National Aeronautics and Space Administration

System Failure Case Studies

NOVEMBER 2008 Volume 2 Issue 9

The Million Mile Rescue

The Solar Heliospheric Observatory spacecraft (SOHO) is a major element of the joint ESA/NASA International Solar Terrestrial Program. It was launched on December 2, 1995, and successfully completed its primary mission by 1997. After implementation of code modifications meant to increase SOHO's lifetime during its extended operations phase, multiple errors in the new command sequences repeatedly sent the spacecraft into an emergency safe mode. One key error remained undetected while ground controllers made a critical mistake based on an unconfirmed and faulty assumption. SOHO's attitude progressively destabilized until all communication was lost in the early hours of June 25, 1998. It took three months to miraculously recover and restore SOHO to full mission status.

BACKGROUND

The Solar Heliospheric Observatory (SOHO) is a joint international project between NASA and the European Space Agency (ESA) to study the Sun, from its deep core to the outer corona, and the solar winds, using 12 on-board scientific instruments (Figure 1). Launched on December 2, 1995, SOHO was designed for a two year mission. But in 1997, the mission was extended to 2003 because of its spectacular success. This extension was the basis of the code modification that sparked this mishap. After recovery, subsequent extensions were granted through 2009.

SOHO was designed to revolve around the Sun in lock step with the Earth's own revolution (Figure 2) by maintaining a halo orbit around the First Lagrangian point, where the combined gravity of the Earth and the Sun keep SOHO's orbit anchored in the Earth-Sun line. Once in this orbit, SOHO's attitude was generally stable and used spinning reaction wheels controlled by an Attitude Control Unit (ACU) computer to autonomously adjust for internal or external disturbance torques. If the wheels reached a spin near their design limit, ACU automatically despun the wheels, used thrusters to stabilize attitude, and then reactivated the wheels to resume attitude control. The ACU used a gyroscope (Gyro C) to sense roll attitude during these maneuvers.

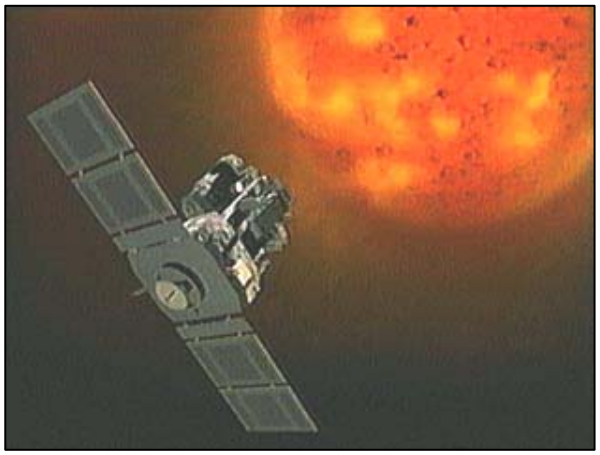

Figure 1: Artist's conception of the SOHO spacecraft.

SOHO also contained a second gyro (Gyro B), used solely for fault detection, e.g. to sense excessive roll rates (beyond some predetermined tolerance). If an excessive roll rate was detected, SOHO was triggered to enter a "safe mode," where it ensured that its panels were facing the Sun, temporarily suspended the ACU computer, and then awaited ground commands. This was called an Emergency Sun Reacquisition (ESR) mode, and it required ground commands to restore normal operations under the ACU. During recovery from an ESR, ground controllers used the third and final gyro (Gyro A), instead of Gyro C, for roll rate sensing. The recovery sequence

On June 25, 1998, all communication with SOHO was lost.

Proximate Cause:

- Errors in software code configured the gyros incorrectly and caused inaccurate thruster firings which destabilized the spacecraft

Underlying Issues:

- Software code modifications were not properly documented, communicated, tested, or approved
- Operators failed to follow procedures to check the spin status Gyro A before taking actions
- Staffing levels were inadequate for the schedule
- Detailed training specific to SOHO was insufficient

finished with a recalibration of all three gyros and a restoration of Gyro C to roll rate sensing.

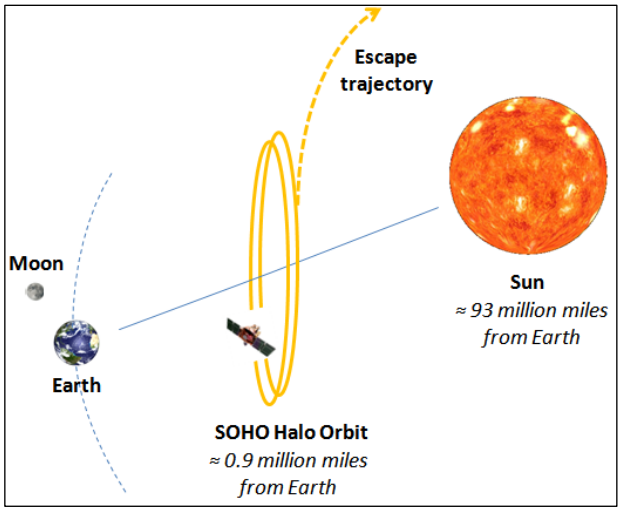

Figure 2: SOHO's halo orbit is about four times the distance away from Earth as the Moon. Escape trajectory is also shown. Schematic is not to scale.

What Happened?

Gyroscope Misconfigurations

Each gyro is used only for its specific independent function. And all three require periodic calibrations to account for drift bias, which is a common result of mechanical wear, angular changes, or exposure to extreme temperatures. The drift bias is determined by ground engineers and is then uplinked to the spacecraft's on-board computer with the correct coordinates for each gyro, allowing the spacecraft's attitude control functions to operate accurately. Due to the same mechanical and thermal wear that causes drift bias, gyros eventually become non-operational, which became a concern as the SOHO mission was extended.

Gyro	Function	Used by ACU?	Used during ESR?
A	Roll rate sensing	No	Yes
B	Excessive roll rate detection	Yes	Yes
C	Roll rate sensing	Yes	No

In February 1997, the flight operations team modified gyro command sequences to attempt to address this issue. Specifically, a command was written to deactivate (spin down) Gyro A when not in use, which is any time other than ESR mode. The code was supposed to include a function to respin Gyro A upon entering an ESR (a function actually mandated for spacecraft safety). However, this function was erroneously omitted in the new command sequence. The modification had been introduced with a Mission Operations Change Request (MOCR) in March 1997 but was not used in gyro calibrations until June 24, 1998. Therefore, even though the SOHO spacecraft had entered the ESR mode four times prior to June 24, the code modifications were not in use and did not affect successful recoveries by ground crews. But the software modifications also contained a second critical error. The fault detection setting on Gyro B was 20 times more sensitive than it should have been. It was this latter error that triggered this mishap and sent SOHO into its fifth ESR mode (ESR-5) at 7:16 pm on June 24, 1998.

The recovery effort began immediately but was complicated by the aggressive scientific task schedule planned for June 24-29. The core SOHO team was already working on a compressed timeline without the luxury of additional support or contingency time. Ground controllers quickly discovered and corrected the error in Gyro B but did not notice that Gyro A had not reactivated during the ESR. Shortly thereafter, as a normal part of the recovery sequence, all three gyros were recalibrated, and the ACU was activated to make any necessary adjustments using its thrusters. However, when the ACU attempted to correct for the drift bias on the spun down Gyro A, its roll rate reading did not change with thruster firings. The ACU continuously attempted to correct for a perceived (but non-existent) roll attitude error until the actual roll rate increased so significantly that Gyro B's fault detection accurately triggered ESR-6 at 10:35 pm.

Critical Decision Mistake

Again, recovery efforts initiated immediately. It was observed that Gyro B's readings of an excessive roll rate did not agree with Gyro A's nominal reading for the roll rate, but the flight operations crew still failed to notice that Gyro A was not even spinning. Gyro C was not consulted, since it was replaced by Gyro A during ESR. In a rapid decision, the flight operations manager incorrectly concluded that it was Gyro B (and not Gyro A) that was faulty. Gyro B was ordered to be shut down, which also rendered fault detection capability inactive. When control was returned to the ACU for the recalibration sequence of recovery, roll thruster firing resumed and Sun-pointing errors eventually resulted in pitch and yaw thruster firings. This produced unstable spinning of the spacecraft that exceeded allowed limits for a Sun-pointing anomaly and triggered ESR-7 at 12:38 am on June 25. Within minutes, SOHO's attitude diverged beyond control. Power, communications, and telemetry signal were all lost. By 12:43 am, SOHO was officially lost in space.

The Million Mile Rescue

Within hours, investigation teams at both ESA and NASA had been assembled. On June 28 they convened at Goddard Space Flight Center in Greenbelt, MD, to begin recovery efforts. Based on the last few minutes of telemetry, simulations predicted possible trajectories for SOHO indicating that if the spacecraft was not recovered

by mid-November, it would diverge and escape into a solar orbit (Figure 2). By a stroke of good fortune, calculations also indicated that in roughly 90 days the spin of the spacecraft would naturally align the solar arrays with the Sun for about half of a spin period, giving the recovery team the opportunity to regain control over SOHO within the time window. On July 23, combining the Arecibo radio telescope in Puerto Rico with NASA's Deep Space Network in California the team was able to locate the spacecraft's radar echoes and confirm both its location and spin rate.

The flight operations team uplinked commands to SOHO for 12 hours a day, searching for any signs of return communication. On August 3, contact was established. Over the next two months, SOHO was progressively restored to normal operating mode. On September 25, about 90 days after contact was initially lost, SOHO was fully operational. Remarkably, all 12 scientific instruments remained in complete working condition despite having been subjected to temperatures from -120 °C to 100 °C during the 3-month ordeal.

Proximate Cause

The SOHO Mission Interruption Joint ESA/NASA Investigation Board (IB) determined that the mishap was a direct result of ground operations errors and that there were no anomalies on-board the spacecraft itself. Due to critical software errors in the modified gyro command sequence, SOHO's gyros were configured incorrectly, causing the ACU to erroneously fire its thrusters until the spacecraft destabilized. This was exacerbated by a key decision to shut down a gyro believed to be malfunctioning in favor of a gyro that was actually inactive.

Underlying Issues

Lack of Change Control

Modifications to the command sequences were not properly documented, communicated, reviewed, or approved by either ESA or NASA. The MOCR itself was an internal flight operations document only distributed within the team. The only testing performed was by a NASA computer-based simulator that verified each change separately, but not all together. The IB found that there was little done to determine any implications of the changes on overall system reliability. There were no code walkthroughs, no independent reviews, and no hard copies of the command sequences. The filename itself was not updated to reflect that modifications had been made.

"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

The spin status of the gyros was not obvious to ground controllers and allowed roll rate readings to be collected and misinterpreted, even when the gyro was despun. An effective design would have made it inescapably clear whether or not a gyro was spinning.

Failure to Follow Procedures

The ESR safe mode was designed to give flight operations and engineering teams sufficient time to understand problematic anomalies before taking action. SOHO was programmed to store the last three telemetry frames prior to an ESR so that they would be available for examination by ground crews. The operations procedures specifically stated that before attempting a recovery, Gyro A should be confirmed to be spinning and the last three telemetry frames should be analyzed. The SOHO operations team did not take advantage of this design and instead chose to initiate recovery sequences almost immediately after each ESR was triggered without checking either Gyro A's spin status or the telemetry data. If the spin status of Gyro A had been verified according to proper procedures, the operations team would have known that the destabilizing thruster firings were not due to a faulty Gyro B. When Gyro B was spun down, SOHO lost its autonomous fault detection system. Standard procedures require that such a critical action be approved by a Materials Review Board so as to provide a formal review by senior management and engineers before proceeding; however, no such board was ever convened.

Overly Aggressive Task Scheduling

The scientific activities planned for June 24-29 did not allow for contingency time in the schedule. The flight operations team felt that they did not have adequate time to analyze the results of gyro calibrations. Normally, recalibrated gyros were given 12 hours for verification that the drift biases had been corrected before moving forward. But with SOHO, the operational timeline simulations were being implemented in parallel with performance of the actual timeline. Even as operations continued, scientists were debating discrepancies between the results of ESA and NASA simulations as to the feasibility of the "compressed" timeline. The core SOHO team was expected to perform sufficiently without being augmented by additional staff. However, the IB determined that the actual staffing of the project was not commensurate with that originally agreed upon in the ESA/NASA Mission Management Plan. As a result, during the ESRs, key engineers were preparing for upcoming science tasks rather than assisting in the recovery. Recovery efforts were rushed in order to return the spacecraft to performing its science operations as quickly as possible. Ironically, the prioritization of science over spacecraft safety contributed to the loss of science operations for three months and risked the total loss of SOHO.

Inadequate Staffing and Training

The IB stated that the flight operations team had not been provided the necessary training in the details of the SOHO spacecraft design and operations to effectively diagnose and resolve anomalous conditions with the spacecraft. Reasons for this included high turnover of personnel and descoping of roles. For example, the Mission Management Plan required a dedicated NASA project operations director responsible for programmatic matters, overall technical direction to the flight operations team, and interfacing with the ESA technical support manager. This position changed hands five times throughout the mission lifetime (including as recent as three weeks prior to the mishap) and had been descoped to require that only 10% of one NASA individuals' time be dedicated to tracking SOHO operations. Therefore, the flight operations team relied heavily on the only two staff members with comprehensive knowledge of the spacecraft. Unfortunately, neither of these two had any expertise in the programming language used to code the command sequence scripts.

AFTERMATH

The SOHO Mission Interruption Joint ESA/NASA IB released its final report one month prior to the full recovery of the SOHO spacecraft, urging that its recommendations be reviewed before the resumption of normal SOHO operations. The Board called for a review of the change control process by both ESA and NASA, as well as an examination of all past changes made since the SOHO launch. The Board also recommended an immediate audit of all on-going ESA/NASA International Solar Terrestrial Program flight operations, including an independent assessment of the NASA SOHO simulator, to be led by ESA. Overall, the Board cited a lack of clear leadership in handling contingency situations concerning the spacecraft's health and safety.

LESSONS LEARNED FOR NASA

Modifications or updates to procedural scripts should require formal approval before implementation, and the entire script (not just the modification) should be revalidated. Flight critical software must undergo rigorous independent validation and verification. On-off status of equipment should be unmistakably clear.

Operational timelines should be planned and validated before implementation, not in parallel with implementation, with the proper attention and reserve given to contingency planning and safety. Risk-based analyses of operations plans should be performed to determine the appropriate levels of insight and oversight to ensure that risks are adequately recognized and controlled. Tests and simulations should be coordinated as not to conflict with management and operations of real-time, on-orbit events. The health and safety of a spacecraft are critical in achieving any scientific or operational goals.

Staffing levels should be assessed, strengthened as required, and provide the capability for surge support to contingency operations. This can be difficult in extended operations that may have limited budget flexibility. But operations teams must be well trained on the systems they will be required to use and should practice emergency and off-nominal situations. Management should be prepared for team turnover and ensure that all staff has the appropriate knowledge needed for successful operations.

Questions for Discussion

- Are all changes or modifications documented, reviewed, and approved by a clear authority?
- When working with others, do you feel that everyone's roles and responsibilities are clearly delineated? Are staff fully trained?
- Are staffing levels adequate to meet schedule demands without sacrificing formal procedures? Do you have adequate surge support capabilities?
- How are priorities set in contingency situations? Are they risk based? Do they circumvent formal procedures?

References:

ESA Bulletin 97 – SOHO's Recovery – "An Unprecedented Success Story", March 1999, http://sohowww.nascom.nasa.gov /operations/Recovery/vandenbu.pdf

Final Report – Joint NASA/ESA Investigation Board, SOHO Mission Interruption, August 31, 1998, http://umbra.nascom.nasa.gov/soho/SOHO_final_report

NASA Public Lesson Learned 0664, SOHO Mission Interruption, December 01, 1999, http://www.nasa.gov/ offices/oce/llis/0664.html

"Evaluating Accident Models Using Recent Aerospace Accidents" – Nancy Leveson, June 25, 2001, http://csel.eng.ohio-state.edu/woods/accident_reports/NASA/ leveson_soho.pdf

Artist rendition of the SOHO spacecraft [Online Image], http:// www.exploratorium.edu/eclipse/cme_images/soho_30x.jpg

SYSTEM FAILURE CASE STUDIES
A product of the NASA Safety Center

Executive Editor: Steve Wander stephen.m.wander@nasa.gov
Developed by: ARES Corporation

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