National Aeronautics and Space Administration

SYSTEM FAILURE CASE STUDIES

AUGUST 2009 *VOLUME 3 ISSUE 05*

Lost In Translation

The signal from NASA's Mars Climate Orbiter disappeared on Thursday, September 23, 1999. After a nine-month journey from earth, the spacecraft was moving into orbit around Mars when communications stopped. Ground software had miscalculated the spacecraft's trajectory. Instead of lightly skimming the Martian atmosphere, the spacecraft was orbiting more than 170 kilometers below its target altitude. Heat and drag from the atmosphere presumably destroyed the satellite.

Background

Mission Overview

The Mars Climate Orbiter (MCO) began the second phase of NASA's Mars exploration program. The first phase launched two spacecraft, the Mars Global Surveyor and the Mars Pathfinder, in 1996 to take global pictures of the planet and begin the search for water on Mars. The MCO followed in late 1998 to study climate and to serve as a communications relay for the Mars Polar Lander, which launched just three weeks later.

The MCO spent nine and a half months traveling to Mars. When it arrived, the mission plan called for an orbital insertion burn followed by a two-week "aerobraking" process to reduce velocity and move into a circular Martian orbit. This process had to be completed before the Polar Lander arrived so the command team on earth could use the MCO to communicate with the Lander.

Navigation

As on many spacecraft, the MCO used thrusters to control its trajectory, while reaction wheels controlled its attitude and orientation. To keep the spacecraft aligned properly when the reaction wheels built up excess momentum, Angular Momentum Desaturation (AMD) events de-spun the fly-wheels and balanced the change in momentum with a thruster burn.

After each AMD, spacecraft "Small Forces" software sent data to its companion software on earth to calculate the MCO's new position. The team used outputs from the ground software to track the MCO's trajectory and direct later AMD events.

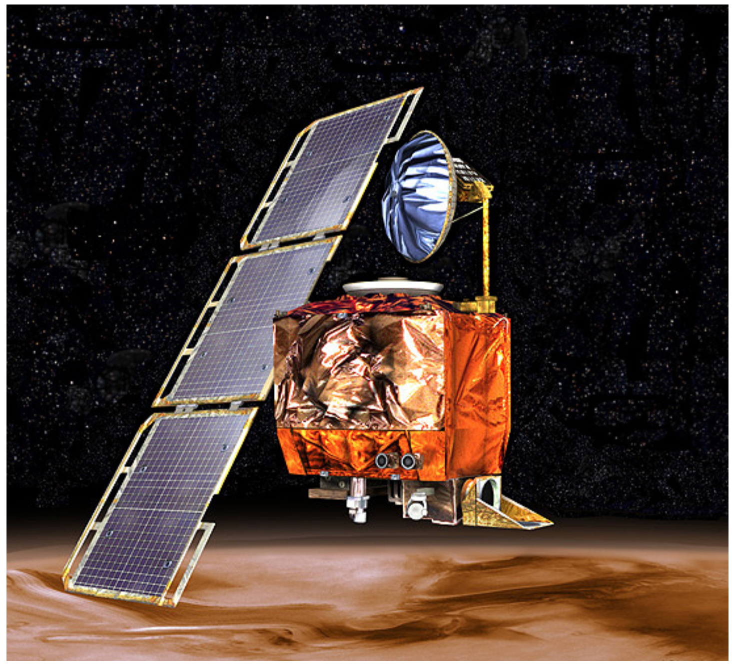

Figure 1: Artist's conception of the Mars Climate Orbiter and its asymmetrical solar array.

September 23, 1999: The Mars Climate Orbiter approached Mars 170km too close to the surface; atmospheric forces are believed to have destroyed the spacecraft.

Proximate Cause:

- Ground software used English units, while onboard software worked in metric. The discrepancy caused errors in trajectory calculations which sent the spacecraft too close to Mars.

Underlying Issues:

- Verification and validation processes did not verify that navigation software met requirements.
- The navigation team was unfamiliar with the spacecraft and its controls and unprepared for off-nominal conditions.
- Concerns were only informally communicated.

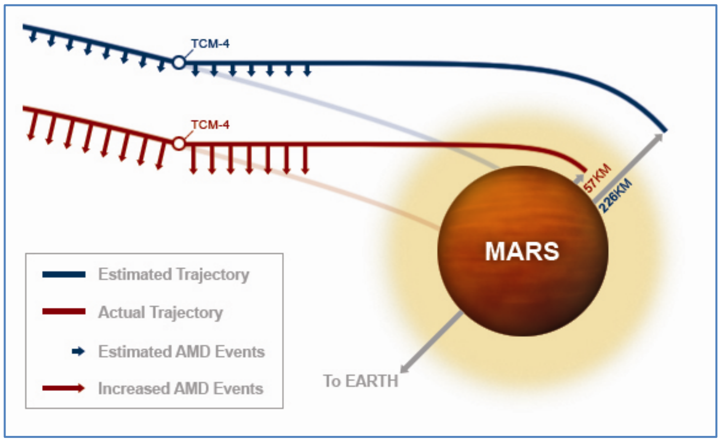

Figure 2: Actual vs. estimated approach to Mars (not to scale).

What Happened?

For the first four months of the MCO's journey, problems in the ground navigation software (not the units problem that ultimately destroyed the mission) forced the navigation team to rely on emails from the contractor to track the spacecraft's progress. When the software problem was finally fixed, operators noticed anomalous data in the ground software files. These anomalies were discussed informally but never resolved; the investigation board wrote that the anomalies eventually "slipped through the cracks."

Unknown to the navigation team, the ground Small Forces software operated in English units, while other software was metric-based. Instead of reporting figures in Newtons, the ground software calculated the trajectory in pounds force, increasing figures by a factor of 4.45. The difference increased the thruster force for each AMD event, which meant each AMD event introduced a larger trajectory change to the spacecraft than was being calculated and used in the ground navigation software. With each AMD event, the spacecraft moved farther away from its supposed location.

As the spacecraft approached Mars, the navigation team executed their final planned Trajectory Correction Maneuver, TCM-4, to align the trajectory for the Mars orbital insertion burn. If the MCO had been in the proper location, the burn would have placed the spacecraft in an elliptical orbit 226 kilometers above the planet's surface.

During the week between TCM-4 and the insertion burn, Mars's gravity pulled the MCO closer to the planet. With only one hour remaining before the scheduled burn, more precise calculations indicated that the MCO was nearing an altitude as low as 110 km, just 30 km over the minimum survivable altitude. The navigation team discussed executing an emergency trajectory change, TCM-5, to increase altitude but decided to stick to the original timeline. Executing TCM-5 would have delayed the orbital insertion burn, which would have interrupted communications with the Mars Polar Lander and put the Lander's mission at risk.

The team expected to briefly lose contact approximately five minutes into the orbital insertion burn. Forty-nine seconds earlier than anticipated, the signal disappeared. The team never regained contact with the MCO. Later calculations made with corrected values estimated the MCO's altitude was only about 57km, far too low for the spacecraft to survive (Figure 2).

Proximate Cause

Ground navigation software used English units, but all other calculations treated data from the ground navigation software as if it were in metric units. Verification and Validation did not catch the discrepancy, which introduced a bias in trajectory calculations that sent the MCO too close to Mars. Increased atmospheric stress presumably destroyed the spacecraft.

"People make errors. The problem here was not the error. It was the failure of us to look at it end-to-end and find it. It's unfair to rely on any one person."

-Tom Gavin, NASA Jet Propulsion Laboratory

Underlying Issues

It would have been easy to focus on the contractor who developed the ground navigation software for the mishap. After all, the software requirements specified metric units, but the contractor delivered a product that worked with English units. However, the mishap investigation board uncovered a wide array of issues that contributed to the MCO's failure. NASA lost the MCO because the verification and validation process did not confirm that the navigation software met requirements. The project team also had an opportunity to catch the error during the mission, when several anomalies hinted at problems with the software, but incomplete understanding of the spacecraft's design, coupled with communication problems between various elements of the MCO operations team prevented the team from recognizing and mitigating the problem.

Verification and Validation

Neither the programmers who developed the Small Forces software nor the testing team properly used the Mars Surveyor Program's Software Interface Specification (SIS) to ensure the Small Forces software was compatible. The investigation board found no evidence of complete, end-to-end testing for the Small Forces software, and they could not determine whether independent verification and validation had been performed on the software in question. In any case, the interface control process and interface verification were not sufficiently rigorous.

Communication between Project Elements

Although the navigation team discussed concerns about the MCO's trajectory among themselves, they did not fully communicate their concerns to the spacecraft operations team or project management. Overall, there was little cross-communication or shared understanding between various teams on the project. Team members relied on informal communication channels rather than using standard methods for reporting concerns. Teams were isolated from the other teams, particularly the operations navigation team.

Preparation and Understanding

The Mars Surveyor program used the same operations navigation team for all of its missions. While this cost-effective approach could also quickly develop experience, numerous obligations of the navigators prevented them from developing in-depth systems knowledge of the MCO. The team was running three missions simultaneously—the Mars Global Surveyor, the MCO, and the Mars Polar Lander—and the team lacked sufficient staffing to fully support all three missions at once. With oversubscribed team members, minimal training and an incomplete knowledge of the MCO's design, the operations navigation team relied on their intimate knowledge of the Mars Surveyor to operate the MCO. Assumptions based on this prior knowledge contributed to mission failure.

The mishap investigation board determined that the contingency Trajectory Change Maneuver (TCM-5) might have saved the mission. However, even if the team had understood that TCM-5 was critical to the MCO's survival, they were not prepared for the maneuver. Analysis and tests for TCM-5 had not been completed, and procedures for the operation were not fully developed. Rather than making a risk-informed decision, they allowed timeline concerns to dictate their decision.

Aftermath

In the days following the MCO failure, the operations navigation team successfully patched the software for the Polar Lander, which reached Mars on the correct trajectory three weeks after the MCO was lost. Unfortunately, there were unrelated software problems in the Lander's descent sequence, and the Lander crashed on Mars's surface.

In the wake of these failures, the MCO investigation board issued a Report on Project Management in NASA to highlight some of the problems the MCO team experienced and articulate lessons learned to be incorporated in future missions.

Meanwhile, the Mars program continued. In 2005, the Mars Reconnaissance Orbiter proved to be a huge success, returning more data than all other Mars missions to date. Future missions include the Mars Science Laboratory, which is scheduled to launch in fall 2011 to continue testing Martian rocks and soil.

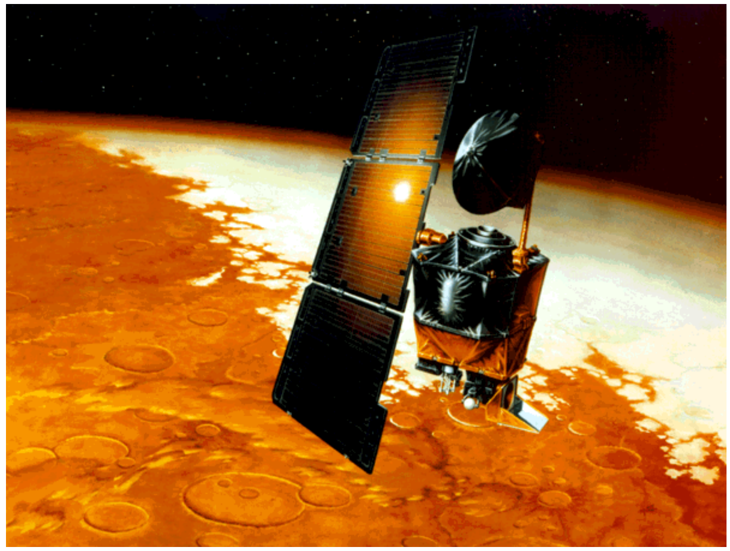

Figure 3: Artist's conception of the Mars Climate Orbiter above the Martian landscape.

For Future NASA Missions

Verify Requirements

The Mars Climate Orbiter's crucial lesson for NASA is to verify that requirements have been followed. The verification and validation (V&V) process should trace directly to the mission requirements. Always include independent reviews for mission-critical software in the V&V process. Make sure the review team represents the skill set necessary to conduct a thorough, disciplined review. Independent reviews for all mission-critical components should have caught the fatal unit mismatch before the MCO left earth.

Identify Hazards

When the MCO reached Mars, the operations team chose to pursue the original mission timeline rather than execute TCM-5 to move the MCO farther from Mars. They decided to proceed as planned because their ideal timeline did not allow for an additional trajectory change, and they were unprepared for this off-nominal scenario. Their decision was not based on the risk associated with their current course. It is always important to define and quantify acceptable risk at the beginning of a project, then assess and prioritize risks throughout. During the life of any project, continue to systematically assess what could go wrong or what may have been overlooked. Engage operations personnel early in the project so they understand significant risks. If the operations team had acquired a better understanding of the MCO's navigation, they might have recognized the risk involved in sticking to the original mission timeline.

Communicate with Project Teams

Communication barriers between project elements contributed to the MCO mission failure. Each team worked independently, with little cross-communication between groups. To prevent isolation and improve communication, include all project groups when going over critical tasks, and invite entire project teams to all meetings. Ensure project elements effectively share concerns and dispel assumptions.

To uncover risks and ensure that concerns reach the appropriate parties, information must flow up, down and sideways. Although the operations navigation team discussed concerns among themselves, they did not adequately share them with other project teams. Encourage open communication and support a policy that empowers all team members to forcefully elevate any issue to the highest priority within the appropriate engineering discipline until it is understood. As this mishap demonstrates, even seemingly minor concerns need to be formally addressed. Use problem reporting processes to mitigate unresolved problems and ensure resolution. Everyone is responsible for filing anomaly reports to ensure decision makers have access to critical information.

From Awareness to Action

Many of the issues highlighted by the Mars Climate Orbiter mishap investigation in 1999 were identified as contributing factors in the 2005 Demonstration of Autonomous Rendezvous Technology (DART) mission failure (see “Fender Bender,” SFCS 2.7). As this repetition shows, simply identifying the problems that cause mission failures is not enough; each mission team needs to determine how to implement the lessons learned from previous missions. Because the best plans and best intentions can be quickly derailed by the pressures of running an operation, this requires a concerted effort both before and during the mission. Periodically step back to evaluate the execution of your mission and your role in it.

Questions for Discussion

- How can you personally improve communication between teams in your project? What changes could your team implement to improve communication both within your own team and with other elements?
- Are your tasks and responsibilities clearly defined? Do you understand your colleagues’ roles?
- Does your team maintain a prioritized list of risks? How could you improve your process for tracking risk?
- What steps has your team taken to prepare for off-nominal conditions?
- Does your review team represent all of the skills and expertise necessary to adequately review your software/hardware, or should you bring in additional support to guarantee thorough reviews?

References:

Mars Climate Orbiter Mishap Investigation Board Phase I Report, NASA, November 10, 1999.

Mars Climate Orbiter, Artist’s Conception. [Online Image], NASA. Accessed 13 December 2008. <http://nssdc.gsfc.nasa.gov/nmc/masterCatalog.do?sc=1998-073A>

Mars Climate Orbiter, Artist’s Conception. [Online Image], NASA. Accessed 13 December 2008. <http://mars.jpl.nasa.gov/msp98/orbiter/moi.html>

Mars Climate Orbiter, Artist’s Conception. [Online Image], NASA. Accessed 13 December 2008. <http://www.jpl.nasa.gov/jplhistory/captions/mars climateorbiter-t.php>

Clark, Greg. *Navigation Team Was Unfamiliar With Mars Climate Orbiter*. Space.com. 10 November 1999. Accessed 19 January 2009. <http://www.space.com/news/mco_report-b_991110.html>

Mars Missions: Historical Log. JPL. Accessed 18 January *2009.* <http://mars.jpl.nasa.gov/missions/log/>

Mars Program Independent Assessment Team Summary Report. NASA. 14 March, 2000. Accessed 23 April 2009. <ftp://ftp.hq.nasa.gov/pub/pao/reports/2000/2000_mpiat_summary.pdf>

Oberg, James. *Why The Mars Probe Went Off Course.* Spectrum Magazine. December 1999. Accessed 20 January 2009. <http://www.jamesoberg.com/mars/loss.html>

Report on Project Management in NASA. Mars Climate Orbiter Mishap Investigation Board. 13 March 2000.

Acknowledgements:

Special thanks to Greg Dukeman for his insightful peer review.

SYSTEM FAILURE CASE STUDIES

NASA SAFETY CENTER

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