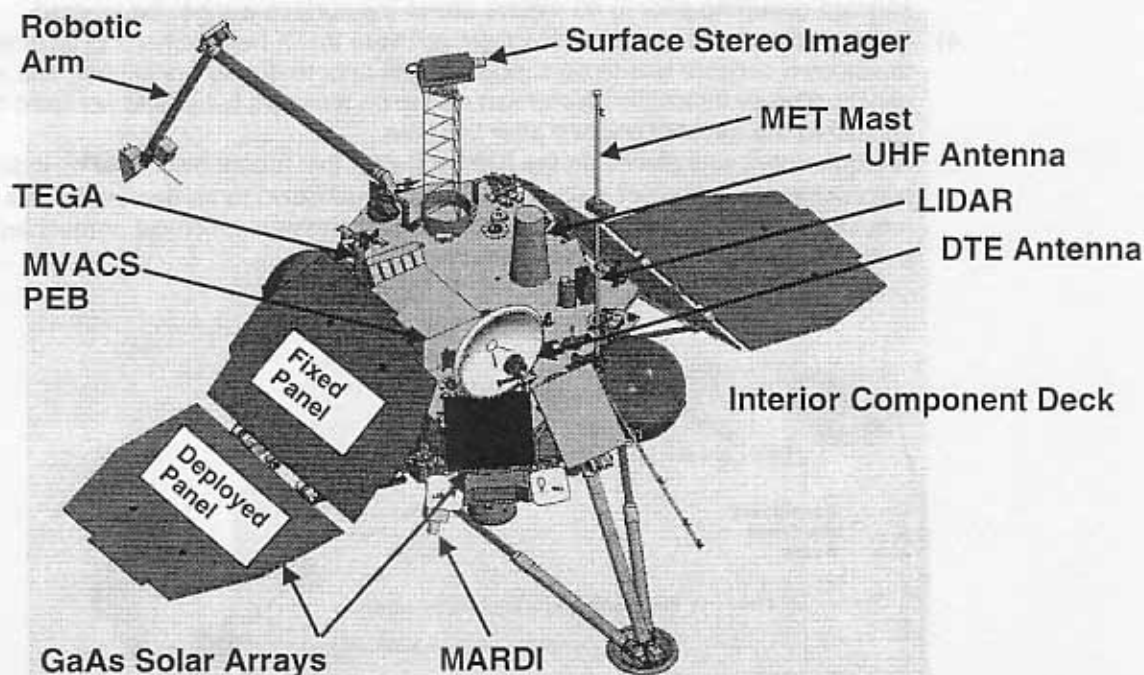
Landing Site Not Survivable
Loss of Control Due to Dynamic Effects In Entry, Descent, and Landing
Loss of Control Due to Propellant Migration and Resulting Center-Of-Mass Offset
Parachute Draped Over Lander After Touchdown
Heatshield Failure Due to Micrometeoroid Impact During Cruise
Lander Engines Prematurely Shut Down Due to Touchdown Sensor Signal

**Table 2: List of Most Plausible Failures [3]**

The loss of the Mars Climate Orbiter just two and a half months prior to MPL landing caused an in-depth review of MPL to ascertain if it was ready for entry, descent, and landing (EDL). A review board chaired by Jet Propulsion Laboratory with the participation of Lockheed Martin Astronautics (LMA), other NASA participants and consultants did identify an issue with the temperature of the Lander descent engines (which was resolved prior to entry) but otherwise gave the Lander a clean bill-of-health to proceed. A detailed fault tree was produced during this pre-landing period that included some consideration of what was to become the most probable cause of failure but that effort did not result in discovery of the problem. Many dollars were spent after the landing event with three Review Boards investigating the cause of the failure. However, the weakness inside MPL was not so obvious that it could be found by external reviews.

On January 18, 2000, six weeks after we last heard from MPL, an LMA engineer running a test sequence on the Mars 2001 Lander software accidentally stimulated a logic error in the software used to shut off the descent engines on touchdown. That same software was used on MPL and the discovery led LMA engineers to the most probable cause of the MPL failure: premature shutdown of the descent engines 40 meters above the surface of Mars. How had this logic error escaped detection over a period of two years of development, a year of spacecraft system testing, and the intensive pre - and post - landing review by hundreds of engineers? There is no single explanation, but to infer that the Faster-Better-Cheaper (FBC) project management approach was the cause, is too simplistic.

There is no question that the flight software logic error was the result of a human error. A competent person made a mistake and all the check and balance processes failed to detect the error. Multiple system level tests confirmed proper operation of the touchdown sensor logic (without the presence of transients) and those tests gave the team the confidence to launch. Over the course of the failure investigation two main camps of thought developed as to the reason that the logic error went undetected. One camp pointed to events during definition of requirements and execution of the design phase as the root-cause. The second camp focused on the system test program as the source of the systemic failure to detect the logic error. Each of those perspectives will be discussed in the following paragraphs.



**Figure 6. Mars Polar Lander**

#### **Description of the Applicable Mission Events and Design Elements**

During the six minutes of the Entry, Descent, and Landing phase of the mission more than 30 mechanical events had to occur without failure. Figure 7 shows the event timeline. Three deceleration periods were to result in a soft landing near Mars South Pole. During Hypersonic Entry, the aeroshell protected the Lander vehicle from high temperatures created during direct, high speed, entry into the atmosphere. Secondly, a parachute was deployed and the heatshield was jettisoned. And lastly, twelve hydrazine fueled descent engines were fired during the last 1200 meters of free-flight to bring the Lander to a final relative velocity of 1.4 meters/second at touchdown.

The engines were required to be shutdown within 50 milliseconds of the first indication of contact with the surface in order to land without tipping over in the worst-case dynamics and slope conditions. A Hall-effect transducer was imbedded in the main attach point of each of the three landing legs to act as a touchdown (TD) sensor. Touchdown of a given leg would create a force and thus displace the leg until a permanent magnet in the leg strut created a signal out of the touchdown sensor. On-board flight software (FSW) sampled the three touchdown sensors at a 100 Hz rate. The first leg of the three to indicate touchdown caused the flight software to close all 12 descent engine valves within 25 milliseconds after the indication of touchdown.

Several design and software requirements were imposed on the spacecraft because the consequence of an erroneous indication of touchdown was mission catastrophic:

- 1) A requirement was placed on the landing legs that the touchdown sensors could not be actuated by the dynamic environment existing during terminal descent. Consequently, springs sized at 222 N were placed in each leg to resist the dynamic accelerations expected when the descent engines were pulsing,
- 2) The high-rate software process to read the touchdown sensors was started prior to entry to avoid a sudden change in microprocessor utilization during the critical EDL events,



- 3) A requirement was placed on the flight software that signals from the touchdown sensors occurring prior to 40 meters above the surface were to be ignored,
- 4) A requirement was placed on the flight software that a health check of all three touchdown sensors was to be conducted just prior to 40 meters altitude and any sensor already indicating touchdown was to be declared failed and not used to shutdown the descent engines after this time.
- 5) A requirement was placed on the flight software that touchdown must be indicated in two consecutive reads of a single sensor for touchdown to be declared. This requirement was promulgated in order to reject transient electrical or mechanical events from the touchdown determination.

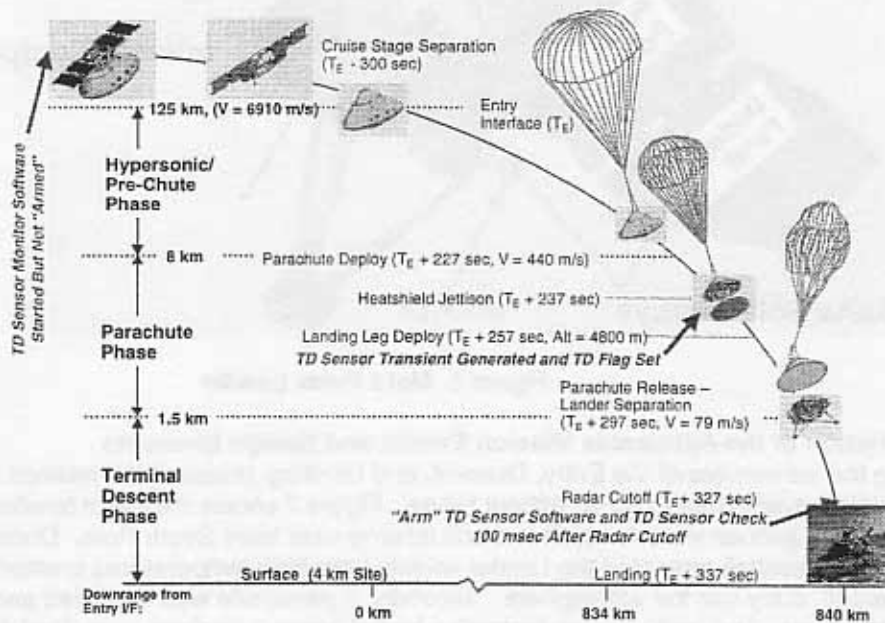


Figure 7. MPL Entry Descent and Landing Events

#### Description of the "Most Probable" In-flight Failure Scenario

Once the heatshield was jettisoned, the landing legs were deployed from their stowed position. A powerful coil spring propelled each leg outward until mechanisms in the main leg strut and side struts locked the leg into the extended position. During this event it was later demonstrated that, for a large majority of the test cases, the rebound of the legs after lock-up was sufficient to cause a 5 to 33 millisecond transient output signal from the touchdown sensors in the legs. Transients greater than 11 milliseconds would cause a false touchdown indication. During the leg deployment the flight software sensed and stored a touchdown sensor transient signal as the de-facto touchdown event. After leg deployment MPL likely continued to progress through the subsequent programmed events of Parachute / Backshell separation and initiation of powered descent towards the surface of Mars.

At 40 meters above the surface the landing radar had reached the design limit of altitude resolution and was turned off. Immediately thereafter the health check of the touchdown sensors was automatically performed and all sensors were most likely indicating no-touchdown. After the successful health check the flight software proceeded to check the status of the higher level touchdown flag. Unfortunately, a touchdown flag probably had been set during the earlier leg

deploy event and all descent engines were immediately stopped. The resulting free-fall of the Lander to the surface would have destroyed the vehicle.

### Factors Associated With the Touchdown Sensor Logic Error

There have been assertions by outside observers that shortcuts were made in the definition, design, and test phases of MPL. From the participant's viewpoint, all customary and prudent steps were executed in the development process. System and subsystem requirements were defined and documented, software code requirement and design tabletop reviews were held. Software unit testing was conducted. Subsystem mechanisms tests were performed to qualify touchdown sensor and leg hardware. Multiple vehicle system level tests were performed using flight and flight-like touchdown sensors in end-to-end "test like you fly" performance tests of the logic.

Over the development timeframe of the MPL a series of unrelated events conspired to prevent detection of the software logic error. Table 3 lists key events in the history of the touchdown sensor code and testing. The contributing factors that led to the exposure to human error can be stated as:

- 1) Ambiguous requirement in the Software Requirement Specification,
  - 2) Missing allocation of "Do not use TD Sensor Data" requirement to the Systems Level Requirement Specification,
  - 3) No written definition of potential TD sensor transients present at the FSW interface,
  - 4) Unrelated engineering error in the TD sensor wiring instructions during ground test.
- These contributing factors are not listed in any order of importance and any one addressed separately might have changed the course of history.

5/17/96	Brainstorm Meeting for Detail Design Requirements for Hall-Effect TD Sensors
8/6/96	Lander Mechanisms Review with Customer, No Issues on TD Sensor
8/1/96	Table Top Review of FSW Structures & Mechanisms Code Requirements
9/18/96	TD Sensor Design and Implementation Requirements approved at MPL System Design Meeting
12/4/96	Delta Table-Top Review of FSW Structures & Mechanisms Code Requirements
1/24/97	Design Walk-Through of FSW Structures & Mechanisms Code
6/16/97	Engineering Development Unit Leg Deploy Test Indicating TD Sensor Signal During Deployment. No Surprise to Subsystem Test Staff
6/30/97	Code Walk-Through of FSW Structures & Mech Code
7/10/97	Leg Deployment Verification Plan Table-Top Meeting
11/17/97	MPL Formal Verification Review with JPL
4/16/98	EDL/MOI Verification Review with JPL
6/4/98	System Test Leg Deploy Test (TD Sensors Miswired) With FSW TD Sensor Code Operating
6/4/98 - 6/9/98	Flight TD Sensor Wiring Error Corrected And Tested By Manual Leg Manipulation
12/3/99	MPL Landing
1/18/00	MSP '01 Lander Test Laboratory Event Stimulates FSW TD Monitor Code Error
2/23-2/24/00	Ground Leg Deploy of MSP '01 Flight Legs Show TD Sensor Signal Consistently Present

**Table 3. Key Events in the Development of the Touchdown Sensor Code Issue**

### Ambiguous Software Requirement

The engineering change that implemented the Hall Effect TD sensor also placed requirements on the flight software. In that change, a requirement to "not use the TD sensor data until 40 meters above the surface" was written. That requirement was weak in that it stated the requirement in the negative making it difficult to verify. More importantly, when that requirement was flowed

down into the structures and mechanisms software module it was not mapped to a single equivalent requirement but into several alternative requirements which did not communicate the intent of the original. Because the software engineer who wrote the TD sensor code requirements also wrote the TD sensor code the intent was preserved in human memory. Unfortunately, a second software engineer performed the unit testing and there was no clear software module requirement to "not use the TD sensor data" with which to drive a verification test of that function and none was performed.

TD sensor software requirements and code reviews were held with Systems Engineering in attendance. One of the impacts of FBC occurred when the systems engineer who authored the TD sensor engineering change notice could not be present during those reviews due to other priority demands of the Project. Perhaps the problems with requirements flow-down could have been identified during the development of the code if the most knowledgeable system engineer would have been present.

#### **Missing Allocation of a Mission Critical Requirement to Systems Level Verification**

It was the policy of the MSP '98 systems engineering to capture, at the systems level, requirements deemed to be "Mission Critical" even though they may affect only a single subsystem. Verification of all systems level requirements was allocated to analysis, inspection, or test. Subsystems were responsible for the definition and verification of their requirements. In this case the engineering change which defined the "do not use TD sensor data" requirement did so at the subsystem level and did not create a systems level requirement. If a systems level requirement would have been created it would have been allocated a verification methodology (perhaps a leg deployment test on the flight vehicle) and tracked to closure instead of relying only on a subsystem test process.

#### **No Written Definition of Touchdown Sensor Transients**

Transient signals on critical sensing lines have created problems in past space missions. The MPL design team was very concerned about transients on the touchdown sensor lines created by dynamic environments causing displacement of the leg or electrical transients during the pyrotechnic events and engine firings of EDL. To address those concerns the original "do not use TD sensor data" requirement was written to avoid any unforeseen TD sensor transient from causing engine shutdown prior to the last possible moment (40 meters above the surface). The requirement to ignore the TD sensors until just before landing was so well known across the project that it was taken for granted by all parties. This led to group-think across various subsystems, and during systems testing, that there was no longer a need for concern about transient signals. After landing day it was discovered that TD sensor transients had been observed during leg development testing years earlier but not flagged because transients had been expected and handled with the imposed requirement.

An effort to define expected transient signals on critical sensor lines could have resulted in a requirement to characterize potential transients and subsequently use that characterization to create an input condition for a software unit test on the TD sensor logic to insure rejection of the transient. The additional requirement on flight software to receive the same touchdown indication on two consecutive reads was a form of transient rejection but was created with the thought that it would be used to detect a hard-failure of a sensor which occurred sometime prior to landing. If the requirement would have been for three consecutive readings before sensor data was considered valid then the transient created by leg deployment would have been successfully filtered out. However, the need to terminate thrust from the descent engines within 50 milliseconds of touchdown forced a minimization of the number of consecutive samples required to declare TD sensor output as valid.

## Unrelated Engineering Error in the TD Sensor Wiring Instructions

The TD sensors had wire pig-tails extending out of the sensor that were to be wired to the main spacecraft harness. The connections were made for the first time based on engineering instructions that were erroneous. If the wiring had been correct, and if the leg deployments on the test floor created sufficient transients on the TD sensor lines, then the system level leg deployment test could have identified the logic error. As it was, the system level leg deployment test did identify the wiring error (see next section). Prior tests of the TD sensor logic utilized a flight-spare TD sensor in a special fixture which was manipulated manually by a technician to simulate touchdown. In the change-over from the TD sensor simulator to the flight units the wiring error was introduced into the test flow.

Several items made the check-out of the TD sensor wiring difficult to perform. The magnet used to stimulate the Hall Effect transducer during flight was physically separated from the transducer when the legs were in the stowed position. Consequently an external test magnet had to be used to induce a change in the TD sensor signal. In addition, the severe restrictions on spacecraft launch mass resulted in the deletion of connectors between TD sensors and spacecraft harness which contributed to the wiring checkout difficulty. The fact that an error was made in the TD sensor wiring engineering was driven more by the factors just discussed than any problem with the process that generated the wiring instructions. The spacecraft wiring diagrams were produced through a customary process of design reviews with each subsystem, automated harness checkout electronics, and configuration controlled engineering.

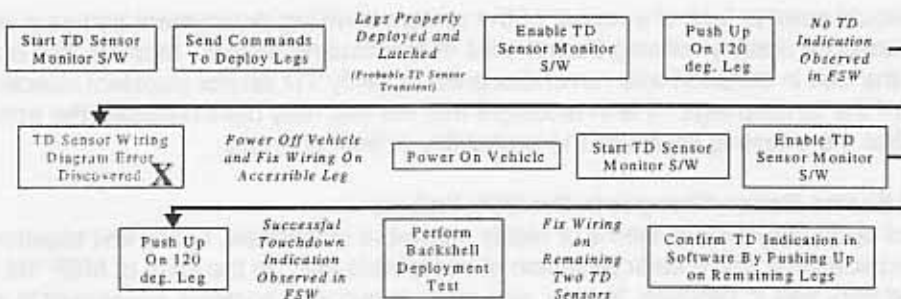


Figure 8. Leg Deployment Test Flow on the Flight Vehicle

## Leg Deployment Test on the Flight Vehicle

On June 4, 1998 a test of the landing leg deployment and TD sensor functionality was conducted on the flight vehicle (Figure 8). The objectives of the test were to use the flight leg deployment commands on the flight hardware to verify all three legs deployed correctly and that after deployment the flight software correctly sensed touchdown when it was manually induced. The vehicle was mounted on three pedestals. The touchdown sensor flight software was started and then the leg deployment commands were issued by the ground console in the order and the spacing used in-flight. The legs successfully deployed. After deployment a technician pushed upwards on one footpad to actuate the touchdown sensor but there was no indication in flight telemetry that touchdown had occurred. It was quickly determined that the wiring instructions for all three sensors were incorrect. The wiring was corrected for the leg that was accessible and a touchdown indication correctly observed in flight telemetry when the footpad was manually displaced. The wiring of the other two TD sensors was corrected and tested in the following days. The test was declared a success.



This test might have detected the TD sensor logic flaw if not for the sensor wiring problem. It is not certain though that the specific physics of the test (i.e. 1 g and physical mounting) would have resulted in rebound of the landing legs and enough of a TD sensor transient to trigger touchdown flag. At the time of the test there was no discussion of repeating the test as it had accomplished the test objectives. The cause of the TD sensor anomaly during the test was obvious, it was documented, fixed, and verified. If we would have recognized that there was a dynamic effect occurring with the TD sensors during leg deployment then the test results would have been evaluated for a potential repeat. Perhaps if TD sensor transients were better defined (item 3) the team might have used this system level test to verify the software logic. A repeat of the leg deployment test would have resulted in disassembly of the flight vehicle and a potential recycle through some system level environmental testing to recreate the same series of events at the time of the original leg deployment test.

On MPL the "Test Like You Fly" criteria was applied early and often by the members of the team. In the morning status meetings and test procedure reviews "Test Like You Fly" was embraced and voiced by the staff. In association with "Test Like You Fly", Faster-Better-Cheaper dictates that the technical team makes its best informed decision of test anomalies and their resolution and make a case for changes in the test flow if issues were unresolved. Some critics have proposed that all tests be repeated in their entirety if there is any deviation to expected results. To do so fails to recognize any reality of cost, schedule, or even additional risk to the hardware. The test team on the floor has the responsibility to determine the course of action after an anomaly to insure that all test objectives are achieved.

Those who would point to lack of a repeat of the system level leg deployment test as a weakness will find that concern notably missing from the list of contributing factors. In short, this is due to the fact that the test in question was never designed to verify TD sensor transient rejection during deployment of the landing legs. It is in hindsight that the test may have detected the error, but it is also true that more testing improves the probability of finding errors.

### **The Role of Faster-Better-Cheaper in the MPL Failure**

FBC is based upon use of small teams of highly motivated individuals, tightly knit together with lots of communications, and a clear definition of acceptable risk. In the case of MSP '98 this model served very well to produce, launch, and operate two very complex spacecraft in record time and budget. After examination of the contributing factors there is no evidence that FBC concepts caused the MPL failure:

- 1) Processes were defined and followed,
- 2) Requirements were written and flowed to lower levels,
- 3) Testing was not sacrificed to save money or time.

With this said, the central difficulty on MPL was to execute the defined steps with the limited human resources available. Necessary and planned testing was performed at all levels to satisfy verification requirements. There was no time or money or staff available to perform unbounded testing (prior to launch) to explore what might happen in highly off-nominal cases – sometimes called "break-it testing". Certainly break-it testing should not proceed at the cost of verification of the nominal design.

The conclusion of the Review Boards was that the Project did not have sufficient resources to achieve success. That conclusion can be supported by this preceding look at the contributing factors to the MPL failure. Among them; the system engineering staff could not cover all the meetings, the time pressures did not allow any uninterrupted downtime for the team members to recognize subtle interactions of the spacecraft systems, and there was absolute dependence on single individuals with no backups.

Targeted increases in staffing for systems engineering and several other selected groups could have mitigated some contributing factors to the MPL failure. Specific tuning of the MPL procedures for requirement definition, especially in the area of specification of transient signals, can also be made to improve the design. For those that went through the MPL development the recommendation was clear- add about 30% more resources (people or time) but don't abandon FBC.

## CONCLUSIONS

The Mars Polar Lander was a complex space vehicle that had to execute an extremely challenging entry, descent, and landing sequence in a poorly characterized surface environment. Although a most probable cause was identified, there were other technical issues that were resolved at the last minute ("diving catches") along with the "worry items" identified by the failure review boards. Perhaps it was not the right candidate on which to apply FBC principles. There were too many technical issues to address in a short period of time. It is a tribute to the MPL team to have come so close with so few known risks.

With regard to MCO, the story is a little different. Although we will never know, it is highly likely that the vehicle would have successfully completed its mission after successful capture in Mars orbit. The multiple errors made on the ground were mistakes in judgment and lack of rigor in the application of standard practices. This certainly has nothing to do with FBC, but the large amount of work imposed on a small flight team was certainly a contributing factor.

There is a fine line between success and failure in these one-of-a-kind missions. For those of us involved with the technical management of the project, a very important lesson learned is to follow your standard practices rigorously and think carefully about every decision and its potential impact on mission success throughout the life cycle of the project. The fixed launch date put tremendous pressure on project personnel, not allowing any "think" time. That both missions ended in failure was a crushing blow to the hundreds of dedicated personnel who expended years of hard work on the project.

## ACKNOWLEDGEMENT

This work was performed by Lockheed Martin under contract to the Jet Propulsion Laboratory, California Institute of Technology, and by JPL, under contract with the National Aeronautics and Space Administration.

## REFERENCES

1. *Report on the Loss of the Mars Climate Orbiter Mission*, JPL D-18441, November 1999.
2. *Mars Climate Orbiter Mishap Investigation Board, Phase 1 Report*, NASA, November 1999.
3. *Report on the Loss of the Mars Polar Lander and Deep Space 2 Missions*, JPL D-18709, March 2000.
4. *Mars Program Independent Assessment Team Summary Report*, NASA, March 2000.