

Editor's Note: Within an hour after launch, NASA's WIRE (Wide-Field Infrared Explorer) spacecraft prematurely discharged its cryogen, ending the mission. The failure is recounted below (The full NASA report is available online at http://klabs.org/frichcontent/Reports/nasa_wire_lesson.pdf).

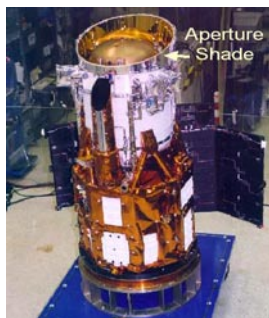
The Loss of WIRE

Summary

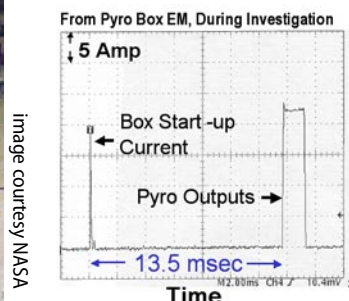
WIRE was launched in March 1999 to survey the galaxies, using a far-infrared sensor cooled by a solid hydrogen cryostat.

To prevent the cryogen from being heated by the Sun, the aperture cover was to be opened only after the satellite had oriented itself properly. The cover design called for its pyro circuits to be "safed" before being sequentially "armed" and "fired."

Unfortunately, a design mistake in the controller chip invalidated all of the inhibition circuits for a few milliseconds upon powering up. All outputs, including "ARM" and "FIRE", were momentarily enabled, and the cover blew open prematurely.



The WIRE Satellite



Transient Demonstration

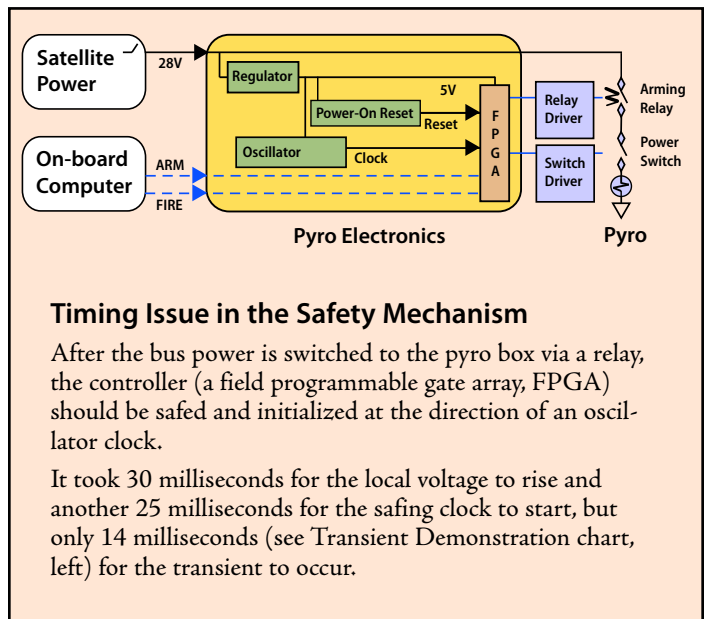
Unforeseen Trouble

The chip could misbehave only after having been turned off for several hours. Although power cycled many times during component testing, it was never unpowered long enough to reveal the problem.

The use of a slow, non-flight-like, power supply during unit testing masked the spurious output—during the transient period there was not enough voltage to close the arming relays. The anomalies repeatedly occurred during later system testing, but because the pyro simulator was very sensitive, a load delay was fitted to the test equipment to filter out spurious triggers, which prevented the start-up glitch from being detected. The warning signs were missed.

Fatal Event Chain

At launch, the chip had been powered down for weeks. Moreover, a fast relay supplied power to the pyro box, sending sufficient voltage to complete the arming circuit. The FIRE switch—commanded by the same controller and therefore not truly independent—set off too, ending the mission.



Timing Issue in the Safety Mechanism

After the bus power is switched to the pyro box via a relay, the controller (a field programmable gate array, FPGA) should be safed and initialized at the direction of an oscillator clock.

It took 30 milliseconds for the local voltage to rise and another 25 milliseconds for the safing clock to start, but only 14 milliseconds (see Transient Demonstration chart, left) for the transient to occur.

Post-mortem

NASA had issued a warning note on this chip, but the contractor and the field engineer from the vendor knew nothing about it. "[We need] an information hotline, set up on an industry-wide lessons learned web page," lamented the engineers later.

Lessons Learned.

- Ensure that sequential safety devices operate independently.
- Beware that many programmable devices do not follow their truth tables at power-on—see <http://www.klabs.org/> for more information.