FAILURE IN SPACECRAFT SYSTEMS

INTRODUCTION

Since the early days of the space program, spacecraft reliability has been steadily improving. Failures, when they do occur, also tend to be less significant.[1] There are, of course, some significant exceptions to the trend. Expensive spacecraft have been lost or impaired by single events that escaped detection prior to launch. Yet the overall trend is toward spacecraft that are more reliable and resilient. In large part, this trend is due to improvements in spacecraft components and subsystems and to the fact that the space environment has been characterized with greater accuracy.

In the future, spacecraft failures are expected to continue to decline. This appendix will provide an overview of spacecraft failure causes, examine some important failure trends, and assess the potential impact of a new tool, the *physics-of-failure* approach, in terms of helping to bring about further improvements in the reliability of space systems.

FAILURE IN SPACECRAFT SYSTEMS

Failures that lead to system anomalies and breakdowns are to be expected in any electromechanical system. For terrestrial systems, engineers can often test devices to the point of failure to evaluate a design; when failures occur in service, components can be recovered and studied. In contrast, expensive spacecraft systems are rarely tested to failure. To analyze failures during a mission, engineers must rely on telemetry, ground-test data, and operational analysis. Only rarely can components be recovered. Failure analyses are complemented

[1] A failure is generally considered substantial or significant if it causes a loss of 33 percent or more of the spacecraft's mission objectives.

by measurements of the space environment that aid engineers in the association of cause and effect.

To support the general study of spacecraft failures, data for individual missions are usually compiled in a database. Currently, there are four main repositories of spacecraft failure data: JPL's Payload Flight Anomaly Database (PFAD), NASA GSFC's Spacecraft Orbital Anomaly Report (SOAR), and the Air Force's Orbital Data Acquisition Program (ODAP) and the Space Systems Engineering Database (SSED).[2]

These data repositories provide a valuable historical record, but the task of acquiring and analyzing failure data is complicated by the lack of common reporting schemes and techniques. Procedures vary between NASA field centers, the Air Force, and industry. Even offices within a given organization can apply different techniques. Various organizations also differ in the way they treat failure events. Some choose to capture every event, no matter how minor, while others maintain some reporting threshold. In some reporting systems, a single failure event can have multiple assigned causes. The number of statistical data points may, therefore, exceed the actual number of reported failures. Most often, though, the cause of failure can be attributed to a single failure category.

The lack of commonality in the bookkeeping of failure data hampers the ability of PA engineers to monitor trends and focus research of spacecraft failure mechanisms. Resource-limited small programs have reported finding it difficult to sort through various failure archives to locate relevant information and apply lessons learned from previous missions.

Classifying Failure

Despite various approaches to classifying failure data, it is possible to create broad categories of failure and to review how manifestations of failure have changed over time. For this purpose, failures can be classified as (1) events caused by the space environment, such as radiation damage to circuits; (2) incidents for which some aspect of the design was inadequate; (3) problems with the quality of the spacecraft or of parts used in the design; or (4) a predetermined set of "other" failures, which include operational errors. A significant number of incidents cannot be attributed and are simply classified as "unknown."

It should be noted that failures are not always unexpected events. Mission timelines and cost factors sometimes demand that a spacecraft, such as

[2]The ODAP and SSED databases are maintained for the Air Force by the Aerospace Corporation.

Voyager, be launched with known problems. Engineers rely on robust designs, redundant systems, and prescribed workarounds to deal with anomalies that are deemed likely because they occurred, and were characterized, during ground testing. Depending on the reporting schema, expected problems may or may not be classifieds as failures.

Failures Caused by the Space Environment

The space environment provides an assortment of hazards whose ill effects can range from degraded performance up to catastrophic loss of a spacecraft. Some hazards involve impact destruction of spacecraft components, a particular problem in LEO.[3] Meteoroids, consisting mainly of comet remnants, and orbital debris fall into this category. Orbital debris consists of spent rocket components, launch and deployment fragments, and inactive payloads. The impact of particles weighing less than a gram can severely damage systems; heavier objects can completely destroy a spacecraft. The Russian Kosmos-1275 spacecraft was believed to have been destroyed in 1981 by a direct hit from a large piece of orbiting debris. Recently, the French Cerise satellite was crippled after being hit by debris (David, 1997a, p. 2), while an avoidance maneuver steered the European Radar Satellite (ERS-1) from a collision with the Russiam Cosmos 614 satellite (Selding, 1997, p. 1). Usually, however, very small particles are involved, leading to erosion and degradation of materials. Space Shuttle Orbiter windows are routinely replaced because of orbital debris damage, and erosion and penetration degrade solar-panel performance over time.

Although orbital debris poses a serious threat to manned and unmanned spacecraft, it remains less statistically significant than other environment factors. For LEO spacecraft, the tenuous upper atmosphere generates significant asymmetric drag on a spacecraft, a force that varies with the solar cycle, which must be countered by onboard propulsion systems. Atomic oxygen in the upper atmosphere can also cause serious deterioration of spacecraft materials and coatings.

Variations in solar and albedo radiation lead to a dynamic spacecraft thermal environment. Thermal and radio frequency interference effects are increasingly important in small spacecraft, since smaller volumes increase the sensitivity and susceptibility of parts and equipment to radiated emissions. Smaller spacecraft also tend to operate at higher computational loads than earlier

---

[3]Potential impact damage is a significant concern for low-flying assets, such as the Space Station, and for the LEO communication satellites now being deployed in great number. A recent study concluded that there is a 50-percent chance of a collision within 5 years for large spacecraft constellations; see Glicksman (1996), p. 6.

spacecraft. As a result, they can run hotter and drive temperatures at thermal junctions to critical limits.

Atmospheric influences, atomic oxygen degradation, and the thermal variations, along with the impact of the magnetic and electric fields, are classified as effects of the neutral space environment. Although significant failures have been caused by the neutral environment, a higher percentage have been caused by the plasma and radiation environments.

Ionized gases with energy levels less than 100 KeV are usually identified as plasmas. The plasma environment surrounding the earth varies with altitude and latitude but is also heavily influenced by solar activity. In geosynchronous orbits (GEO), spacecraft are bathed in a low-concentration, high-energy plasma that is highly sensitive to solar storm activity. Spacecraft moving through this plasma environment can accumulate differential charges. Arcing can result, overloading electrical components, or exposing surfaces to further damage. High-energy particles can also penetrate insulating material, causing leakage paths in electrical networks. Spacecraft charging has been a cause of many significant failures, most notably in GEO communication satellites.

The radiation environment is perhaps the most significant in terms of spacecraft failures. The radiation environment is characterized as containing energetic particles (ranging from 100 KeV up to several GeV) that are either trapped by, or passing through, the earth's magnetosphere. This radiation takes the form of cosmic ray particles, solar protons and heavy ions, and fast electrons. These energetic particles readily penetrate a spacecraft's shell, displacing materials at the atomic level. They unusually have an immediate effect if they happen to impact an electronic component.

How radiation affects circuitry depends of the type and energy of the particle. The majority of occurrences involving radiation are single-event upsets (SEUs), which cause a state change, such as a digit being "flipped" from a zero state to a one. Such events are common and not of concern in most circumstances, since error detection and correction (EDAC) software can locate and reverse the event. Another type of event, of considerably greater concern, is the single-event latchup (SEL), which causes a part to draw excessive current until it is shut down. SELs are serious, but cycling the power to a component will usually reset a circuit. Corollary damage can result, however, since the SEL is effectively a short circuit. The temporary short circuit can overload the power supply, or reduce bus voltage, damaging power-sensitive electronics. A third type of failure is the single-event burnout (SEB). An SEB is not recoverable.

The sensitivity of equipment to radiation damage is a particularly important issue in relation to commercial plastic components, which are used extensively in small spacecraft. This is covered in more detail in Appendix D.

Design Failures

Engineers designing spacecraft components now build upon decades of measurement of, and experience in, the space environment. Yet design failures remain a major source of failure. A design failure occurs when the strength of parts or components, purchased or manufactured, proves insufficient to withstand the loads experienced during the mission. If the load experienced was associated with a phenomenon not yet understood, or of a magnitude not yet recorded, the failure is usually assigned to environmental causes. Design failures are, therefore, associated with oversight or error. It is worth noting that there is no category for failures related to the use of new technology. Failure of a new design would fall under the category of a design failure.

Failures Related to Parts and Quality

When a failure occurs in the absence of unexpected environmental loads or a clear design error, it is usually classified as being caused by a quality or parts problem. Parts failures usually occur randomly. Spacecraft rarely carry sufficient instrumentation to identify the failure of a discrete part. Instead, a component or collection of parts is identified as the source of failure. Failures related to quality occur when similar parts have repeated problems or when a ground test reveals weaknesses in a representative sample of similar parts. Failures caused by incomplete testing, or induced by testing, are also classified as related to quality.

It is important to realize that component reliability data often assume ideal handling and processing. In commercial settings, components are sometimes never touched by human hands. Entire systems are assembled by automated processing equipment. Spacecraft applications remain custom in the sense that human technicians handle parts and components throughout the process. The effects of part handling and processing on manufacturer predictions of reliability are not well understood.

Other Types of Failures

Many failures can be traced to a variety of other events. Operational errors account for some reported failures. These events are usually related to human error, in which a ground operator issues a command that overloads a spacecraft system or component or exposes sensors or instruments to out-of-bound conditions. Many anomaly databases classify normal aging, wear, or depletion of consumables as a failure. Software-related problems are also classified as “other” failures.

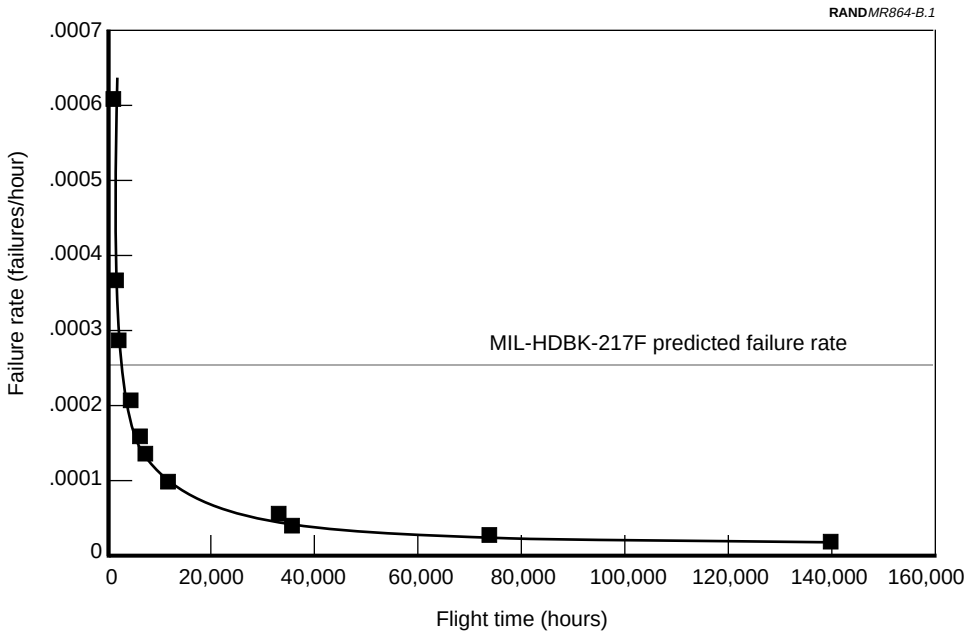
Spacecraft Failures Over Time

Unlike in terrestrial systems, where strain and wear cause failure rate to be a linear function of time, spacecraft failure rates diminish over time. This relationship, a Weibull distribution, is shown in Figure B.1, where the average number of failures reported annually for a given spacecraft decreases.

Analyses that do not account for the relationship shown in Figure B.1 will usually produce overly pessimistic reliability and lifetime estimates. A pessimistic reliability estimate can lead to additional design effort and biased performance trades. This may lead to a more robust design and ultimately to a more reliable spacecraft—which is not always desirable, because additional design efforts usually increase TMC.

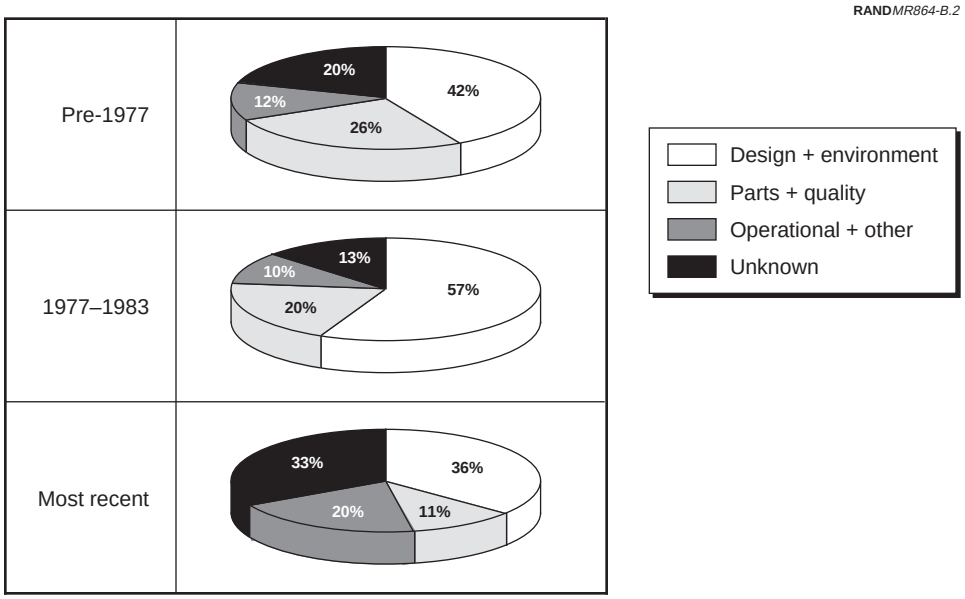
Spacecraft Failure Trends

The categories outlined above are sufficiently common among failure databases to get an idea of where spacecraft reliability is headed. These categories are used in Figure B.2 to draw some high-level conclusions about failure.



SOURCE: Krasich (1995), p. 3.

Figure B.1—Decreasing Rate of Failure with Time on Orbit—Voyager Spacecraft



NOTE: This chart excludes data from the SAMPEX mission.

SOURCES: Pre- and 1977–1983 data, Hecht et al. (1985), p. 47; most recent data, Remez et al. (1996), p. 33.

Figure B.2—Spacecraft Failure Trends

Design and environment causes continue to be the most significant sources of failure. The reductions shown in the most recent data are possibly due to improved design techniques and the use of more refined environmental models. Yet the fact that design and environment factors remain the largest single cause of spacecraft failure is alarming. Failures caused by attributes of the space environment that have been documented and characterized are usually classified as design failures. Since our knowledge of the space environment has steadily improved, it can be presumed that mistakes, or insufficient design margins, are a major barrier to further reducing failure rates. Another recent estimate placed design errors at the top of the list of spacecraft failure causes. (Fleeter, 1997a, p. 14.) Design errors are also predominant in failures that occur prior to launch. A recent review of planetary spacecraft noted that 60 percent of the failures that occurred during test and integration could be traced to design problems. (Gindorf, et al., 1994c, p. 12.)

Parts have traditionally been viewed as the source of failure in spacecraft systems. In the early years of the space program, this was indeed the case, mainly because of quality and reliability problems with evolving microelectronics. Yet recent data clearly show that parts and quality factors are the minor constituent

of spacecraft failures. These data are corroborated by other studies. An analysis of failures in aircraft avionics conducted in 1971 found that 50 percent could be traced to part failures. A similar study conducted in 1990 found part failures to be negligible. (Pecht et al., 1992, p. 1161.)

Scientific investigations of failure mechanisms have revealed that many claims of part failure can be more accurately associated with inadequacies in design or improper handling of components. A recent JPL study reviewed parts-related failures in the Viking, Voyager, Magellan, and Galileo spacecraft. Only 27 failure reports for these missions could be traced to problems with parts, and all but eight were later attributed to design or test deficiencies. None of the parts-related problems were considered serious, although redundant systems prevented an escalation of the problem in seven of the cases. (Gonzalez, 1996b.)

Since the category "other" contains normal wear and old-age events, one would expect this percentage to grow over time. The lower percentage in the 1977–1983 period is possibly due to spacecraft beginning to live longer in this reporting period and to the use of more-sophisticated ground control techniques, which reduced the number of operator-induced failures.

Failure Effects

Another aspect of spacecraft failure data is the severity of failures when they do occur. Figure B.3 depicts the trend in reported failures. The "pre-1977" and "1977 to 1983" data were based on a long-term study of approximately 300 spacecraft. Approximately 36 percent of the early failures were significant; in the 1977 to 1983 sample, the ratio had dropped to 19 percent.[4] A recent study by the NASA Goddard Space Flight Center of 21 spacecraft revealed only 112 anomaly reports with only three significant incidents.[5] (Remez et al., 1996.)

Properly designed spacecraft systems can withstand a myriad of component failures and operating anomalies without suffering a significant loss in performance. The Voyager 1 and 2 missions are among the most notable examples. The Voyager program, widely recognized as a hallmark in planetary exploration, dealt with many component problems throughout its long flight history. (Gonzalez, 1996b.)

---

[4]Both the pre-1977 and the 1977–1983 data are presented in Hecht et al. (1988), p. 14.

[5]The 112 reported incidents exclude an additional 100 incidents from the Small Explorer SAMPEX spacecraft. The SAMPEX data are excluded because the Small Explorer program collects failure-mode data in a form different from other GSFC offices.

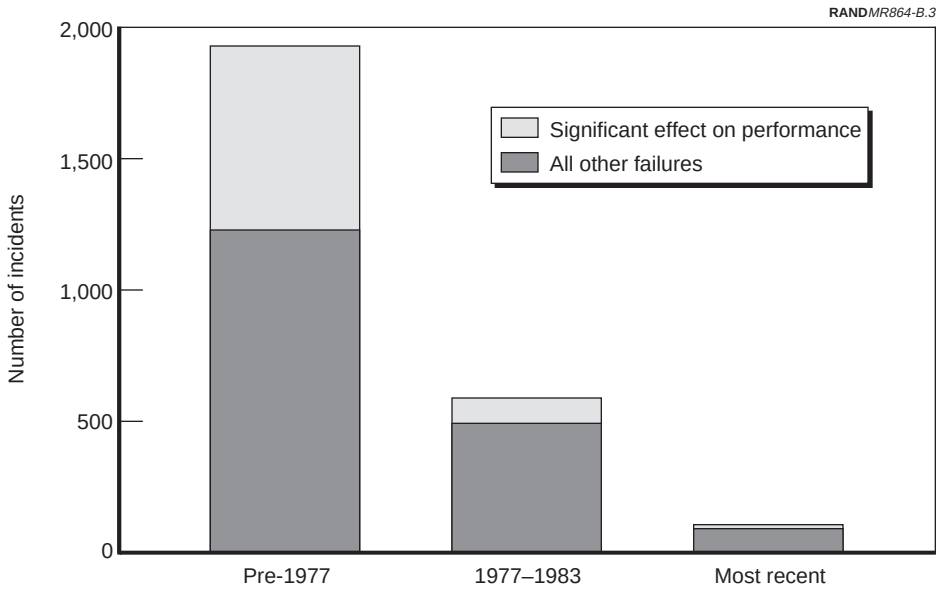


Figure B.3—Decreasing Severity of Failures

Failure in Mechanical Systems

In terms of failures onboard spacecraft, perhaps the area of greatest concern is the performance of mechanical systems. The performance and reliability of electrical and electronic components have improved dramatically in recent years. The design and development of mechanical systems, however, have not advanced in parallel. Many of the most serious recent spacecraft anomalies can be traced to mechanical system failures, as outlined in Table B.1.

Table B.1

Examples of Mechanical Failures in Recent Spacecraft

Mission	Event	Impact	Likely Failure Mode
Mars Observer	Propulsion system failure	Loss of Spacecraft	Leakage and ignition of hypergolic propellants—rupture of high-pressure lines
Galileo	Stuck high-gain antenna	Degraded performance	Excessive friction due to misalignment in antenna restraint pins
Alexis	Damaged solar array	Degraded performance	Attachment bracket broke free after deployment
Mars Global Surveyor	Failure to latch solar array	Modification of flight plan	Structural failure of solar array damper arm attach fitting

Compared to electrical and electronic systems, mechanical systems are usually nonredundant; when they fail, there is greater likelihood of loss of function or catastrophic failure. (Oberhettinger, 1994, pp. 16–24.) Mechanical systems are unique in that

- They are frequently first-time applications that often lack heritage.
- Repetitive testing is often difficult or impossible, as in the case of pyrotechnic devices.
- It is more difficult to conduct environmental testing that recreates the forces a mechanical design will experience in space. Testing in a one-g environment can stress devices past the design point, possibly inducing failures during operation.
- Long periods of storage or transit in space often precede their use. Mechanical systems can lose lubricant or gather corrosion that leads to later failure.

One method of avoiding failure in mechanical systems is to avoid using them. Future missions will likely require more complex mechanical systems, however, so avoidance will not be a reasonable approach for most missions. Advanced mission concepts, like deployable structures, will require miniature mechanical devices that are both reliable and precise. Improving the reliability of mechanical systems remains, therefore, a high-priority item.

RESEARCHING FAILURE MECHANISMS—THE PHYSICS-OF-FAILURE APPROACH

In the modern marketplace, quality and reliability are more closely related than ever before. To remain competitive, product manufacturers have applied ever more stringent quality standards, enabling them to deliver higher-reliability devices.

Underlying the drive for better quality and reliability is a shift from empirical understandings of failure mechanisms to a more scientific approach. The *physics-of-failure* approach applies reliability models, built from exhaustive failure analysis and analytical modeling, to environments in which empirical models have long been the rule. (See Pecht, 1996b, and Stadterman et al., 1996.)

Scientific approaches to failure are certainly not new. The physics-of-failure approach embodies techniques well known to structural engineers responsible for building large structures—only one unit is built, and a failure would mean significant loss of life and property. The central advantage of the physics-of-

failure approach is that it provides a foundation upon which to *predict* how a new design will behave under given conditions, an appealing feature for small spacecraft engineers.

In terrestrial applications, the physics-of-failure approach has helped to increase design confidence and boost quality and reliability, perhaps most readily demonstrated in the case of microelectronic components. In terms of quality, the defect rate for high-volume electronics, for example, is now so low that traditional methods of acceptance testing make little sense.[6] The process that produces Intel's Pentium® microprocessor, a complex device with fine feature sizes, averages 17 defects per million units produced.[7] Strategies that identify and replicate proven components, such as Known Good Die (KGD) practices, are also reducing defect rates in highly integrated (stacked) electronic components.[8] Reliability improvements are equally impressive. The Pentium® processor has a mean time between failures (MTBF) of 36 million hours. This level of reliability means that the central processing unit (CPU) is unlikely to fail within the normal lifetime of a modern personal computer. The high quality of mass-produced microelectronic components has led the automotive sector to set some of the industry's most stringent qualification standards, with zero allowable rejects (Pecht, 1996c, p. 22).

In space applications, the physics-of-failure approach seeks to augment the traditional postmortem analysis of failure data with an expanded knowledge base of failure mechanisms. Data from physics-of-failure research should help to reduce both failure rates and failure severity, improving the reliability of space components and systems. The physics-of-failure approach could also assist with

- *Application of technology*. More so than in the past, small spacecraft rely on advanced technology for which few historical reliability data are available. The physics-of-failure approach offers a means of evaluating how new designs will operate, based on a more refined understanding of the response of materials and the behavior of analogous systems.

---

[6]Research conducted at Rome Air Force Base's Reliability Analysis Center (RAC) in 1992 concluded that the average failure rate for commercial electronics was approximately 0.02 failures/10^6 hours (see Priore and Farrell, 1992).

[7]Quality data for Intel microelectronics are available at its developer Web site: **http://support.intel.com/oem_developer/**.

[8]Dense electronics, such as the stacking of chips into multichip modules (MCMs), take up less space, require less power, and are easier to integrate than discrete components. These attributes make MCMs very popular among small spacecraft builders. MCMs typically cannot be tested before final fabrication, however, at which point a chip fault requires scrapping the part. To help prevent chip failures, integrated circuit dies that are known to be error free are precertified—the KGD process.

- *Risk mitigation*. Gains in robustness and component reliability translate directly into reduced overall mission risk. Also, an ability to estimate reliability at the part or component level supports improved design optimization of the overall spacecraft.
- *Failure awareness*. The physics-of-failure methodology allows the spacecraft engineer to predict with greater assurance the "first failure" of a given component or design.[9] By creating new tools for predicting performance, the physics-of-failure approach can help spacecraft teams focus on aspects of failure analysis early in the design process.

The study of failure physics, like any other scientific discipline, requires testing to validate hypotheses and gather data on failure mechanisms. A significant amount of research can be conducted on the ground, but some amount of space-based research will likely be necessary. Physics-of-failure research will likely make extensive use of low-cost "time-in-space" facilities, such as Shuttle-deployed free-flying spacecraft. Inexpensive long-duration missions might allow data to be gathered on actual performance in space, with components being returned to earth for analysis.

IMPLICATIONS FOR FUTURE SPACECRAFT

As discussed above, spacecraft have been steadily becoming more reliable. Discounting cases of catastrophic loss, failures have been generally fewer and less likely to affect mission objectives significantly. It is, however, unclear that this trend will continue with the current generation of small spacecraft.

Chapter Two mentioned that one of the consequences of budget reduction and the shift to smaller spacecraft has been a greater willingness to accept risk. Later, Chapter Five described the "risk as a resource" approach, in which risk is treated as a variable in the many engineering trades that are made during the planning and design of a mission. Created from discussions with small spacecraft teams, Table B.2 presents a qualitative assessment of how many of the steps taken to achieve cost reduction affect risk.

Some small spacecraft trends raise the potential for failure, introduce new failure sources, cause failure sources to be overlooked, or reduce the spacecraft's resilience. Perhaps the most obvious example of this is the potential for launch

---

[9]For terrestrial applications, component manufacturers are concerned primarily with the number of failures likely to occur in a given period of time (failures in time or FIT), or the mean time between failures (MTBF). These data are less useful to the spacecraft engineer. For commercial components, increasingly used in small spacecraft, the importance of the problem is elevated, since manufacturers cannot, and often will not, supply the information a spacecraft designer needs to ensure design reliability (see Appendix D).

Table B.2

Risk in Small Spacecraft Programs

Small Spacecraft Strategy	Manifestations	Risk of Failure
Simplified design	Rescoping mission requirements	Neutral
	Design reuse	Decrease
	Reduced redundancy	Increase
	Mainly incremental improvements	Neutral
	Use of commercial plastic-encapsulated electronic parts	Increase
Streamlined test procedures	Test at higher level of integration	Increase
	Reduced test plans	Increase
Reduced procurement oversight	PI-mode management	Neutral
	Performance-based contracting	Neutral
Other attributes	Smaller teams	Increase
	Small launch vehicle	Increase

failure. Small spacecraft operate in a weight class in which there is a significant risk of failure associated with the launcher. Of the four Air Force STEP spacecraft that have been completed, two have been lost due to launch failures. Several new small launch systems are currently being developed, but it is unlikely that they will be able to demonstrate near-term reliability.[10]

Lengthy launch delays can also introduce sources of failure. Unplanned periods of dormancy can lead to such failure-inducing situations as lubricant loss, the introduction of corrosion, or the loss of battery potency.[11] Small programs are particularly susceptible, since funds may not be available for adequate retesting prior to a delayed launch.

Another area where failure could place smaller spacecraft at greater risk is the use of redundant systems. Failures do not necessarily place mission objectives in jeopardy if backup systems are available or if the spacecraft design is sufficiently flexible to allow workarounds. Historically, redundancy has been a central method of achieving resistance to failure and has been incorporated up to the point at which the incremental costs of including it began to exceed reductions in the cost of failure.

[10]Historically, it has taken an average of 57 flights for a new launch system to reach a sustained reliability of better than 75 percent; see Chow (1993), p. 44.

[11]The effects of dormancy on component degradation were studied extensively under the Spacecraft Aging Study at the Air Force Phillips Laboratory using the P-80 (Teal Ruby) spacecraft, which was built but never flown. Loss of lubricant, which occurred during transportation and dormant storage, is suspected to be a major factor in the failure of the Galileo spacecraft to deploy its high-gain antenna fully.

There is considerable disagreement in the small spacecraft community regarding the use of redundant systems. Many engineers feel that "single-string" systems are inherently reliable because of their simplicity. In general, redundancy increases the complexity of the spacecraft, which is contrary to the notion of reliability through simplicity. Increasing levels of component and device reliability further argue against the need for backup systems. Redundancy is also costly in terms of the resources that must be devoted to backup systems. Redundant systems add mass, consume power, require more wiring, and increase the dimensions of the software used to operate the spacecraft. Cost, however, is the most usually cited reason for limiting the use of redundancy. Many engineers feel that budgets are simply not adequate to consider redundancy in small spacecraft.

Although it adds a financial and technical burden, redundancy has been a critical factor in many successful past missions. As noted above, the Voyager mission experienced many failures, but these were largely countered by redundancy and workarounds. Redundancy has been shown to be especially important in certain systems. The telecommunications system is one example: If ground controllers lose the ability to "talk" to a spacecraft, the potential for in-flight repair or reconfiguration is also lost. A 1994 JPL study of the critical telecommunications system on six prior missions (Voyager 1 and 2, Viking 1 and 2, Galileo, and Magellan) revealed that redundancy likely saved five of these missions from catastrophic failure. (Brown, 1994, p. 14.) The affordability of redundancy, in terms of using it on small spacecraft, is also changing. Discussions with component and subsystem suppliers suggest that the cost of adding redundancy is declining. Several small spacecraft missions (for example, Discovery-NEAR and SSTI-Clark) have taken advantage of these trends and implemented designs that are heavily redundant, within tightly constrained budgets.

Offsetting the higher risk of failure associated with such areas as launch and use of redundancy are trends that promise continued reduction in the number and severity of failures. Spacecraft parts and equipment are expected to continue to become more reliable (a subject covered more thoroughly in Appendix D). Future small spacecraft are likely to rely more heavily upon autonomous systems for fault detection, isolation, and recovery. An early example of this trend is the EDAC software now used extensively to correct automatically for SEU errors. Future autonomous software agents, capable of resolving complex problems and reconfiguring spacecraft systems, have the potential to reduce failure effects significantly. (Man, 1997, p. 4.) Software is usually less capable, however, when it comes to dealing with mechanical failures and might actually increase the consequences of failure if corrective actions are implemented that

impede the ability of ground controllers to intervene. (Oberhettinger et al., 1994, p. 26.)

Management approaches that emphasize "failure awareness" are important elements of efforts to ensure that reliability improvement trends continue. Noteworthy throughout the course of this study was the variation in approaches taken to manage risk in small spacecraft programs. Risk-management approaches often depend on the experience of the most senior engineers on a given team. Reducing this variability is the major goal of NASA OSMA's effort to formalize risk management approaches under the "risk as a resource" theme. Repeating past mistakes has also been a source of frustration for many programs. This has spurred efforts to pass on the experiences of senior managers and engineers to younger spacecraft designers.[12]

Summary

Almost four decades of experience in building spacecraft and measuring the space environment have yielded a refined understanding of how to avoid failure. This experience is reflected in the fact that

- The number of spacecraft failures has been steadily decreasing.
- Failures, when they do occur, are less severe.

Within these trends, however, are some significant areas of concern that could affect continuous improvement in mission performance:

- Design-related failures are playing a more significant role as the total number of failures diminishes.
- Mechanical failures contribute significantly to reduced performance or loss of spacecraft.

These areas deserve special attention in terms of focusing failure-reduction initiatives.

An area of great promise, in terms of understanding failure mechanisms and improving the construction of spacecraft, is the physics-of-failure approach. The goal of this approach is to replace empirical models of failure with more rigorous scientific analyses of how failure occurs in spacecraft components and subsystems. The increasing accuracy of failure models should aid in reducing

[12]NASA GSFC has consolidated past experiences into a Space Engineering Lessons Learned (SELL) database. JPL sponsors a "Common Threads" workshop to relate past experience; see Brown et al. (1996).

the number of design errors and serious mechanical failures. The physics-of-failure approach is also important in terms of helping to predict the performance of new technology and providing new tools that increase an awareness of failure early in the design process.

To assist physics-of-failure initiatives, a greater degree of cooperation between the various organizations collecting and disseminating failure data is needed. The adoption of common recording and reporting formats would assist in the preparation of actuarial data. Funding for joint analysis efforts might be considered with the aim of providing a foundation for improved reliability and longevity estimates.

NASA has adopted a higher-risk approach in shifting to smaller spacecraft. One possible outcome is, in the short-term, a higher rate of failure that would disrupt the trends described above. Yet, as the reliability of small launchers improves, as small spacecraft programs incorporate high reliability systems, and as new design techniques proliferate, it is likely that future small spacecraft will continue the trend toward fewer failures.