The Million Mile Rescue: SOHO Lost in Space

Leadership ViTS Meeting
November 2008

Bryan O'Connor
Chief, Safety and Mission Assurance

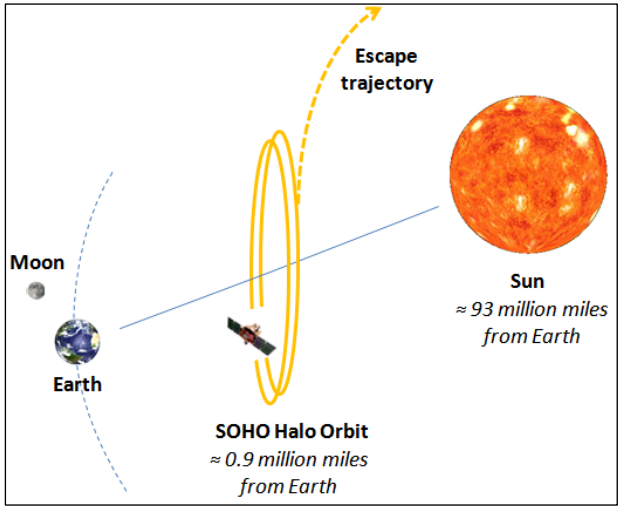
Jim Lloyd
Deputy Chief, Safety and Mission Assurance

This and previous presentations are archived at:

http://pbma.nasa.gov/pbma_main_cid_584

Lost in Space

- The Solar Heliospheric Observatory spacecraft (SOHO) began its 2-year mission to study the Sun and solar winds in 1995 and experienced tremendous scientific success, earning it multiple mission extensions currently through 2009.
- The first mission extension came in 1997. Software modifications were uploaded to the Attitude Control Unit (ACU) computer, instructing it to conserve operation of its gyroscopes, used for attitude sensing, anticipating the extended missions.
- Modifications were implemented on June 24, 1998, and immediately triggered alarms that sent SOHO into a "safe mode," which could only be resolved by ground operators. Once attitude stability was established, each gyro was returned to the ACU for recalibration before resuming operations.
- Recalibration consisted of thruster-based adjustments to eliminate "drift biases" that occur from thermal and mechanical wear over time.



SOHO revolved around the Sun in lock step with the Earth's revolution, while maintaining its own halo orbit about four times the distance away from he Earth as the Moon. Schematic is not to scale.

- Ground operators found that an error in the code modifications had triggered the alarm. But they failed to detect another critical error -- that is, one of the gyros never started spinning. Attempts to recalibrate the despun gyro resulted in a series of safe modes and thruster firings that progressively spun SOHO out of control.
- By 12:43 am on June 25, 1998, SOHO's attitude had diverged so far beyond control that all power, communications, and telemetry signal were lost. The next 3 months were spent on a massive, labor-intensive recovery of the $1 billion joint project between NASA and ESA.

Code Errors

- SOHO had three gyros. With the modified code, Gyro C sensed the roll rate during nominal operations. Gyro B was used to detect excessive role rates. Gyro A was de-spun for conservation.
- If excessive role rates were detected, a "safe mode" was triggered where Gyro A was reactivated (respun) to replace Gyro C as the roll rate sensor. After stabilization and recalibration, Gyro A was despun, and Gyro C was respun.

Gyro	Function	Used in nominal ops?	Used in "safe mode"?
A	Roll rate sensing	No	Yes
B	Excessive roll rate detection	Yes	Yes
C	Roll rate sensing	Yes	No

- The modified code contained <u>two errors</u>:
  1. Code to respin Gyro A in safe mode was inadvertently omitted.
  2. Gyro B's fault detection setting was 20 times more sensitive than its specification.

- Gyro B's settings triggered the safe mode on June 24, 1998. Ground operators quickly fixed the error but failed to confirm the spin status of Gyro A before initiating the recalibration attitude adjustments. As the despun gyro's readings did not change with thruster firings, SOHO's *actual* roll rate did until it was sufficiently high to trigger another safe mode.
- <u>CRITICAL DECISION MISTAKE</u> – With Gyro C inactive in safe mode, operators incorrectly concluded that Gyro B's fault detection was defective and shut it down. They resumed recalibration thruster firings based on Gyro A's nominal roll rate readings.
- SOHO's attitude progressively worsened until all communication was lost in the early morning of June 25, 1998. After 3 months of intense analytical work and some good fortune, contact was eventually reestablished and SOHO was returned to full operational capability. In June 2008, SOHO marked a milestone by discovering its 1500th comet, more than all other such comet observers combined.

Proximate Cause

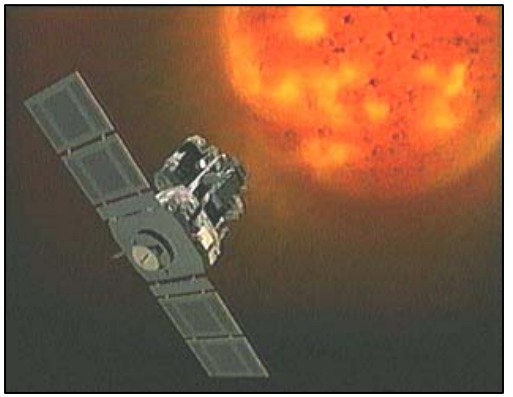
- Critical errors in the code modified to conserve gyro usage configured the gyros incorrectly and caused inaccurate thruster firings which progressively destabilized the spacecraft.

Root Cause/Underlying Issues

- Lack of Change Control
  - Code modifications were not properly documented, communicated, tested or approved by either NASA or ESA.
  - There were no independent reviews, no hard copies of command sequences, and no changes to the filename.
  - The spin status of the gyros was not obvious to ground operators, such that it allowed roll rate readings to be collected and misinterpreted, even as the gyro itself was despun.
- Failure to Follow Procedures
  - Safe mode procedures specifically stated that the last three telemetry frames be examined and spin status of gyros be confirmed before attempting recovery, neither of which was done.
  - Gyro B was spun down without the procedural approval of a Materials Review Board.
- Overly Aggressive Task Scheduling
  - The scientific activities planned for June 24-29 did not allow for contingency time in the schedule and were to be performed without any additional staff.
  - To maintain the schedule, key engineers were planning experiments instead of assisting in the safe mode recovery.
- Inadequate Staffing and Training
  - The flight operations team was not properly trained in the details of the SOHO design and operations.
  - Frequent turnover resulted in only two members of the operations team with comprehensive knowledge of SOHO, neither of whom had any expertise in the programming language used in the gyro command sequences.

Lessons Learned for NASA

- Modifications or updates to flight critical software should require formal validation, verification, and approval of the entire script before implementation.
- The “on-off” status of equipment should be unmistakably clear to prevent a false sense of redundancy or reliability. An effective design should not allow sensors to provide data that can be misinterpreted as valid when in fact the device is inactive.
- Achievement of mission objectives often depend on the health and safety of the spacecraft. With the reality of limited budgets in extended phases, time should be taken to carefully review the operational timeline for feasibility.
- Procedures are essential for determining whether or not it is appropriate to proceed, and established procedures must not be circumvented.
- Programs and projects need to properly plan for and handle turnover of control, ensuring that all staff have specific knowledge pertinent to the particular spacecraft.



“At any time during the … emergency situation, the verification of the spinning status of Gyro A would have precluded the mishap.”

ESA/NASA Investigation Board