ISHEM 2005 Papers
First International Forum on Integrated System Health Engineering and Management in Aerospace

November 7-10, 2005
Napa, California, USA

ISHEM Sponsored by
NASA Ames Research Center
NASA Marshall Space Flight Center

Corporate Sponsors
ATK Thiokol
Boeing
Gormley and Associates
Pratt & Whitney Rocketdyne
Qualtech Systems, Inc.
From Data Collection to Lessons Learned
Space Failure Information Exploitation at The Aerospace Corporation

Jonathan F. Binkley, Paul G. Cheng, Patrick L. Smith, and William F. Tosney
The Aerospace Corporation
Los Angeles, CA 90009

ABSTRACT
The Aerospace Corporation extracts lessons learned from launch vehicle and satellite anomalies to help the space community avoid repetition of mishaps. Incorporated in reports to industry, program reviews, and journal publications, the lessons lend themselves to influence new acquisition guidelines and military specifications. Government and the commercial space communities, which share a common interest in quality improvement, should work together to establish more comprehensive and effective approaches to developing and disseminating lessons learned.

A “One Strike You’re Out” Environment

“Space is unforgiving; thousands of good decisions can be undone by a single engineering flaw or workmanship error, and these flaws and errors can result in catastrophe,” observed the Defense Science Board (Defense Science Board 2003). Indeed, despite many years of experience, so many accidents still occur (Frost and Sullivan 2004) that insurance rates for commercial satellites approach 25% (Aviation Week 2003, Aviation Week 2005).

Consequently insights from past anomalies are of considerable interest to many stakeholders. Acquisition policy makers, design engineers, risk assessment specialists, and quality assurance managers seek answers to many questions: What types of components are the most trouble-prone? What is the cost/benefit ratio of redundancy? What is an acceptable tradeoff between newer technology and manufacturing maturity? Which environmental tests are the most perceptive? Why do satellites fail despite extensive verification efforts?

The Aerospace Corporation’s Space System Engineering Database
The Aerospace Corporation operates a Federally Funded Research and Development Center for the United States Air Force, providing objective assessments for National Security Space (NSS) programs. The Corporation is directly accountable for many oversight functions necessary to ensure NSS mission success. Prior to any launch, Aerospace provides a letter to its NSS customer confirming the mission’s readiness as concluded by a rigorous assessment that draws upon the collective expertise of a cadre of engineers with expertise in a wide variety of disciplines. Aerospace has
applied this process to several hundred launches, reducing risks (as compared with commercial launch programs for the first three flights) tenfold.

To assist the Air Force and its other customers in the conception, design, acquisition, and operation of space systems, The Aerospace Corporation began developing the Space Systems Engineering Database (SSED) in 1992 to acquire and manage validated technical information, primarily on NSS systems and programs (Tosney 1992, Tosney 1993). Figure 1 shows the SSED architecture.*

![Figure 1. Architectures of the SSED and Salient Features of its Anomaly Domain](image)

**Anomaly Data Collection**

The SSED archives anomaly and discrepancy reports, primarily from NSS programs, including information on over 20,000 launch vehicle and satellite anomalies that occurred in the factory, at the launch site, during flight, or in operation. Most of these anomalies are routine test and operational

---

* Other organizations have established databases similar to the SSED. For the European counterpart of the SSED, see (Messidoro 2005).
problems. System-level satellite tests, for example, typically generate dozens of discrepancy reports; even successful launches are marred by scores of anomalous telemetry readings. Major anomalies result in exhaustive investigations, many of which are thoroughly documented in the SSED.

The SSED contains less information on anomalies occurring on civil, commercial, and foreign programs. Thorough reports of commercial U.S. launch failures are usually available to The Aerospace Corporation because the same launchers are used by NSS programs. Many reports of NASA satellite failure reports are also available. The Aerospace Corporation has even found a few Japanese and Russian failure investigation reports and had them translated into English. However, compared to the air transport industry, the space community is tight-lipped about failures: Root causes of failures—even the presence of defects—in commercial satellites are routinely not disclosed (Space News 2005). The SSED’s collection of anomaly information is therefore far from complete.

**Anomaly Data Archiving and Retrieval**

The anomaly information in the SSED is organized in a relational database that allows cross-program retrieval and analysis of anomalies by unit, subsystem, contractor, and many other categories including the severity and impact on the mission. Supporting anomaly documentation from contractors and failure investigations is digitized and annotated with extensive metadata. Over 100,000 documents of various types have been archived; all can be searched via a web interface.

The SSED anomaly data has supported a wide variety of studies (Arnheim 2005, Tosney 1997, Tosney 2001a, Tosney 2001b, Wendler 2003, White 2002). Here’s a hypothetical example showing how the SSED enables component engineers to bore into causes of individual anomalies: An engineer was asked to investigate a Program X reaction wheel that showed signs of impending failure. A database search for “Program X + reaction wheels + anomaly + lubrication” found 18 Program X-specific documents, primarily design packages, test information, and operational reports. With some analysis the engineer determined that the wheel’s performance appeared to be “in-family” for this block of satellites. The engineer also performed a broader search, finding 153 similar documents from other programs. Based on this information, the engineer was able to estimate the likelihood that a second wheel might fail should the first wheel in fact malfunction prematurely.

**Post-Flight Anomaly Analysis**

Engineers at The Aerospace Corporation carefully analyze all off-nominal reports from NSS programs, seeking to identify engineering errors, workmanship escapes, model deficiencies, test inadequacies, defective parts, hostile environments, or other factors that may warrant correction.

For example, all off-nominal telemetry readings from a launch program are logged in the SSED. A technical expert is assigned to account for each anomaly and the reasons why it occurred. Every anomaly investigation is tracked by the program office as part of Aerospace’s flight-readiness verification responsibilities. Fault-management lessons, reliability impacts, and suggested corrective
actions are documented. Fortunately, all operational launches from this program have been successful thus far, bucking the high odds of infant mortalities.

This rigorous “post-flight analysis” tracking procedure is prompted by the expensive lesson from, among others, Defense Support Program (DSP) F-19 which was stranded in the wrong orbit (U. S. Air Force 1999) because the Inertial Upper Stage (IUS) technicians wrapped insulating tape too close to a connector, preventing stage separation.* Afterwards, engineers reviewing the telemetry from previous IUS flights realized that the connector was jammed every time. In fact, seven of the previous flights dodged failure only because the taped connectors were jerked apart when they hit the allowable stops—the flight just before DSP-19 had the narrowest escape. Unfortunately, the warning signs in the telemetry data were not heeded.

Why Do Satellites Fail?

"It's always the simple stuff that kills you........It's not that they are stupid, with all the testing systems everything looked good."  
James Cantrell, Main Engineer for the Skipper Mission

Skipper failed because its solar panels were connected backwards (Associated Press 1996).

Table 1 summarizes the causes of recent U.S. Government satellite failures. Evidently, satellite mishaps are primarily due to preventable engineering mistakes, instead of poor workmanship, defective parts, or an unexpectedly hostile environment. On the other hand, launches typically fail due to production and workmanship defects, though five out of six U.S. unmanned launches failures since 1999 also occurred as a result of engineering errors.

* The thermal tape on the connector plug housing should be wrapped to leave enough clearance so the harness could disengage. Assembly instructions stated that the tape shall be applied “within 0.5 inches of the mounting bracket flange” (instead of, for example, “no closer than 0.5 inches and no farther than 1.0 inch”). Unaware that the parts had to unfasten and thinking that the they should wrap the tapes as tightly as possible, the technicians applied the tapes so close to the flange that the separator jammed.
These failure statistics highlight the challenge faced by the verification and review efforts that precede each mission: Flight items can only be checked and verified against known requirements. But engineering mistakes occur in endless, subtle ways: an overlooked or poorly worded requirement, a unit mix-up, or even a typo. Besides saying that robustness and quality must be “designed in,” how else can one guard against subtle mistakes?

Table 1. U.S. Government Satellite Failures (1990–2002) *

<table>
<thead>
<tr>
<th>Date</th>
<th>Program</th>
<th>Cause</th>
<th>Engineering Mistake</th>
<th>Technology Surprise</th>
</tr>
</thead>
<tbody>
<tr>
<td>04/90</td>
<td>Hubble</td>
<td>A defect in the optical corrector used in manufacturing and in QA misshaped the mirror</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>07/92</td>
<td>TSS-1</td>
<td>Mechanism jammed by a bolt added after I&amp;T</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>09/92</td>
<td>Mars Observer</td>
<td>Corroded braze jammed a regulator, causing an overpressure that breached the propulsion line—parts not qualified for long duration mission/braze not on the vendor materials list</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>08/93</td>
<td>NOAA 13</td>
<td>Charger shorted by a long screw due to low dimensional tolerance and stress imparted by added instrument</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>10/93</td>
<td>Landsat F</td>
<td>Pyrovalve explosion</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>01/94</td>
<td>Clementine</td>
<td>CPU froze, depleting fuel - fault management ineffective</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>05/94</td>
<td>MSTI 2</td>
<td>Micrometeoroid/debris impact or charging</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>12/95</td>
<td>Skipper</td>
<td>Solar array miswired/Test did not ascertain current direction</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>02/96</td>
<td>TSS-1R</td>
<td>Contamination inside the tether caused arcing</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>08/97</td>
<td>Lewis</td>
<td>Power loss—flawed GN&amp;C design/inadequate monitoring</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>10/97</td>
<td>STEP-4</td>
<td>Satellite/launcher resonance caused vibration damage</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>10/98</td>
<td>STEX</td>
<td>Solar array fatigued—analysis run on wrong configuration</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>12/98</td>
<td>MCO</td>
<td>Burned up due to unit mix-up/vulnerable navigation</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>01/99</td>
<td>MPL</td>
<td>Requirement flowdown error shut engine down prematurely</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>03/99</td>
<td>WIRE</td>
<td>Unexpected logic chip start-up transient prematurely fired pyros; inhibit circuit design was flawed</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>08/01</td>
<td>SimpleSat</td>
<td>Transmitter arcing</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>07/02</td>
<td>CONTOUR</td>
<td>Structural failure caused by excessive heating during SRM firing—Plume analysis used to qualify design by similarity was misled by a typo in an AIAA paper</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

Benefits of Learning Lessons

“Fools say that they learn by experience, I prefer to profit by others’ experience.” Otto Bismarck

Smart engineers learn from failures. Consider the Clementine spacecraft. Equipped with an inadequate central processor, Clementine’s on-board computer encountered a series of glitches, all handled without difficulty—until a numeric overflow occurred just at the point when the computer had begun firing the thrusters. A “watchdog timer” algorithm, designed to stop the thrusters from continuously firing, could not execute since the computer had crashed. The fuel was depleted; the mission ended.

Engineers on the Near Earth Asteroid Rendezvous (NEAR) mission grasped a key insight from the Clementine failure: the watchdog function should be hard-wired in case the computer shuts down. As it happened, NEAR later suffered a computer crash similar to Clementine’s. For the next 27 hours, until the computer could be rebooted, NEAR’s thrusters fired thousands of times, but each firing lasted only a fraction of a second before being cut off by the still-operative watchdog timer. NEAR survived (NASA 1999, Lee 2004).

Hurdles to Lesson Learning

To facilitate lesson learning NASA set up an extensive, publicly accessible, lessons learned database. Yet a General Accounting Office (GAO) audit report recently concluded that the NASA initiative has not been effective (GAO 2002). A primary impediment was a reluctance to share failure experiences, the consequence of which can be illustrated by an incident with the Orion rocket: Someone forgot to install a voltage-reduction component into the test meter used to check the motor’s circuit continuity. As a result the rocket accidentally ignited on its horizontal test stand in 1993, killing a Swedish range technician. When details of this accident were eventually made public, spokespersons for two other facilities revealed that they also had inadvertently ignited rockets with the same meter (Casey 2004).

Busy engineers often neglect to research lessons on past projects. The Wide-Field Infrared Explorer (WIRE) mission failed due to an unanticipated start-up quirk of a logic controller. Although the controller start-up behavior was described in the device’s Data Book and NASA’s “Application Notes,” neither the designers nor the vendor’s field engineer knew about the problem. “[We need] an information hotline, set up on an industry-wide lessons learned web page,” WIRE engineers said later (Gibbons 1999).

Even when a lesson is widely known throughout the industry, it may still be overlooked. A Maxus rocket crashed in 1991 because spent hydraulic fluid, which drained at the nozzle exit plane, caught fire. The flame, which was recirculated by external air flow into the aft area, damaged an uninsulated guidance cable, causing the vehicle to veer off course. This incident was widely reported and caused several programs to redesign the fluid drains away from the plume or to add cable insulation. However, one program did not—despite using a very similar thruster vector control system—and its maiden flight subsequently suffered the same type of failure.
Lessons Learned Program: “Driver’s Education” for Space Engineers

The Aerospace Corporation has published a series of “Space Systems Engineering Lessons Learned,” following the GAO’s “storytelling” guidelines and focusing on three questions:

1. Why did the mistake occur? (Usually, some improper engineering practices.)
2. What prevented its detection? (The verification approach was likely flawed.)
3. How was the flaw able to bring down the entire system? (The fault management or redundancy design was probably inadequate.)

Each lesson uses the after-action report to highlight key engineering practices that should have been followed. Thus far, 100 lessons, based on 79 catastrophic failures, 32 major anomalies (such as loss of an instrument), 21 ground problems (such as test damage) and three mission recoveries, have been published and distributed to industry (Cheng 2002). An example is shown below.

A Sample Lesson

A satellite’s bus provides power to the primary receiver (Rx A) via a fuse (①) and to the back-up via a circuit breaker (②). The receiver power was, via an “OR” diode (③), i.e., permitting the downstream circuits to draw current from either receiver), tapped off by two transmitter (Tx)/antenna switches (④) and two commercial grade status indicator relays (⑤) commanded by the flight computer (⑥). The system requirements stated that status indicator relays should receive pulsed commands.

Software documents did not pick up this specification, and a constant voltage was supplied instead. Unit test overlooked the mistake because the test set software correctly drove the relays with pulsed signals. System test should have caught the error because the continuously powered coils drew five extra watts, a considerable amount in a low-power system. Unfortunately, the extra power draw was not noticed.

Thought as not crucial and thus not space qualified, the relays shorted under continuous heating, tripping the circuit breaker and disabling Receiver B. Receiver A, supposedly isolated, also blew the fuse because it was tied to the short via the “OR” diode. The mission ended.

Several lessons can be drawn from this incident, including:

• Ensure that the architecture isolates faults (isolation resistors or downstream fuses could have prevent the system collapse).
• Create a verification matrix and make sure requirements are correctly implemented (the flight software did not met the system requirements).
• Incorporate flight software into test at the earliest opportunity.
• Inspect all test data for trends and “out-of-family” values, even when all values are within expectation. Seek to explain all anomalous data.
• Check for shorting and commercial part usage in failure analysis.
Additional examples include:

- A computer would not boot up in space because low-temperature turn-on drew much larger current than steady-state operation. The current limiter, adapted from another mission, was undersized, and the failure signature during ground tests was not noticed. Lesson: Check start-up behaviors at low temperatures, including fault-tolerance circuits.

- An instrument’s power supply malfunctioned in space. The problem was not caught because the test set supplied backup power. Lesson: Independently confirm performance for functions temporarily provided by test sets.

- A payload was damaged during thermal vacuum testing because the test cable, which was not space-qualified, induced multipaction breakdown. Lesson: Equipment used in simulated space environments must be space-rated.

- A launch failed because during ground software change, part of the code was inadvertently left out. Lesson: Change control processes for software, including ground software, require the same degree of rigor as the original development.

- The reset window of a computer’s start-up watchdog timer was set too short, and the processor could not boot up in space. Lesson: Provide a back-up start mode lest a single parameter error cause infinite looping (for example, after several unsuccessful attempts, the spacecraft should be able to switch to an emergency start mode requiring less system resources but permitting ground intervention).

100 Questions for Technical Review

Failure reports routinely lament “inadequate reviewing.” How can reviewers, in a few hours, find a mistake that has escaped years of design and quality checks by the contractor and program office?

To help reviewers check that designers have not repeated past mistakes, the prescriptive lessons have been recast as “100 Questions for Technical Review,” (Cheng 2005) which are open-ended and must be tailored to particular situations by reviewers based on their expertise. A reviewer earns his pay if just one of these questions gets the response: “You know, we hadn’t thought about that, we better check it!”

Here are some examples:

- Are units and tolerances specified? (This question is based on an incident where a vehicle was damaged because the ground support equipment used a wrong flow rate. Coordination and reviews did not catch the mistake because the requirement only mentioned a “desired” rate.)

- Have all “heritage equipment” test and flight anomalies been resolved? (On several launches a valve stuck open, and the trouble was disregarded because it was survivable. The valve stuck closed in the next launch and the rocket veered off course.)
− Have all critical analyses been placed under configuration control? (Two launches failed because air entered the turbopumps, where it froze and jammed the turbines. The original analysis showing that air could not come in was invalidated by design changes.)

− Has the fault-protection system been independently verified? (A phantom problem spoofed a launcher’s fault-management logic, terminating a flight.)

− How are database parameters verified? (A launch failed because a parameter, manually entered into the avionics database, had a misplaced decimal point.)

− Are handover procedures between two sources of control well defined? (A rocket blew up when ground- and airplane-based command signals contended for control, confusing the self-destruct unit.)

− Are drawing tolerances compatible with manufacturing processes? (A satellite was lost due to a short caused by tolerance stack-up.)

− Have designs been analytically established before testing? (The magnetic torque rods on a satellite were set during test instead of being determined by analysis. Unfortunately the test engineer did not realize the Earth’s Magnetic North pole is in Antarctica and consequently set the phasing wrong. The spacecraft tumbled after deployment.)

**The Way Ahead**

The Aerospace Corporation has prototyped the task of collecting anomaly information and extracting lessons, as described in this paper, as part of its mission assurance responsibilities to its National Security Space customers. To make even greater progress toward improving space system reliability will require cooperation of the space communities.

It is currently difficult to conduct comprehensive cross-program reliability studies and derive experience-based reliability estimates for common space hardware (such as batteries, thrusters, and star trackers), similar to methods used in the nuclear and chemical process industry because detailed design and manufacturing information currently reside in stovepiped contractor databases. To address this challenge, the customers have expressed interest in a system that will task each System Program Office to not only manage and validate their mission assurance data, but also transfer this information to the SSED system for use across the NSS enterprise.

The Aerospace Corporation has proposed an anomaly reporting format along with a series of standards for associated configuration data (Davis 2005). Aerospace is also working on a pilot program toward a centralized, comprehensive database of satellite design, pedigree and anomaly information—a database that contains complete as-built parts lists for all satellites that will, for example, enable potentially defective parts to be quickly and thoroughly identified. Tracking the development and testing history for every major satellite component will allow later anomalies to be correlated to specific manufacturing and testing shortfalls. Data sharing agreements are being developed to allow this information to be centralized, with appropriate protection of contractors’ proprietary information.
Working with the NSS customers, The Aerospace Corporation is also striving to improve its lessons dissemination process, most importantly by directly incorporating them, with sufficient technical depth, into engineering standards, mission assurance handbooks, testing guidelines, and military specifications. Each new specification or standard should be referenced to actual failure histories and lessons learned, to ensure that designers understand why the specification or standard is being promulgated. We hope that this initiative will create a closed-loop learning process that will help avert future mistakes.

Concluding Remarks

The Aerospace Corporation collects space system anomaly information, feeding back lessons learned into programs’ design, review, verification, and acquisition processes. Web, database and document search technologies are being harnessed to improve access to this information. Still, proprietary and stove-piped information barriers remain serious impediments to community-wide information sharing and lesson learning. Government and the commercial space communities must work together to establish more comprehensive and effective approaches toward developing and disseminating lessons learned.

“It has been said that the only thing we learn from history is that we do not learn. But surely we can learn if we have the will to do so.”

Chief Justice Earl Warren

References


