SYSTEM FAILURE CASE STUDIES

APRIL 2010 *VOLUME 4 ISSUE 4*

Mission to Mars

After eleven months in transit, and only three days away from entering the red planet's orbit, Mars Observer dropped from contact with its Earthbound NASA controllers. The project team could not restore communication with the spacecraft; no signals were detected from it in the following months, and NASA was forced to declare Mars Observer permanently lost. NASA Administrator Dan Goldin asked the Naval Research Laboratory to form an investigation board.

BACKGROUND

Ambitious Vehicle

Seventeen years had passed since NASA had last visited Mars. Sent to map the Martian surface, collect atmospheric, geologic and gravitational data, the billion-dollar Mars Observer (Figure 1) was to be the first flight of the planned Planetary Observer series of missions.

The heavily instrumented, 4,500-pound vehicle rode a Titan III rocket from Cape Canaveral, Florida on September 25, 1992 and reached Mars 337 days later. Designers and scientists anticipated a full Martian year of data collection (about 687 Earth days).

Changing Requirements

During its eight-year lifecycle prior to launch, the Mars Observer project weathered significant funding decreases, changes in the number of experiments to be conducted on Mars, and removal of follow-on missions. The designated launch vehicle changed from the Space Transportation System (Shuttle) to the Titan III rocket. Under the impact of such changes, the original schedule extended by two years and project cost doubled.

In an effort to manage cost and schedule risk, the Mars Observer mission crew employed a large number of heritage parts. The team also made tradeoffs in redundancy for several pounds of spacecraft weight. Much trust in qualification for the mission flight was granted to these heritage components.

WHAT HAPPENED?

Orbit Entry Maneuvers

After a successful eleven-month journey, the first orbit maneuver into Mars took place on August 21, 1993, as scheduled. This maneuver called for the firing of two

Figure 1: An illustration of the Mars Observer in its operational configuration in orbit.

pyrotechnic valves, which allowed helium to flow through, ultimately pressurizing the fuel tank. Firing of the main engines for actual orbit entry was to take place three days later.

During this important mission event, the team was concerned that the firing of the valve might shock and damage the amplifiers in the telecommunications systems. In order to protect the amplifiers, the team made the decision to turn the spacecraft transmitters off during valve firing. Once the firing was complete, and the tank was pressurized, the transmitters would be commanded back into operation by the team. Figure 2 shows the trajectory of the spacecraft and the

Mars Observer loses communications after planned telemetry shutdown.

Probable and Possible Proximate Causes:

- Probable: oxidizer leakage and mixing with fuel in the propulsion system with subsequent explosion
- Possible: power bus short circuit and power loss
- Possible: propellant tank rupture from regulator failure
- Possible: propellant tank rupture from ejection of initiator from pyro valve

Underlying Issues:

- Inadequate Testing
- Tradeoff Decisions
- Telemetry Priorities in Design

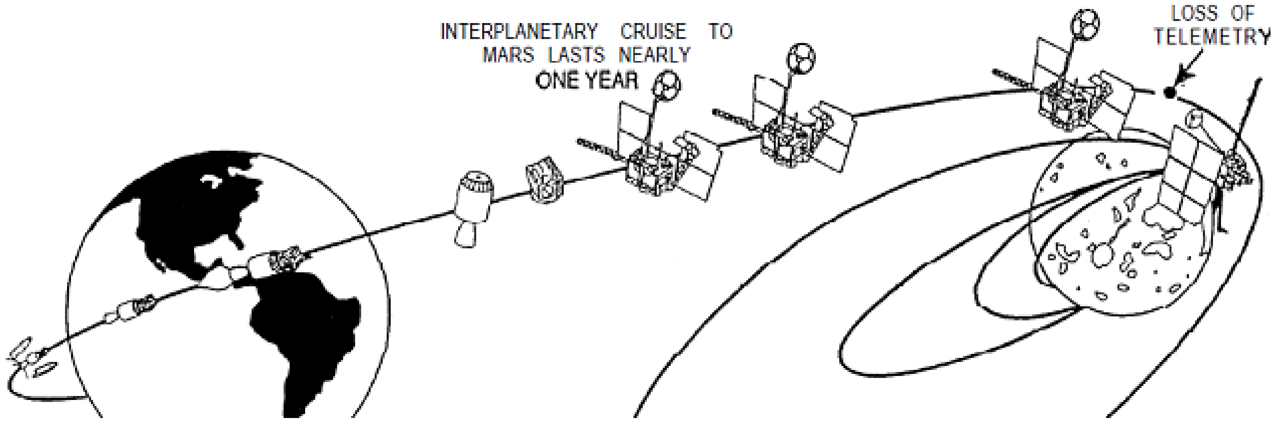

Figure 2: Diagram of the planned journey to Mars. The point where telemetry was turned off is seen in the upper right.

location in space where the team switched off telemetry.

Loss of Telemetry

The transmitters were to remain off for ten minutes. Taking into account the four minutes of warm-up time, the transmitters were to remain off for a total of 14 minutes. During this time, something happened to the spacecraft that prevented communication from being reestablished. The JPL Deep Space Network was reconfigured to optimize attempts at communication. Efforts continued into the next year but were unsuccessful.

Thus was the Mission Failure Investigation Board challenged; no physical evidence or telemetry existed to investigate. Yet through close examination of design, construction and environmental stressors, the Board was able to establish a probable mishap cause and pinpoint several weak spots in the program.

Proximate Cause

To attack the mystery, the Board employed a step-wise, process-of-elimination approach. Working backward in time from the loss of signal, fifty-nine different scenarios were theorized and studied across all spacecraft systems. The surviving scenario deemed most probable was the leak of the oxidizer (nitrogen tetroxide or NTO) through a series of check valves during their 11-month exposure to extreme cold (Figure 3). Even a few tenths of a gram of NTO mixed with the fuel (monomethyl hydrazine) in the tubing would have become explosive.

Other scenarios considered possible but less likely:
-Electrical Power System failure from a regulated power bus short circuit;

-Propellant tank rupture following regulator failure and overpressurization;

-Severe spacecraft damage from explosive ejection of a NASA Standard Initiator from its pyro valve.

Underlying Issues

Fixed-Price Procurement

The Board noted that the program's fixed-price acquisition and management strategy intended only minor modifications to a commercial, Earth-orbital production-line spacecraft. That guiding philosophy, relying on components designed for operation in a more benign environment, assembled an overall impressive vehicle. But the resulting systems were not fully understood, and flaws existed that escaped detection because component heritage was accepted as reliable for interplanetary operations. Some components were so heavily modified that their heritage was lost. Others with intact heritage were not re-qualified for a three-year interplanetary mission.

Inadequate Testing

The board identified the propulsion pressurization system check valves as unfit for an interplanetary Mars mission.

Testing showed that the valves could keep leaks down to an acceptable level during the Earth-orbiting mission for which

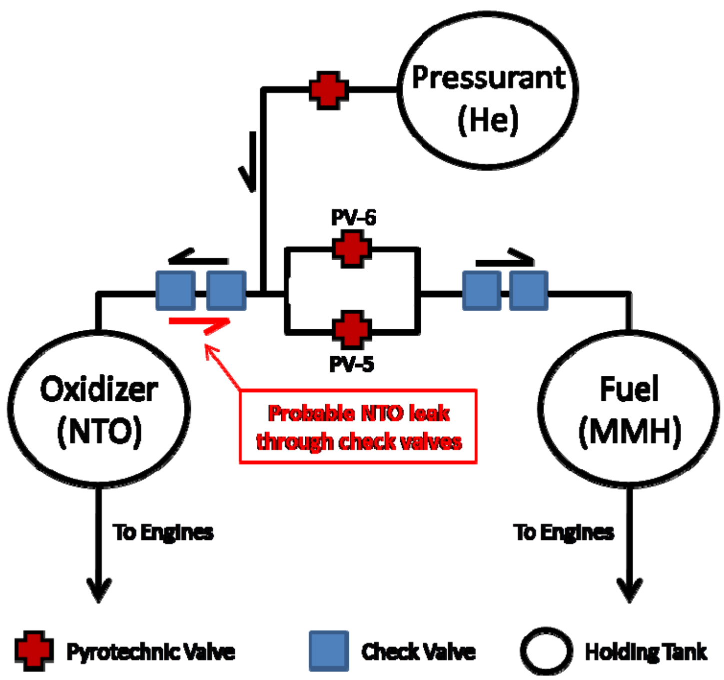

Figure 3: Diagram of section in propulsion system where explosion may have occurred. Investigators believe Oxidizer leaked through check valves (indicated by red arrow) and mixed with fuel when pyro valves 5&6 were opened.

they were designed. During their long journey to Mars, however, the valves were exposed to much more radical temperature and pressure changes, over a much longer period than original testing had qualified them to sustain. The likelihood for vapor particles to leak and accumulate in the tubing increased to the point where only a tiny leak (tenths of a gram) posed a significant explosion hazard. In defense of the designers, no leak ‘standard’ or minimum had yet been established from previous NASA projects.

Tradeoff Decisions

Fixed-price management limited the use of locally available system engineering expertise.

Of course, Mars Observer is not the first mission to face financial constraints. Though engineers typically face the need to make compromises, this mission also lacked a solid risk management plan to regulate these trade-offs. For example, the team cut the redundancy of the propulsion system to save several pounds. Given the overall spacecraft mass and the importance of this system, this decision opened the mission to unnecessary risk.

Telemetry Priorities in Design

Another significant mass tradeoff was in the telemetry design. When testing revealed amplifier vulnerability to vibration, the project team decided to turn off telemetry during heavy vibration events to protect the amplifiers. One of these heavy vibration events was the critical orbit entry maneuver, where telemetry cut out permanently.

Alternatively, the design could have been made robust enough to withstand the orbital entry burn, and allow constant telemetry transmission. Even if a failure occurred in another onboard system, engineers would then gain direct knowledge of an event sequence, and thus any failure causes.

Aftermath

Once telemetry could not be restored, the NASA team activated several antennas at different locations around the world in an attempt to catch and improve reception. These and other methods tried over the next few months failed to detect any communication from the spacecraft. Since orbit entry sequence maneuvers were already programmed into Mars Observer before the loss of telemetry, there was a chance that the spacecraft would go into orbit without further communication. Recovery efforts were directed in two channels: 1) the predicted orbit path and 2) the point where the spacecraft would have been if it had not entered orbit. Neither one of these efforts picked up any signals from the spacecraft.

The team also attempted to turn on the beacon transmitter in the Mars Balloon Relay (MBR) system, which is separate from the spacecraft transmitter system. Activity from the MBR system would mean that Mars Observer was intact, and that only the communication system was damaged. This attempt was also unsuccessful, but the team realized later on that they could not have turned on the MBR while the spacecraft was in “safe” mode, which it was.

The later realization about the MBR system led the Board to believe that the team did not have as solid an understanding of the spacecraft as expected. The further failures of all recovery efforts also led the Board to the conclusion that the spacecraft met with a catastrophic event, permanently ending the search for Mars Observer.

Following a detailed review of the development of Mars Observer, the Board emphasized several observations that, while not found to be directly connected with the mishap, would benefit future programs and projects:

-There was over-reliance on heritage hardware and software, especially since the mission fundamentally differed from the mission for which the heritage items were designed.

-The firm-fixed price contract philosophy was correct at the inception of the program but became too cumbersome after 1987 when requirements changed; a more flexible approach that took advantage of JPL experience and oversight would have served better.

-System integration to sustain actual mission-driven operational and environmental demands fell short of what was needed.

-Propulsion and telemetry mass tradeoffs done at the cost of redundancy were not appropriate.

-Spacecraft autonomy was given too much trust when its execution was not fully tested or understood.

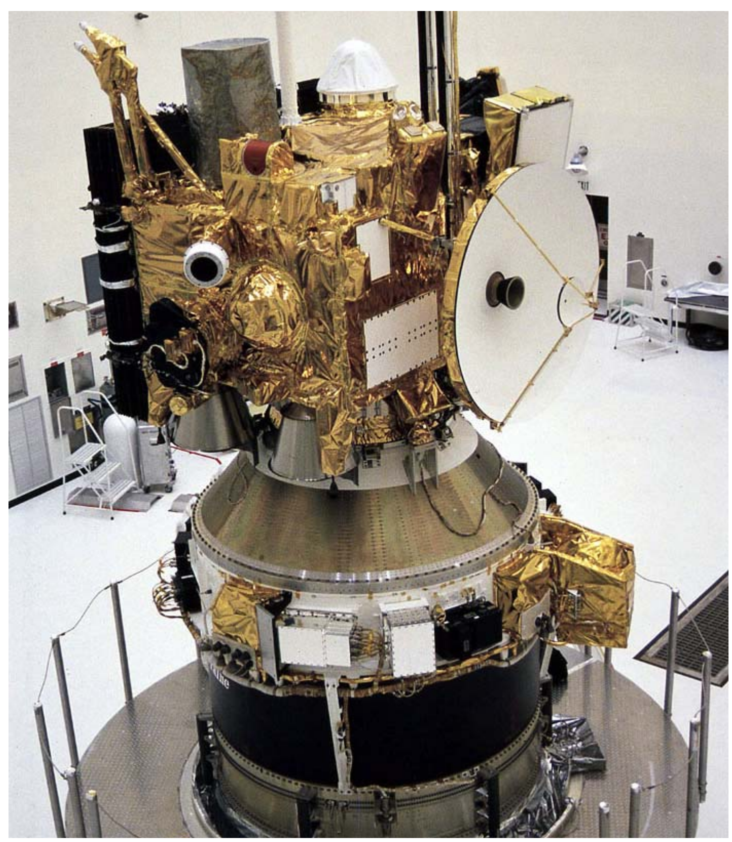

Figure 4: Mars Observer in its launch configuration, in preparation for departure.

For Future NASA Missions

The Mars Observer example shows us that unexpected consequences can follow from each design and risk management decision. A thorough, well-conceived and executed testing plan that meets or exceeds all mission demands is the best defense. When assessing commercial capability to deliver spacecraft with unique and complex missions, caution should be exercised and sufficient budget 'margin' built in to take advantage of the best experience and oversight available.

Planning also proves to be just as important as careful execution, and the lack of forward thinking can result in mission failure. Failure to identify new or existing hazards, or assess the degree of uncertainty imposed by the accepted management approach can be very costly. A comprehensive risk management plan should be established at the start of every project and followed through completion.

Additionally, though design tradeoffs are a way of life in spaceflight, reliable system operation with the ability to adapt to minor failures becomes more important as increasing time and distance interfere with spacecraft control from Earth. The Mars Rovers Spirit and Opportunity are marvelous examples of this lesson learned.

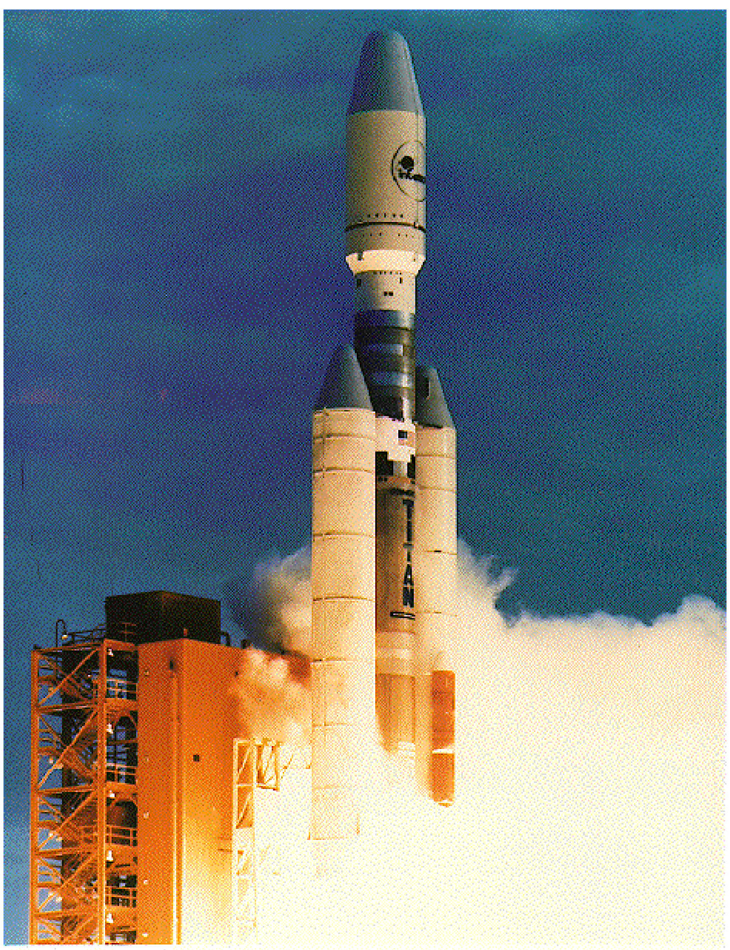

Figure 5: September 25, 1992 - Mars Observer launch aboard a Titan III rocket.

Questions for Discussion

- Does your organization have a functional risk management process in place? How do you ensure that changes to risks flow to all project plans?
- How do you determine when a heritage component or system has lost its heritage and needs to be requalified?
- Do you have a system to test and preserve the quality of all parts, heritage or new, in a project?
- What actions can you take if outside pressures threaten the reliability of your system?

When conceived, Mars Observer was intended to be the first in a series of production-line spacecraft. In actual construction and flight, it was not. Recognition of such a change and downstream management as a result is difficult, but necessary.

References:

Harland, David, and Ralph Lorenz. Space System Failures. Chichester, UK: Springer, 2005. 184-187.

"Mars Observer," Astronautix. Retrieved from http://www.astronautix.com/craft/marerver.htm.

"Mars Observer," JPL History. Retrieved from http://www.jpl.nasa.gov/jplhistory/captions/marsobserver-t.php.

"Mars Observer," Mission Failure Investigation Board Report, December 1993.

Mars Observer Investigation Report Released. Retrieved from www.msss.com/mars/observer/project/mo_loss/nasa_mo_loss.txt.

"Mishap Delays Mission to Mars," NY Times, August 28, 1992.

"NASA Loses Communication with Mars Observer," NY Times, August 23, 1993.

SYSTEM FAILURE CASE STUDIES

NSC
NASA SAFETY CENTER

Executive Editor: Steve Lilley steve.k.lilley@nasa.gov
Developed by: ARES Corporation