National Aeronautics and Space Administration

System Failure Case Studies

OCTOBER 2007 Volume 1 Issue 8

LEWIS SPINS OUT OF CONTROL

The Lewis Spacecraft Mission was conceived as a demonstration of NASA's ***Faster, Better, Cheaper*** *(FBC) paradigm. Lewis was successfully launched on August 23, 1997, from Vandenberg Air Force Base, California on a Lockheed Martin Launch Vehicle (LMLV-1). Over the next three days a series of on-orbit failures occurred including a serious malfunction of the attitude control system (ACS). The ACS issues led to improper vehicle attitude, inability to charge the solar array, discharge of batteries, and loss of command and control. Last contact was on August 26, 1997. The spacecraft re-entered the atmosphere and was destroyed 33 days later, calling into question the value of FBC.*

Artist's conception of the (unspinning) Lewis Spacecraft

BACKGROUND:

Mission: The Lewis Spacecraft Program was initiated in support of NASA's "Mission to Planet Earth." The spacecraft was outfitted with advanced Earth-imaging instruments intended to push the state-of-the-art.

Contract: NASA awarded TRW a $58M cost-plus-award fee contract in June 1994 which called for launch within 24 months of the award. Under the performance-based contracting model, the intent was to fully utilize commercial best practices. As a result the contract did not include a government-directed deliverable requirements list or any government-specified technical requirements. Additionally, there were no performance, quality assurance, or other government standards imposed.

Management: Lewis was managed at Headquarters under NASA's Small Satellite Technology Initiative (SSTI) Program. The four year project saw frequent turnover in TRW management tasked with oversight of Lewis development. During a single 14 month period TRW saw four different Program managers and four General/Division managers.

Project Team Location: In January 1995, just six months after the contract was awarded, TRW moved most of their project team from Chantilly, VA to Redondo Beach, CA. The ACS development team and the flight operations team remained in Virginia, while integration, testing, and ACS functional discipline experts moved to California.

Contract Management: Between August 1994 and February 1995, communication between NASA and TRW over cost control and changes in scope became increasingly adversarial. In March 1995, NASA issued TRW a formal budget overrun notice to "show cause and cure."

Cost Containment Initiatives: As part of the cost savings "cure," TRW made the decision to go to a one shift ground control crew even for early on orbit operations – a decision that was not known to NASA (or to senior TRW

Lewis Spacecraft lost after only three days in orbit

Proximate Causes:

- Inappropriate application of ACS software and lack of design peer review
- Inconsistent monitoring during critical early operational phase

Underlying Issues:

- Ineffective and inconsistent project leadership
- Incomplete and unsustained articulation and communication of ***Faster, Better, Cheaper***
- Inadequate test and verification of heritage hardware/software
- Insufficient budget to support robust ground operations

executives) until after the on orbit failure. Another cost containment idea was to use the ACS "Safe Mode" (designed to maintain stable satellite attitude with solar panels facing the sun) designed for the Total Ozone Mapping Spacecraft (TOMS), a vehicle with a different mass distribution and solar array orientation than Lewis.

Contract Modifications: In May 1996, after the Pegasus XL failure, NASA issued a change order replacing the Pegasus launch vehicle with the LMLV-1 booster and extending the mission from a three-year, 0.83 design reliability rating to a five-year, 0.86 design reliability rating, which increased the contract value to $64.8M.

Critical Event Timeline *

	August 23
2:51 a.m.	Launch from Vandenberg AFB to 300km parking orbit.
3:10 a.m.	Power switches unexpectedly from Bus A to Bus B.
1:30 p.m.	Data recorders fail to playback.
	August 25
Morning	Spacecraft reconfigured back to A-side processor.
10:17 a.m.	Contact with the spacecraft lost for three hours.
1:17 p.m.**	Contact reestablished; spacecraft pitch and yaw 28 degrees off the Sun; batteries at 43% depth of discharge (DOD).
	Spacecraft restored to Safe Mode, and observed as stable for four hours. Batteries fully charged.
7:00 p.m.**	Ground operations cease; staff begins nine hour rest period, electing not to request emergency ops team.
	August 26
Early a.m.	Autonomous ACS attempts to maintain intermediate axis mode, result in excessive thruster firings and eventual ACS shut-down.
4:02 a.m.	Edge-on spin discovered. Batteries at 72% DOD.
5:32 a.m.**	Batteries at 82% DOD.
6:17 a.m.	Flight Control attempts to arrest spacecraft rotation by firing ACS thrusters; contact never re-established.
	September 28
7:58 a.m.**	Lewis re-enters earth's atmosphere and burns up.

** Eastern Daylight Time* *** Approximate time*

CRITICAL EVENTS:

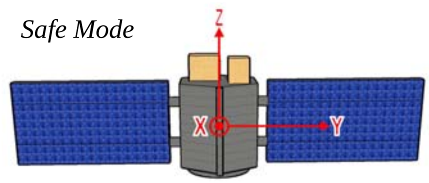
The Lewis Spacecraft was launched on August 23rd and began experiencing problems almost immediately. Ground control maintained intermittent contact while attempting to correct the failures. At 1:17 pm on August 25th, contact was re-established with the spacecraft (after having been lost for three hours), and the ground station determined that Lewis was pointing 28 degrees (pitch and yaw) off the Sun and that the batteries were at a 43% depth of discharge (DOD). Despite this condition of flying with a serious "known unknown" in-flight anomaly, the flight operations team restored Lewis to Safe Mode and went off shift for 9 hours. The operations manager chose not to call in a stand-by emergency ground control team from Redondo Beach when operators went off duty.

Later that morning the ground station noticed that the spacecraft batteries were beginning to discharge rapidly while the spacecraft was rotating unstably about its x-axis despite entering Safe Mode. At approximately 5:32 am (82% DOD), the flight controllers attempted to arrest the rotation by issuing three, one-second fire commands to selected ACS thrusters. Regrettably, only the first fire command was executed as flight operations controllers misaddressed the second and third commands, sending them to the B-side, rather than the A-side, computer. Contact with the spacecraft was never re-established.

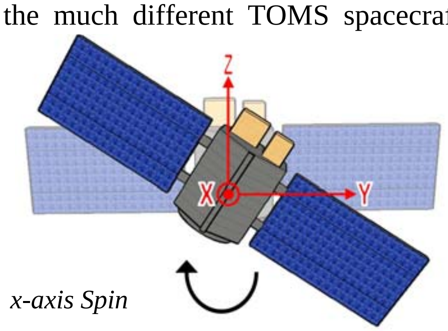
DEGRADING ATTITUDE CONTROL

Safe Mode: "Safe Mode" describes the operational attitude in which the spacecraft's x-axis was oriented toward the sun with the extended solar panels (whose length was oriented along the y-axis) fully exposed to sunlight to ensure continual charging of the batteries. The ACS, which consisted of flight software and eight onboard thrusters, had the job of holding Lewis in this stable, sun-facing attitude.

Safe Mode

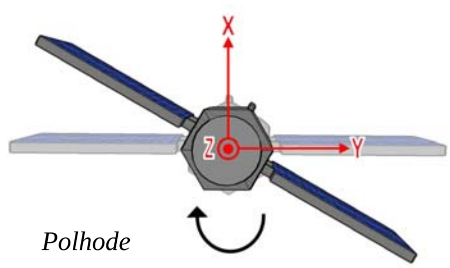


Spinning Up: It is believed that during the early morning of August 26, while ground control was off duty, the inappropriate application of the ACS software (designed for the much different TOMS spacecraft) resulted in ACS thruster firings that, instead of stabilizing the spacecraft, resulted in a net spin about the x-axis. The ACS system was controlled by a two-axis gyro that provided no rate information about the x-axis.



x-axis Spin

Tumble Back Flip: The "wind milling" Lewis spacecraft gradually slowed as a result of mechanical energy dissipation. As it did, the spacecraft underwent an unfortunate change in orientation, flipping its principal axis of rotation by 90 degrees due to a



Polhode

well-understood phenomenon known as ***polhode*** motion (Greek for "path of the pole"). ***Polhode*** motion describes the natural reorientation of a spinning object about its principal axis (i.e., the axis where the percentage of mass is located furthest from the axis of rotation) in accordance with the fundamental law of conservation of angular momentum. As angular velocity decreased, Lewis gradually migrated 90 degrees, transferring the spinning motion from the x-axis to the z-axis. The die was now cast. With the solar panels spinning edge-on to the sun, there was no way to maintain the necessary battery charge.

See related videos from NASA Skylab that explain the ***polhode*** concept: http://einstein.stanford.edu/highlights/hl_polhode_story.html (accessed June 2007).

PROXIMATE CAUSE:

The Lewis Spacecraft Mishap Failure Investigation Board (LSMFIB) found that spacecraft failed due to the combination of a technically flawed attitude-control system design and insufficient monitoring of the spacecraft during its crucial early operations phase.

UNDERLYING ISSUES:

Weak Project Management

Leadership sets the tone. The transient TRW management environment made it difficult to articulate program values (e.g., balance, quality, integrity, belt-and-suspenders, never fly with a known unknown, test as you fly – fly as you test). The LSMFIB noted that "the decision to operate the early on-orbit mission with only a single shift ground control crew was not clearly communicated to senior TRW or NASA management." In the absence of consistent leadership, a singular cost containment emphasis emerged as the leadership theme.

<u>Project Team Dislocation:</u> The decision to move TRW technical and management core capabilities to Redondo Beach in January 1995 was a significant factor because it isolated the Lewis ACS and flight operations sub-system managers from critical discipline experts and corporate assurance processes that might have challenged design assumptions and pressed for more extensive simulation and training of operations personnel. In general, TRW was to provide a functional group peer review which was completed for all other systems; however a similar review was not conducted for the ACS design.

Poorly Articulated Approach: FBC

Striving to address relevant issues within a politically charged context, the mishap board's report consequently identified a litany of contributing causes while attempting to address serious problems with the foundations of FBC (the need for cost realism and independent assessment and review).

<u>"Toss it over the fence":</u> In implementing the new FBC management paradigm, there existed a fundamental disconnect and lack of communication between NASA and TRW. The FBC model, by design, called for projects like Lewis to be managed at NASA Headquarters rather than at Centers, relying on TRW to provide the necessary technical oversight. The request for proposal did not include government-specified technical requirements, quality assurance, or other government standards. In the absence of higher level policy guidance NASA program executives struggled to define FBC in practical terms. As an overarching cost and schedule emphasis emerged traditional NASA assurance control functions eroded.

In this context, the LSMFIB called for increased independent technical review and implementation of risk management practices, more clearly identified rolls and responsibilities, and more effective communication among project team personnel.

<u>Ineffective Resource and Requirement Management:</u> The LSMFIB observed that enormous cost containment pressures and adversarial relationships existed between NASA and TRW throughout the project life-cycle. The board also felt that the formulation process was constrained to the extent that mission success was in jeopardy from the start. The board noted that "meaningful trade space must be provided along with clearly articulated priorities. Price realism at the outset is essential and mid-program change should be implemented with adequate adjustments in cost and schedule."

Poor Hardware/Software Verification

Misapplication of a "heritage design" (borrowed from a previous application) for the ACS represents a fatal error. The "heritage trap" occurs in making flawed assumptions regarding the applicability of a specific technology to another operating environment or another hardware configuration. The largely undefined FBC paradigm encouraged the use of heritage hardware and software as a means of saving the expense of design verification testing and analysis.

The ACS system verification was likewise flawed. The verification activity modeled a limited set of nominal, on-orbit attitude control cases, failing to model a thruster imbalance scenario that ultimately led to the loss of the spacecraft.

Failed Intervention

The LSMFIB identified multiple failures in operational planning and execution noting that the "contractor implemented a single crew operation as a cost savings measure, leaving the ground control function unmanned during critical on-orbit failure events." (Referring to the serious ACS problems experienced during the early morning of August 26.) "Even after numerous critical anomalies the operations team failed to declare an emergency that might have signaled the need for round-the-clock monitoring and brought broader knowledge and expertise to bear on the recovery efforts."

AFTERMATH:

In the wake of the Lewis failure NASA cancelled the SSTI-2 Clark Mission, companion to Lewis scheduled for launch in early 1998. The most celebrated (and singular) FBC success story was the Pathfinder Mission which reached Mars in July 1997. This was followed by back-to-back mission failures with the losses of the Mars Climate Orbiter in September 1999 and the Mars Polar Lander three months later. Only a year later, NASA cancelled both the X-33 Venture-Star Program managed by Lockheed Martin and the X-34 Program managed by Orbital Sciences Corporation. FBC faded into history with the change in NASA Administration in 2001, leading to a shift back to a balanced government role in managing space program development and implementation.

LESSONS LEARNED FOR NASA:

The NASA Lewis spacecraft serves as a cautionary tale for those proposing radical cost saving or cycle-time reduction techniques in complex space programs. While continual process improvement and incorporation of time-saving technology can move a program toward a more lean operating posture, there are simply no shortcuts in the fundamental life-cycle systems engineering disciplines, in particular, areas of test, verification, quality assurance, operations management, and independent review. NASA's current emphasis on "program review consolidation" must be carefully implemented to ensure that independent safety and mission assurance reviews are not compromised.

Specific failures in test and verification were evident in this case. In some ways, Lewis was the ultimate heritage trap in which the TOMS attitude control software was used for pre-programmed, nominal operating conditions. It would appear that no one challenged the assumptions. Lewis further makes the case for independent verification and validation (IV&V) of flight software. The "validation" portion of IV&V would have been beneficial as the ACS software was perfectly fine (for a TOMS class spacecraft) but was misapplied in the case of Lewis. The consequence of staffing and training flight operations "on the cheap" is another important object lesson. The Lewis controllers were unable handle off-nominal behavior on their own and chose not to engage the emergency backup team.

Other inter-related issues to consider include the lack of depth on the flight operations team, and the lack of urgency, follow-through, and management attention in addressing numerous flight anomalies, including power system and data recording issues, and obvious attitude control problems prior to the final ACS-related break down.

Ultimately, the Lewis Spacecraft failure is a reminder that NASA should never compromise the Agency's historical core value of systems engineering excellence and independent reviews.

Questions for Discussion

- Many NASA engineers have expressed the belief that the solution to the FBC equation is a null set (i.e., one can achieve at most two of the three objectives on any project). What do you think?
- Do you consider the Lewis failure a relevant case study for the current COTS (Commercial Orbital Transportation Services) program and/or other commercial space ventures?
- The current NASA governance approach has been likened to a three-legged stool, balancing program management, engineering, and safety assurance roles and authority. Do you think this balance has been achieved? Will this arrangement preclude another Lewis-type failure?
- Who on your program or project team (by name) will stand up and actively challenge technical assumptions and decisions such as the call to use TOMS ACS software on the Lewis Spacecraft?

References:

Lewis Spacecraft Mission Failure Investigation Board - Final Report, NASA, 1998.

NASA Public Lesson Learned: 0625, Lewis Spacecraft Failure Investigation Board, http://www.nasa.gov/offices/oce/llis/0625.html, (accessed May 2007)

TRW Release: 97-208, *Attempts to Contact Lewis Spacecraft Unsuccessful; Re-Entry Likely Next Week*, 1997.

SYSTEM FAILURE CASE STUDIES
A product of the NASA Safety Center

Executive Editor: Steve Wander stephen.m.wander@nasa.gov

To view this document online and/or to find additional System Failure Case Studies, go to http://pbma.nasa.gov