Failure And Avoiding It In Space Vehicle Mechanisms

Walter Holemans, PSC
Don Gibbons, Lockheed Martin

Virginia Polytechnic Institute and State University
Aerospace and Ocean Engineering Department
Blacksburg, VA

The History of Failure

- 60 years since the advent of ballistic missiles and 42 years since the first successful launch of an artificial satellite, the reliability of the best launch vehicles and best space vehicles is 19 in 20. The worst organizations experience catastrophic failure in 1 of 2 vehicles.
- The methods to efficiently attain space vehicle reliability are not consistently practiced or not well understood

A Number of Failures Can Be Attributed to Mechanisms and/or the Devices That Control Them.

<table>
<thead>
<tr>
<th>MISSION</th>
<th>MECHANISM FAILURE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Galileo High Gain Antenna</td>
<td>Umbrella like deployable won’t open completely</td>
</tr>
<tr>
<td>Macsat GG-Boom</td>
<td>Fails to deploy</td>
</tr>
<tr>
<td>Inertial Upper Stage articulating nozzle</td>
<td>Sticks in one orientation</td>
</tr>
<tr>
<td>Pegasus Microsat Launch</td>
<td>Interstage separation incomplete</td>
</tr>
<tr>
<td>Pegasus XL HETE/SAC-B Launch</td>
<td>Not enough power to initiate separation system</td>
</tr>
<tr>
<td>Pegasus XL STEP M1 Launch</td>
<td>Incorrect coefficients in Pegasus ACS system</td>
</tr>
<tr>
<td>Pegasus XL STEP M3 Launch</td>
<td>Packing foam precludes complete articulation of nozzle</td>
</tr>
<tr>
<td>Alexis</td>
<td>Deployable solar panel falls off during launch</td>
</tr>
<tr>
<td>Joust Sounding rocket</td>
<td>Tail fin falls off at launch</td>
</tr>
<tr>
<td>CIRRIS (STS P/L bay Experiment)</td>
<td>Telescope cover door won’t open</td>
</tr>
<tr>
<td>GLOMR (STS Gas Can Launch)</td>
<td>Microswitch would not indicate “gas can lid open”</td>
</tr>
<tr>
<td>Athena I GEMSTAR Launch</td>
<td>Fiber optic Gyro connector shorts at low pressure</td>
</tr>
<tr>
<td>STS Tether Experiment</td>
<td>Short in tethered wire</td>
</tr>
<tr>
<td>STS Challenger Disaster</td>
<td>Poor O-ring design or use beyond design limit</td>
</tr>
<tr>
<td>WIRE</td>
<td>Door opens too early, boils off coolant</td>
</tr>
<tr>
<td>Lewis and Clementine</td>
<td>Thruster fires inappropriately</td>
</tr>
</tbody>
</table>

Failure Commonalities

- All of the failures had several things in common
  - Easily tested and prevented
  - Very simple component causes complete failure or major degradation of performance
- Several of the missions had zero reliability -- they would always fail
- Most failures occurred during first attempted use of mechanism
- Several failures are the result of software operating the mechanism incorrectly
  - Building a system of high reliability subsystems (thruster) and (software) may not necessarily lead to full system (thruster and software) reliability
Everpresent fear of failure

“Because engineers were uncertain whether a device intended to dampen the force of the antenna deployment would work correctly, they used the antenna in its stowed configuration for the first three weeks of mapping. This allowed the team to meet the mission’s minimum science objectives before attempting deployment.”

*Space News* reporting on Mars Global Surveyor, April 12, 1999

- Engineers may not have known how the deployable might fail, but they suspected it was a significant probability
  - Why were the engineers unwilling or incapable of finding all failure modes before flight?
  - Was an unreliable vehicle knowingly launched?
- Did not using the mechanism increase reliability?
  - Could they have avoided the use of the mechanism entirely?

How Do You Know a Mechanism Is As Reliable As Intended?

By testing it

There Are Several Best Practices To Yield Reliable Mechanisms And Space Systems

- **K.I.S.S.** — Keep It Simple Stupid
  - Minimize quantity and magnitude of functional requirements
    - Better to have a reliable device of limited utility than a high performance device of low reliability
  - Minimize required modes of operation
    - Deployables
    - ACS
    - Thermal environment
    - Software
  - Add “redundant components” with great caution
    - Better to make the single unit more reliable than to duplicate a questionable one
    - Two “redundant components” may require a third component to arbitrate!
  - Ruthlessly discard all unnecessary hardware or function
  - Define requirements in greatest detail as early as possible
    - Everything
- Avoid use of mechanisms unless you absolutely have no other choice because:
  - Reliable mechanisms will cost 10 to 50 times more per pound than equivalent function static structures
  - Unreliable mechanisms cost even more!

The Case For K.I.S.S. : Two Satellite Builders’ First Satellite

- DSI, 1986, Builds first satellite—GLOMR, store and forward com. sat. demonstration
  - 180 lb STS Gas can launched
  - No Moving parts (except separation system which NASA supplied)
  - 5 W orbit average power (OAP)
  - No ACS torquers or sensors
  - Mostly industrial electronics housed in cast 1/2 thick walled, pressurized brass sphere
  - $1M, ~18 months to build
    - **RESULT:** Success, customer orders second, DSI leverages success to win more satellite contracts
- AeroAstro, 1990 builds first satellite—Alexis, multi-spectral physics experiment
  - ~180 lb
  - Many mechanisms: 4 deploying solar arrays, several optical covers
  - ACS: Spin Stabilized, Torque rods, other sensors
  - OAP Power > 20 W
  - $5 - $10 M, ~36 Months to build
    - **RESULT:** Initial catastrophic failure-solar array falls off during launch, unable to communicate with SC for weeks, major effort to redesign mission while on orbit

**SUMMARY:** simple systems are easier to make reliable than complex ones—there are fewer ways to fail and less things to test.
...More Best Practices

- Design for terrestrial testing, not just for flight
  - Design test plans to exceed all flight environments
  - Celebrate the failure of a device to pass a test
- Do not bother to design, build or launch devices you cannot or will not test many times
  - As a subsystem alone and as part of the complete system
  - No test = gambling
  - Ideally, test in environments known to be duplicates of flight
    - If you cannot test the whole thing, test as much as possible and use analytical techniques to extrapolate test data to full system behavior
    - Untested analytical models = speculation (gambling)
  - Choose designs that can be tested most completely
  - All unexpected operational failures are due to incomplete testing prior to intended use
- Prototype everything including ground test and support hardware
  - Count on being wrong about at least one major assumption in your design
  - Learn as much as you can
    - Look for and fix all the weaknesses, even ones that don’t cause failure