National Aeronautics and Space Administration

SYSTEM FAILURE CASE STUDIES

FEBRUARY 2009 VOLUME 3 ISSUE 2

Cover Blown

Launched on March 4, 1999, the Wide-Field Infrared Explorer (WIRE) carried an infrared telescope that was meant to study the formation and evolution of galaxies. To prevent the satellite's heat from interfering with faint infrared signals, the telescope was stored in a cryostat cooled by tanks of frozen hydrogen. Approximately twenty minutes after WIRE separated from its launch vehicle, a transient electronic signal released the cryostat cover, exposing the hydrogen tanks to heat from the sun and earth. The hydrogen sublimated and escaped through the vents, sending the spacecraft into an uncontrolled spin. In less than thirty-six hours, the entire four-month supply of solid hydrogen needed to cool the telescope's infrared sensors was gone. The mission ended in failure just four days after launch.

BACKGROUND

The Wide-Field Infrared Explorer (WIRE) was part of NASA's Small Explorer Program (SMEX). Its primary mission was to spend four months surveying the sky with its infrared telescope. Scientists hoped to use data WIRE collected to measure starburst galaxy growth rates and gain a better understanding of how these galaxies form and evolve.

To ensure that heat from the telescope itself did not interfere with the faint infrared signals the sensors were trying to detect, the entire instrument was encased in a cryostat lined with two tanks of frozen hydrogen (Figure 1). The larger tank operated at 12 degrees Kelvin (K) to provide shielding for the primary tank, which kept the infrared detectors below 7 K. The telescope and interior of the cryostat were protected by a cryostat cover that would be released after WIRE was properly oriented and ready to begin its infrared survey (Figures 2 and 3).

WIRE's designers anticipated that the satellite would absorb some heat during launch. To let this heat escape, WIRE was to open vents for both hydrogen tanks soon after the satellite was in orbit. The cryostat cover was to be released later in the mission.

A pyro electronics box—or "pyro box"—controlled the pyrotechnics that would open the vents and later jettison the cryostat cover. Components within the pyro box had variable power on (rise) times; these fraction-of-a-second times increased as the time the pyro box components remained unpowered also increased. Until all of these components were fully powered on, pyro box outputs were unpredictable and not controlled.

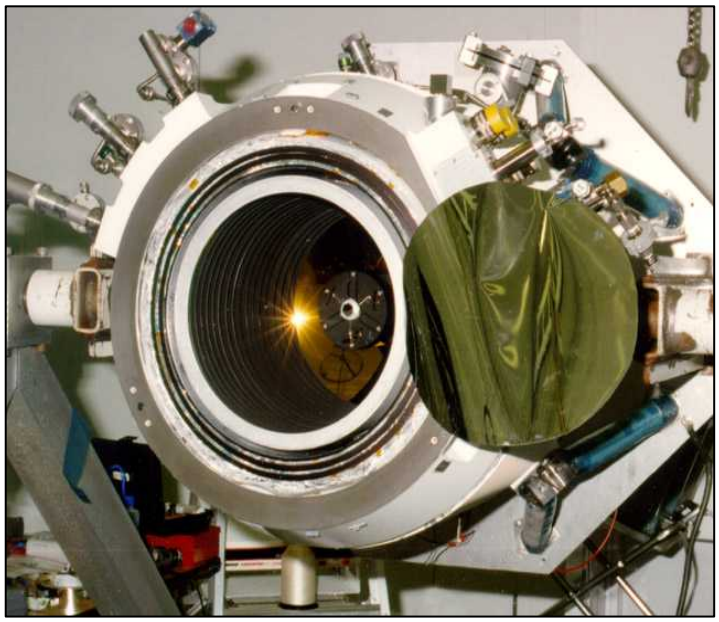

Figure 1: The open cover reveals WIRE's telescope in the center of the cryostat.

WIRE lost its four-month coolant supply within thirty-six hours of launch.

Proximate Cause:

- A transient electronic signal prematurely fired the pyro for the cryostat cover, allowing heat from the sun and earth to sublimate the frozen hydrogen coolant

Underlying Issues:

- The pyro box design did not properly account for the transient start-up characteristics of its components, nor did the attitude control system have appropriate safety margins in its design.
- The pyro box was never peer reviewed, and organizational silos led to insufficient oversight.
- Transient signals during start-up were not recognized during testing because test results were poorly analyzed.

Ground Testing Conditions

In the testing phase, WIRE's pyro box was powered on almost every day, never allowing residual capacitor charges inside to fully bleed off. Prior to launch, however, the pyro box had been powered off for two weeks. Also, ground tests used a power supply with a relatively slow rise time, allowing all devices within the pyro box to power on completely before a full charge was available to ignite the pyrotechnic release charges. In-flight, a relay sent power to the pyro box (and therefore to the release charges) almost instantaneously.

Spacecraft-level tests on the ground used an electro-explosive device (EED) to simulate the pyrotechnic devices that would be used in-flight. The EED had been designed for SAMPEX, the first SMEX mission, and it had been used in ground tests for other SMEX missions before being used for WIRE. It was known to be very sensitive and had a reputation for "false triggers."

Although WIRE's design incorporated elements from previous missions, the pyro design was significantly different from earlier spacecraft. The EED was not modified to address these changes. During WIRE's tests, the EED frequently triggered when the pyro box was powered on, but, because of successful inflight experience from previous missions, the observation team assumed these "false triggers" were test-related only and never communicated them to project management. In fact, otherwise undetected transient signals from the pyro box were triggering the EED during start-up.

What Happened?

Pyrotechnic Misfire

Ground stations monitored WIRE's progress as WIRE's position above the Earth changed, with typical blackouts between stations. As planned, when WIRE made its first pass over McMurdo ground station in Antarctica, about 20 minutes after separation from the launch vehicle, the ground crew up-linked commands to power on the pyro box and then to open the tank vents.

The vents opened successfully, but unknown to the ground crew, at this same time a transient electronic signal was sent to a pyro, releasing the cryostat cover. This cover was designed to shield the telescope and interior of the cryostat and should not have been jettisoned until after the spacecraft was properly oriented.

The spacecraft's spin increased as expected after the ground crew up-linked the commands; however, instead of then decreasing under the guidance of the attitude control system (ACS), spin rates were still increasing as the pass over McMurdo tracking station ended. Ninety minutes after separation, WIRE made its pass over the Poker Flat tracking station in Alaska. The spacecraft's tumble rate was even higher than it had been at the end of the McMurdo pass, and much higher than would have been induced by ejecting the vent covers. The ACS could not control the excessive spin. Tracking stations observed depleting hydrogen levels and increased temperatures in the cryostat over the next station passes.

NORAD tracking data confirmed speculations that the cryostat cover had been accidentally ejected. Without the cover, the interior of the spacecraft had been exposed to heat loads from the sun and earth one hundred times greater than expected. The onboard hydrogen sublimated and rapidly escaped through the open tank vents. The resulting torque spun WIRE up to over 60 revolutions per minute.

On March 5th, just one day after launch, the WIRE Program Executive implemented the pre-drafted contingency plan, acknowledging the inability to keep the telescope cool and shifting the primary objective to regaining control over the spacecraft. Within thirty-six hours of launch, the four-month hydrogen supply was fully depleted. Twelve hours later, the WIRE flight operations team tried to de-spin the spacecraft. The team successfully regained control of the satellite and disabled the infrared telescope seven days after launch.

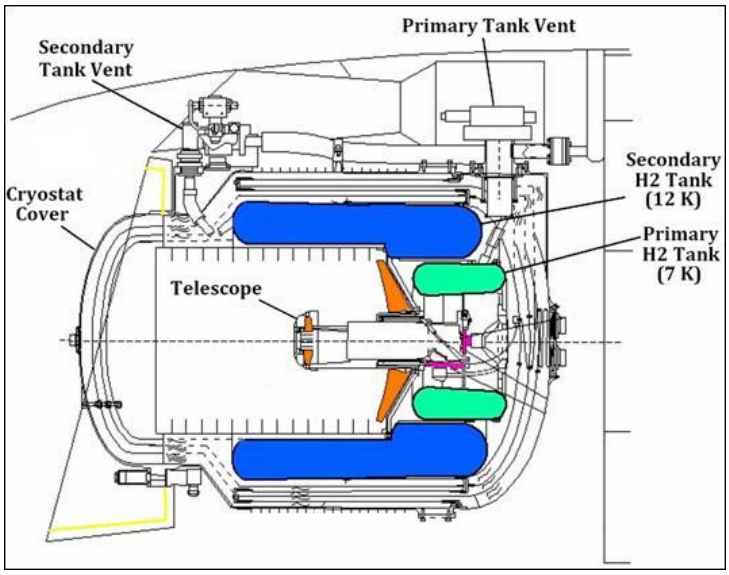

Figure 2: Cutaway of the cryostat showing the cryostat cover protecting the telescope and the two hydrogen tanks.

Proximate Cause

As the pyro box started up, its internal components were in an uncontrolled state for several milliseconds. During this time, a transient electronic signal prematurely fired the pyro and released the cryostat cover. Without its cover, the interior of the cryostat was exposed to heat loads one hundred times larger than anticipated, causing the hydrogen to sublimate. Without the hydrogen coolant, the infrared telescope could no longer distinguish between signal and noise.

Underlying Issues

Failure to Consider Off-Nominal Conditions

Figure 3: WIRE's cryostat cover (gold colored) shields the telescope and hydrogen tanks

The Mishap Investigation Board (MIB) concluded that the design of the pyro box did not adequately account for the transient performance of its components. A lack of documentation contributed to this assumption: one key component in the pyro box had no documentation for its startup characteristics; another component's transient characteristics were included in application notes to its design guide, but not in its device data sheet. WIRE's designers assumed that the various devices in the pyro box would function according to their steady-state characteristics at all times; therefore, nothing was incorporated in the circuitry design to block uncontrolled, transient outputs to the pyrotechnic devices before they were fully functional. Low-fidelity simulations with the EED further masked start-up concerns, burying signals that may have initiated design modifications. After being un-powered for two weeks before launch, the pyro box was highly prone to spurious signals during start-up.

Additionally, the ACS design considered only the cryogen flows expected during the primary mission operations. A member of the WIRE JPL Review Board contended that even the planned tank venting to release heat after launch could have overwhelmed the ACS. This suggested a marginal ACS authority over nominal conditions and minimal design consideration for worst-case scenarios. The Mishap Investigation Board concluded that the hydrogen venting induced by unplanned sublimation produced a torque approximately twice what the ACS was capable of controlling.

Lack of Peer Review

The pyro box design was not reviewed with the other systems because it had not been completed in time for the Systems Design Review. Due to management turnover, there was also no pyro box review during the regular instrument design reviews. The new instrument manager was not informed that a make-up review had to be conducted. The MIB found that a peer review of the pyro box circuitry and design process would have identified the neglected start-up characteristics that caused WIRE's failure.

The organizational structure of the WIRE project team was designed to optimize the respective strengths of different groups, but it ultimately impeded communication and discouraged design and testing reviews. Goddard Space Flight Center (GSFC) had the responsibility for overall mission management, and NASA's Jet Propulsion Lab (JPL) was responsible for instrument development, but Utah State University was the actual contractor in charge of instrument implementation. Professing a motto of "insight, not oversight," teams gave too much deference to the silos of this organizational structure. Out of professional courtesy for each other, neither JPL nor GSFC took the lead in overseeing activities at the other center, particularly concerning oversight of the contractor. As a result, proper peer reviews were never implemented.

"The underlying theme of this mishap is that the ideal models of components do not match their actual behavior."

-WIRE MIB, 1999

Incomplete Test Procedures & Analysis

During spacecraft integration testing for the pyro box, the device simulator responded to transient signals sent to the pyros within 2 milliseconds (msec) of powering-up the device. Without fully analyzing these results, the team attributed the early triggers to shortcomings of the device simulator, which was known to be unreliable for the first 21 msec. Because the pyro box components' start up characteristics depended on time spent powered off, these transients were not observed in immediate retests. During testing, the pyro box was powered on almost every day and there was not enough downtime to produce a transient signal comparable to that experienced on-orbit after two weeks of being powered down. The testing team focused on the simulator issue and failed to make a correlation between the test results and the variable start-up characteristics of the pyro box components.

Tests using a power supply that slowly powered-up the pyro box over 150-200 msec masked the transient signals during start-up. In flight, the box would be powered on by the closure of a relay, but there were no tests conducted with live pyros in this as-flown configuration. Circuit analyses during the failure investigation were able to reproduce the transient signal firing with high fidelity when considering the effects of the time powered off on the start-up characteristics of the pyro box components. The Mishap Investigation Board was able to predict this outcome through proper testing and found that this mishap was not the result of device failure.

Aftermath

The ability to use the telescope as intended was lost, but by May 1999, about a month before the MIB released its final report on the mission loss, WIRE had been converted to

study oscillations in stars with its perfectly functioning star tracker. As early as February 2000, technical journals were publishing papers using data WIRE collected. One of the most notable included the discovery of new oscillations with previously unrecorded amplitudes on the red giant star Alpha Ursae Majoris. By 2004, 14 technical papers had been published using WIRE's data. WIRE operations were moved to Bowie State University in 2004, where WIRE continued to serve as a test bed for science observations, technology experiments, and educational outreach.

For Future NASA Missions

The WIRE failure reminds us to consider all sequences of mission activities, including non-steady-state modes of operation and all start-up or shut-down procedures. We cannot assume that devices will perform according to their designed logic at all times. Device properties during all phases of operation must be well understood and communicated throughout the team. Designs must protect against transient signals being sent from devices in meta-stable or non-deterministic modes. Simulations and tests must be thorough and must specifically check for anomalies during these transitory phases. The fidelity of these tests can be critical in detecting possible failure modes.

Remember to "test as you fly and fly as you test." The EED used in WIRE tests did not adequately mimic the live pyro configuration. Simulations and tests should be conducted in configurations identical to those which will be used in actual operations.

Detailed, independent technical peer reviews should be required by project management and held as often as necessary, with clear definitions to ensure a uniform understanding of the purpose of the review. Experts from each program element should review designs, test programs, and simulator fidelity for critical mission subsystems and components.

WIRE's pyro box was not included in the planned peer review because it was behind schedule; the peer review was never rescheduled because of management turnover. Project management must ensure that action items are tracked to closure. In cases where multiple, complex interfaces exist over major organizational boundaries, greater care and oversight is needed to prevent miscommunication and conflict. Failure modes give no organizational respect or professional courtesy when proven oversight and review controls are bypassed.

Both design and testing must consider off-nominal conditions and worst case scenarios. WIRE's ACS was not designed to counteract any torque from venting beyond what was expected during nominal operations. System and subsystem engineers should build margin into designs to ensure that deviations from expected conditions do not result in mission failure.

Questions for Discussion

- Have you thoroughly considered the transient properties of your system's hardware and software?
- Have you analyzed the potential differences between startup versus operating modes?
- How close is your testing environment to the actual conditions expected during operations?
- Does your project suffer from 'structural secrecy' due to organizational change or barriers?

References:

Everett, David F., et al. *Recovery of the Wife-Field Infrared Explorer Spacecraft*. 14th Annual AIAA/USU Conference on Small Satellites, Session V (Lessons Learned in Success and Failure), August 2000.

NASA Public Lessons Learned 0640, Inadequate Venting Analysis for the WIRE Spacecraft. June 8, 1999, http://www.nasa.gov/offices/oce/llis/0640.html.

Small Explorer WIRE Failure Investigation Report, NASA, May 27, 1999.

WIRE Case Study, Cutaway. [Online Image], NASA APPL, http://www.klabs.org/richcontent/Reports/nasa_wire_lesson.pdf.

WIRE cryostat covered. [Online Images], 1998. http://www.ipac.caltech.edu/wire/indexA.html.

WIRE Mishap Investigation Board Report, NASA, June 8, 1999.

SYSTEM FAILURE CASE STUDIES

NASA SAFETY CENTER

Executive Editor: Steve Lilley steve.k.lilley@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