THE TRAGEDY OF MARS OBSERVER

Glenn E. Cunningham

Former Project Manager
Mars Observer Project
Jet Propulsion Laboratory
California Institute of Technology
Pasadena, California 91109 USA
glenn.e.cunningham@jpl.nasa.gov

Abstract: The Mars Observer project was conceived by the National Aeronautics and Space Administration in the early 1980's as the first of a series of missions that would utilize commercially available earth orbital spacecraft adapted for deep space use. The spacecraft failed catastrophically on August 22, 1993, three days before reaching Mars. Subsequent failure investigations suggested a number of programmatic and technical flaws that may, or may not have contributed to the failure. NASA developed an action plan that called for significant programmatic and technical process changes to current and future projects to avoid additional tragedies like Mars Observer. This paper addresses the potential programmatic and technical flaws in the project, the lessons learned, and the changes that NASA applied to implement the lessons learned.

Keywords: Interplanetary spacecraft, Satellites, Space Vehicles, Aerospace, Failure, Management, Projects

1. MISSION OVERVIEW

The Mars Observer project was developed by the National Aeronautics and Space Administration and the Jet Propulsion Laboratory in a response to the call of the planetary science community to mount a series of relatively low cost missions with very focused objectives to a number of specific solar system targets. Mars was chosen in the early 1980's as the target of the first mission which was called Mars Observer. The specific objectives were to study Mars' atmosphere and surface over the duration of a full Martian year. The spacecraft carried seven instruments to support these studies, as well as a radio relay system (the Mars Balloon Relay) to return data from Russian landers on the surface of Mars. The original name of the mission was the Mars Geoscience Climatology Orbiter to emphasize the scientific goals of geology, geophysics and climatology.

The spacecraft was launched with a Titan III/Transfer Orbit Stage vehicle from Cape Canaveral, Florida, on September 25, 1992. Initially, the spacecraft was to have been launched by the Space Shuttle in 1990, but that plan was scraped as a result of the Challenge disaster.

After a 10-month cruise to Mars, the spacecraft would have been captured into an elliptical Mars orbit with the assistance of two on-board 400 NT rocket engines. Following several additional orbital correction maneuvers, a near circular, frozen, sun synchronous, polar orbit of 2 hours period would be established from which mapping observations would be conducted for one Martian year (two Earth years). Science instruments were body fixed to the spacecraft and pointed at the nadir. Data was to be recorded continuously from the instruments and played back to Earth once each day through a 34 meter tracking station of NASA's Deep Space Network. Small periodic maneuvers would be required to maintain the orbit parameters. Orbital altitude was to be about 375 km.

2. PROGRAMMATIC BACKGROUND

A number of basic assumptions characterized the technical and programmatic development approach of the project. The science instruments were to have been simple and inherited from previous missions; the science investigators were to have been experienced; the spacecraft was to have been an earth orbital craft taken off a current production line with simple modifications; there would be maximum use of industrial contractor inheritance such as hardware, personnel, procedures and product assurance; the spacecraft selection would be made before the science instrument selection to bound and define their interfaces; and there would be continuing stable funding provided in the national budget for the Observer Program.

However, every one of these basic assumptions was violated sometime during the project life cycle. The science payload was augmented with an imaging system after the initial payload selection which used up all of the spacecraft's resource margins; there were no high heritage science instruments available and the quality standards for the chosen instruments was raised; there were several first time science investigators selected; the design of the commercial production line spacecraft had to be modified to support the more complex payload and to improve its reliability, thus violating the inheritance; the science instruments were selected before the spacecraft; Mars Observer became the only Observer mission; and the funding was not stable and was reduced significantly following the Challenger disaster

The project start was at the beginning of fiscal year 1985 (October 1984). The spacecraft contractor selection was delayed by nearly a year as the result of a selection process protest. The launch was slipped two years in the summer of 1987 as a result of the Challenger disaster. The decision to use the Titan launch vehicle was made in the fall of 1988 after maintaining dual (Titan and Shuttle) launch vehicle compatibility for over a year.

Two additional changes were made in the science payload. A mapping spectrometer was removed for programmatic reasons, and a laser altimeter was substituted for the original, and more complex, radar altimeter.

There was a complex management structure required to implement the project. JPL managed the project for NASA, and was responsible for mission design, acquisition of the science instruments, and for direction of flight operations. The launch services were managed through three other NASA centers. The spacecraft was procured by JPL on a fixed price contract, with on-orbit award fee provisions, from RCA Astro Space (which was subsequently purchased by General Electric and then Martin Marietta).

3. SPACECRAFT DESCRIPTION

The Mars observer spacecraft was based on the electrical architecture of the RCA-Astro built Defense Meteorological Satellite Program spacecraft, the mechanical structure of the RCA Satcom bus, and the propulsion of the A2100 orbital positioning stage. The spacecraft was built to NASA class A standards. It was not to have single point failure locations except as specifically approved due to their inherently low risk (most mechanical items, antennas, propulsion system plumbing). The craft's main body was shaped like a box (1.1 x 2.2 x 1.6 meters). With its fuel, the spacecraft and its science instrument payload weighed 2.5 kilograms at launch. The spacecraft was built for a three year lifetime and was equipped with one large solar array, consisting of six (183 x 219 x 9 centimeter) solar panels, for electrical power production.

At launch, the spacecraft's main communications antenna, two instrument booms and solar array were folded close the bus structure. During the Earth to Mars cruise phase of the mission the instrument booms were partially extended, and part of the solar arrays were opened. After the spacecraft was in Mars orbit, the solar arrays would have been fully opened, and the instrument booms would have been fully extended. The main 1.5 meter communications antenna would have been raised on its 5.3 meter boom and automatically tracked the Earth. The solar arrays would have automatically tracked the sun. The spacecraft would be operated semi-autonomously by an on-board computer which had a hot backup. Communications were at X-band for both up and down links. Three tape recorders stored science and engineering data during un-tracked periods,

The propulsion system was required to provide velocity changes for the Earth to Mars trajectory and Mars orbital correction maneuvers, for Mars orbit insertion, and for unloading momentum in reaction wheels that were used for attitude control. It was really two systems - a bipropellant system for the large velocity maneuvers with fuel and oxidizer storage in two large tanks in the central cylinder of the craft, and hydrazine stored in two smaller tanks for the redundant lower force thrusters. The bipropellant system was operated in a blow down mode for the Earth to Mars portion of the mission to remove any concern for pressure regulator leakage.

4. IN-FLIGHT EXPERIENCES

During the cruise portion of the Mars Observer mission, the spacecraft operated well. Flight operations were plagued for a time by a software error in a routine that processed attitude information from the reference stars which caused unexpected loss of inertial references. "The spacecraft conducted an successful experiment in Ka-band communications, and participated in a search for gravity waves. The science payload was checked out and some science instrument calibration activities were conducted. One image of Mars was taken about 30 days away from the planet

5. THE FAILURE

On August 22, 1993, at 00:54 UTC, no downlink was received from following an planned power off-period of the spacecraft's transmitter during which the spacecraft's bi-propellant system was being pressurized. No communications have ever been established with the spacecraft since. The spacecraft was performing normally before the transmitter was turned off.

As a development cost savings, the traveling wave tube amplifiers in the spacecraft's transmitter Were not qualified to be operating with the environmental shock imparted by the pyrotechnic operated valves in the pressurant system. Thus, the on-board programmed sequence to open the pressurant valves first turned off the amplifiers, fired the primary valve and its backup valve, and then would have turned the transmitter back on. This sequence was in the primary computer and in its hot backup computer.

The pressurization event was to have been performed early in the mission (about 30 days after launch) in the original design, but information provided about six months before launch indicated a potential for the pressure regulator to leak and over pressurized the tanks when they were full. The decision was made to avoid this potential problem by using the initial pressure in the tanks to blow the fuel and oxidizer out (blow-down mode) for the first three uses of the system before the large Mars orbit insertion maneuver required additional pressurant to move the large amount of propellants needed. Thus, the pressurization event was replanned to occur just three days before the Mars orbit insertion.

The flight operations team continued to systematically execute corrective and diagnostic commanding sequences to reestablish communications. All attempts were unsuccessful. Since the Mars orbit insertion sequence was preprogrammed and was active in the spacecraft's computers, there was hope that the spacecraft, without its transmitter on, would successfully go into orbit. An attempt was made by radio astronomy telescopes to hear the low power beacon from the on-board Mars Balloon Relay system, but this effort was without success. The Deep Space network continued to track the apparent position of the spacecraft (both at its position in Mars orbit and at its position if it flew by Mars without going into orbit) for three months, also without success.

6. THE FAILURE REVIEW BOARDS

Three failure review boards were established within days of the failure. One was chartered by NASA Headquarters. Another was chartered by JPL. And a third was chartered by the spacecraft's manufacturer, Martin Marietta. A fourth activity at JPL conducted a design validation audit of the spacecraft.

No conclusive cause for the failure was established by any of the three review boards. However, all three arrived at essentially the same set of potential causes. The NASA Board concluded that the spacecraft design was generally sound.

It was further suggested by the NASA Board (Coffey, *et al.*, 1993) that although the result was a very capable spacecraft, the organizational and procedural "system" that developed Mars Observer failed in several areas. In particular, the system failed to react properly to a program that had changed radically from the program that was originally envisioned. Too much reliance was placed on the heritage of spacecraft hardware, software, and procedures, especially since the Mars Observer mission was fundamentally different from the mission of the satellites from which the heritage was derived.

The most probable cause for the failure suggested by the NASA Bard was a breach in the pressurant system caused by a reaction of condensed fuel and oxidizer vapors, where they shouldn't have been, forced together by the pressurant as the tanks were being pressurized. It was postulated that the propellant vapors diffused backwards through a set of check valves and then condensed because the pressurant plumbing was colder than the tanks. The pressurant and propellants were then spewed from the open line, spinning up the spacecraft to a rate that could not have been controlled, corroding electrical lines and connectors, and braking off the spacecraft's booms (including the main communications antenna and, perhaps, the solar stray).

Other causes suggested included an electrical power system failure resulting from a regulated power bus short circuit, a pressure regulator failure resulting in tank over-pressurization and rupture, or the ejection of a NASA Standard initiator at high velocity from a pyrotechnically operated valve that punctured the fuel tank or caused severe damage to some other spacecraft system.

In addition, the JPL Board (Stephenson, *et al.*, 1993) suggested that other credible causes of the failure could be related to the loss of spacecraft computation function in a way that could not have corrected by ground commands, or the loss of both transmitters due to failure of an electronic part.

7. THE PRIMARY LESSONS LEARNED

A number of lessons have been learned by the planetary spacecraft community as a result of the tragedy of the loss of Mars Observer. They span the functions of programmatic management, to spacecraft design, to flight operational procedures:

- Don't use systems in environments for which they have not been previously qualified or tested.
- Provide appropriate isolation between fuel and oxidizer in long term missions.
- Provide for post-assembly cleanliness verification and proper functioning of propellant pressurization system..
- Maintain proper thermal gradients between elements of the propulsion system.
- Maintain attitude control during critical events.
- Provide for a top-down approach to fault protection requirements, implementation and validation.
- Maintain insight into the system operations during critical or first time activities by maintaining downlink telemetry.
- Be vigilant of expendable resources during time of crisis (in the case of Mars Observer, it was battery charge.).
- The discipline and documentation culture associated with, and appropriate for, commercial production line spacecraft is basically incompatible with the discipline and documentation required for a one-of-a-kind spacecraft designed for a complex mission.
- Penetrate the fault tolerant design of control functions to assure that critical redundancy cannot be disabled by a single part failure.
- Assure accurate as-built and as-flown documentation
- Assess programmatic and technical risk constantly during the project's life cycle, especially when conditions and/or assumptions change, and take prompt, appropriate, action.

8. THE NASA ACTION PLAN

Over three hundred individual findings concerning all, programmatic management, technical design and implementation of the Mars Observer spacecraft and project were identified during the failure review process. These findings were cataloged and assessed by the Mars Observer Project Office at JPL and by the Solar System Exploration Division of the Office of Space Science at NASA Headquarters. Together, a set of twelve principal recommendations, grouped as technical, programmatic and strategic, were made to apply the lessons learned from the Mars Observer failure to current and future NASA projects (Kicza, 1994). These actions were assigned to the NASA Chief Engineer, to the sponsoring) program offices at NASA, and to the NASA Office of Safety and Mission Assurance who all took aggressive action in response to the Mars Observer failure to assure their commitment to continuous improvement. They in turn assured that appropriate mechanisms were established and maintained to provide for Agency-wide dissemination of the lessons learned, with a commitment at all levels to implement timely corrective actions in affected areas. The lessons learned are reflected in NASA's Lessons Learned Information System and in the interagency Automated Lessons Learned database, and the summarized findings have been distributed to NASA and the aerospace industry safety, reliability and quality assurance communities.

From a programmatic standpoint, emphasis has been placed on institutionalizing NASA's review process. An agency level Program Management Council has been established with an associated review process that assures project are appropriately structured at initiation; that changes are appropriately reacted to in terms of required modifications to mission scope, schedule, management approach and allocation of resources; and that early and continued emphasis on risk identification, assessment and management are made.

Strategically, future missions will adopt distributed risk strategies with resilience to failure of any single segment during launch, cruise and operations.

8.1 Technical Actions

Spacecraft Heritage. over-reliance or inappropriate reliance on heritage is to be avoid. A NASA policy will address this issue and require inherited designs and procedures to be reviewed with appropriate vigor. It is being implemented by the NASA Chief Engineer and the sponsoring program offices.

Propulsion System Standards and Testing. At issue is the propellant migration process, fuel and oxidizer cleanliness and acceptance test processes. An expert group has been chartered to address these issues under the sponsorship of the NASA Office of Safety and Mission Assurance,

Pyrotechnic Actuated Systems Standards and Testing. The identified issues of pyro initiator and pyro valve thread erosion and pyro shock damage are being addressed by a specially chartered group of experts by the NASA Office of Safety and Mission Assurance.

Telemetry Utilization. Direction has been provided to establish flight rules and attendant procedures for continuous telemetry during critical events, and telemetry utilization and recording for problem resolution by sponsoring program offices.

Software Development Practices. Sponsor program offices are directing current projects to make software investments commensurate with mission costs and complexity and to provide adherence to sound software development practices.

Reliability and Fault Protection. Emphasis on critical evaluation, implementation, validation and risk assessment of single point failure and autonomous fault protection systems is being directed by sponsoring program offices

Project level System Engineering. Project level systems engineering to provide for project level tradeoffs, verification and validation, and identification of corrective actions is being required by sponsoring program offices.

Operations Practices. Emphasis is being placed on establishing spacecraft-savvy operations teams and the establishment of time critical contingency plans through training and the development of operations plans and procedure modifications as directed by the sponsoring program offices.

Manufacturing and inspection. The NASA Office of Safety and Mission Assurance is calling, for contractor audits, internal review of quality plans, and the review of critical design review criteria to assure smooth transition into the manufacturing phase in addressing the issues of as-built documentation, workmanship and quality control of spacecraft.

6'.2 *Programmatic Actions*

Program/Project Manager Development. Assuring training programs, management career paths of increasing responsibility and authority by sponsoring program offices and the Progtan~/Project Management Steering Group will assure qualified personnel to fill program/project management roles.

Acquisition Strategy. Periodic *review* and reassessment of contractual vehicles by sponsoring program offices, along *with* the utilization of performance assessment tools and methodologies will avoid inappropriate contracting strategies,

Lessons Learned. Agency-wide dissemination of lessons learned is being implemented. The **NASA** Office of Safety and Mission Assurance will perform audits to assure conformity to corrective action implementation. Policies, proccdurcs, NASA Management Instructions and NASA Handbooks will updated to reflect the lessons learned

8.3 *Strategic Actions*

Distribution of Risk. A re-evaluation of current missions and strategies \\ras made to confirm appropriate distribution of risk to avoid sole reliance on single elements to fulfill strategic objectives. Sponsoring program offices are to adopt (distributed risk strategies.

9. APPLICATION OF THE MARS OBSERVER LESSONS TO FUTURE MARS MISSIONS

NASA implemented a rapid recovery from the failure of Mars Observer through the establishment of the Mars Surveyor Program with a series of multiple, low cost missions to Mars at each opportunity over the next decade. A prime ingredient, in the formulation of this program and the spacecraft development and flight operations that implement it, is the strict incorporation of the lessons learned from Mars Observer rrnd the directions of the NASA Action Plan as discussed above.

The first of the Surveyor missions is Mars Global Surveyor to be launched in November 1996. ‘l’his spacecraft, while much smaller than the Mars Observer spacecraft, is constructed with the residual electronics from Mars Observer. These electronics have been appropriately retrofitted to eliminate the deficiencies identified by the Mars Observer failure investigations. The propulsion system is new, however, and incorporates all the lessons discussed above. Because of the small size of the spacecraft, dictated by the usc of the Delta II launch vehicle, aerobraking will be used to put the spacecraft in its mapping orbit at Mars. For the same reasons, only part of the Mars Observe] science instrument payload can be accommodated. The two heavier instruments are being assigned to two future launch opportunities in older to strategically distribute the risk of loss of science data. Combinations of orbiters and landers to carry a varied science suite also distribute the risk of mission return across the mission set.

Project level system engineering, formalized risk assessment evaluations that correlate potential risks with financial reserves, cost plus performance award contracting and significant partnering, with the spacecraft industrial contractor are other hallmarks of Mars Global Surveyor that arc direct results of the Mars Observer lessons. These processes are also being carried forward to the future Mars Surveyor missions in the 1998 and 2001 launch opportunities.

With the mandate of a $100M-$120M pcr year cost profile to fund all aspects of the Surveyor missions, a strict cost driven paradigm is being applied. This prevents mission performance from growing at the expense of programmatic risk. Spacecraft at-c being developed as special purpose vehicles, with the attendant specialized care required, rather than as production line items

A common mission operations system is being established to operate all of the Surveyor mission in-flight as well as to provide a common ground data system to also be used for spacecraft system test. A scheme of sharing personnel between development activities, spacecraft test and flight operations will ensure to highest trained individuals are available for critical activities. Procedural development and flight rules will be guided by the Mars Observer lessons and experience.

10. CONCLUSIONS

Although the failure of the Mars Observer spacecraft was a tragic loss for the Mars planetary science community and NASA, it revealed a strategy flaw and a number of design and implementation practices and procedures that, while not necessarily contributing to Mars Observer's failure, needed to be corrected in order that mission risk be decreased.

NASA, JPL and the spacecraft development community have responded vigorously to the re-establishment of the Mars exploration program and are using the lessons discussed herein to avoid another mission tragedy like the failure of Mats Observer.

ACKNOWLEDGEMENT

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

REFERENCES

Coffey, T. P., *et al* (1993). Executive Summary, *Mars Observer Mission Failure Investigation Board Report*, 1, B-4 to B-7, National Aeronautics and Space Administration, Washington DC.

Kicza, M. E. (1994). *Mars Observer Corrective Action Plan*, National Aeronautics and Space Administration, Washington DC.

Stephenson, R. R., *et al* (1993). Executive Summary, *Mars Observer Loss of Signal: Special Review Board Final Report, 1-2,* Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA.