RELIABILITY

LESSONS FROM NASA

Design reviews, failure analysis, and redundancy are favored over predictions and life testing for spacecraft success

Spacecraft differ from other products of technology in several critical respects. They are exposed to hostile environments unlike any on earth. They cannot be repaired once they are launched. Production of a particular craft has been limited to one or at most a few models. The designs challenge the state of the art and use the latest hardware, which must be proved for the space environment by thorough testing.

These factors—along with demands for greater accuracy and complexity—have pushed up the cost of spacecraft and have made a high rate of success essential. They have forced the National Aeronautics and Space Administration to take a reliability approach that differs somewhat from that in many earthly endeavors. NASA has found that some of the traditional tools of reliability engineering, such as life testing, reliability demonstration testing, maintainability analysis, and direct failure analysis, are impractical for spacecraft. Some NASA engineers will tell you, "We don't play the numbers game," meaning that NASA's faith is placed largely in engineering failure modes out, rather than relying on statistical predictions based on handbook failure rates.

Reliability pursued on three fronts

In place of a statistical approach, the space agency uses what it refers to as an engineering approach to mission reliability. NASA's philosophy is that reliability is designed in and defects are tested out. Though the missions have different requirements for different functions—satellites that orbit earth, those that travel vast interplanetary distances, and those that carry astronauts—there is a disciplined and coordinated attack against unreliability on three fronts:

1. Application of effective design principles—and the extensive and meticulous reviews of designs.
2. Control and screening of all parts.
3. Testing of the entire spacecraft or its prototype for predicted capabilities.

These three ensure the proper balance of what NASA considers to be the three main ingredients of a reliable spacecraft: design, parts, and workmanship.

The usual analytical methods of reliability engineering, based on parts-failure-rate data and the assumption of constant failure rates, have resulted in unnecessarily pessimistic predictions for spacecraft missions. At the same time the effects of the space environment and the interaction of components of new design cannot be predicted analytically. Hence analytical predictions are likely to miss the most critical failure modes.

Walter C. Williams NASA

On the other hand, because of costs, very little hardware is built beyond that actually flown, so life testing, the other major tool of reliability engineering, is not feasible.

Design is the cornerstone of success

In its threefold attack on unreliability, NASA has found design to be the most critical determinant of spacecraft performance. Half of the causes of component failures in spacecraft cannot be determined, but of those that have been pinpointed by the space agency, 42 percent have been errors in design, 15 percent defective parts, 8 percent faulty workmanship, and 35 percent miscellaneous external causes, such as high radiation particles, spacecraft charging, or depletion of consumable materials.

To an important degree, the ingredients for success or failure can be built into the design of the hardware. The keys are to take every advantage of lessons learned from prior missions; to make the design as simple as possible, consistent with mission objectives; and to use flight-proven hardware and design ideas wherever possible.

Two very valuable design tools used by the space agency are redundancy and analysis of failure modes. The latter is formally called failure-modes effects and criticality analysis (FMECA).

After a spectacularly dismal start, this reliability approach that evolved gradually has been highly successful, in light of the difficulty of the missions. In 1958, its initial year of operation, the NASA record was four failures in four attempts. The following year, 8 of 14 missions were successful. Through the 1960s the record shows 195 successful missions in 246 attempts, or a 79-percent success rate, while in the 1970s, 60 of 66 missions, or 91 percent, were successful. There have been no unsuccessful NASA missions since 1975. The criteria for success differ from mission to mission, but are usually based on achieving the goal set for the mission, landing a man on the moon or gathering data on Mars for a year, for example. In the early years, with the goal of landing men on the moon and returning them safely to earth, the unknown risks of space travel and the prestige of the nation dictated a need to subjugate all objectives to reliability. Cost was secondary. By the time the Apollo program reached its goal in 1969, the overall successes of NASA's spacecraft enabled some unmanned missions to sacrifice reliability to reduce costs. This tradeoff was spurred by inflation and budget cuts.

The successful flight and landing of the Space Shuttle Columbia alters the relationship of reliability to other goals. For the first time, it will be possible to retrieve, repair, and refurbish space hardware. The ability to refurbish and refly is expected to make the more costly payloads, which are generally those most critical to the achievement of national objectives, more cost-effective.

The key step in ensuring reliability is NASA's extensive series

0018-9235/81/1000-0079$00.75©1981 IEEE

of design reviews. These are carried out by the NASA field centers.

The reviews provide a forum for members of the project team to hear and be heard, and they force project members and contractors to rethink the reliability of the system. There may be seven or eight formal reviews. They begin while the project is still being studied and they continue until the spacecraft is launched.

At the Goddard Space Flight Center, where normally 20 or 30 near-earth orbiting projects are concurrently under study, an independent review of projects is also done. Center specialists who are not members of the project team are called on to review the design, thereby introducing a fresh viewpoint and a wider range of experience than is available within the project itself. This type of independent review is not done at other NASA centers, which normally concentrate on one or two long-term projects—for example, the Voyagers at the Jet Propulsion Laboratory and the Space Shuttle at the Johnson Space Center. However, the other centers supplement their project review teams with experts who are not involved with the project.

In its design consideration, NASA has found hardware redundancy extremely valuable. It has helped guard against components containing incipient material or workmanship defects, and it has been a key to the success of a number of missions. On the other hand, redundancy is not a complete defense against systematic defects or generic flaws.

The value of functional redundancy, both in terms of alternative uses of on-board hardware and in flexibility in ground operations, should also not be overlooked. A number of cases can be cited where missions have been saved or extended because of swift actions by ground control personnel. One example is the degradation of the star tracker used for navigation by Voyager 1 on its way to Jupiter and Saturn. The tracker lost its pointing accuracy because of radiation damage during its encounter with Jupiter, and the Saturn part of the mission was saved only when ground personnel "fooled" the Voyager computer by reprogramming one of the spare words in the software to command the tracker to extend its field of view, thus enabling it to lock onto navigational stars.

Failure-mode analysis improves designs

The other extremely valuable tool in incorporating reliability into the basic design of the spacecraft is FMECA. This is a disciplined investigation of possible failure modes and their potential effects on mission performance, ending in a search for better designs. The analysis normally begins when the design effort is initiated, and it is maintained throughout the design process. It is carried out by the design engineer or an engineering support group in conjunction with the reliability engineer.

The analysis serves to document the design process, identifying all credible failure modes of the component level and specifying the effect of the failure mode at the component, subsystem, and system levels. These effects are further identified or classified into a list based on worst-case effect—for example, loss of life or loss of mission. For those hardware failure modes where redesign is not done, extra margins of safety and extensive testing and inspection can justify retaining that aspect of the design.

In the manned programs, with human safety and costly hardware at stake, redundancy is the key to avoiding difficulties. On the other hand, for unmanned earth-orbiting missions and some interplanetary missions, redundancy varies, depending on cost-risk tradeoffs. Some low-cost projects are flown with single-string designs that have no hardware redundancy above the subassembly level. For example, the Stratospheric Aerosol Gas Experiment satellite, a low-cost project, has had battery problems that may cut its life; it has lost 3 of its 21 series-connected cells. If the project had not been low-cost, the satellite would have had a backup battery. Even so, its design life was one year, and it has already been performing its mission for two and a half years at slightly reduced levels.

Two projects with different objectives

Comparisons of two major NASA projects with quite different objectives—the Voyager and the Space Shuttle—illustrate variations in design approaches. The major considerations for the Voyager project were long life, communication time, and limited launch opportunity. For the Shuttle, the avionics subsystems employed redundancy to ensure that they were "fail-operate, fail-safe," which means that no single failure would be able to block mission objectives and no second failure able to have an adverse impact on the crew or flight safety.

Required life in the case of both Voyager spacecraft was more than four years. To meet this, the project laid down rigorous requirements, the most important being low susceptibility to failure, autonomous operation, and an emphasis on proven approaches and simplicity in design.

The requirement for low susceptibility to failure specified that "no single failure shall cause the loss of all data return from more than one science instrument or the loss of more than 50 percent of the engineering data." It meant the extensive use of redundancy on both Voyager spacecraft and the use of proven practices. The redundancy was incorporated at the subsystem level with simple switching from prime to backup [see figure]. This approach, derived from the Mariner-Viking experience, is simple and straightforward, compared with designs where redundancy is incorporated at lower assembly levels.

The redundancy for Voyager was largely to prevent any single electrical, electronic, or electromechanical piece-part failure from having a catastrophic effect on the mission. With redundancy keyed at higher levels, the designers did not provide it within circuits.

Reliance was placed on FMECAs and testing to prove faults would not propagate to the redundant subsystem or elsewhere on the spacecraft. The analyses were largely confined to the interface circuits and conducted at the parts level, and they included the circuits involved in redundancy switching. Since it was determined that failures of electronic parts within a block would most likely cause the entire block to fail, detailed analyses were not performed on designs within a single block.

Autonomous operation enhances Voyager reliability

The Voyager life requirement led to significant advances over Mariner-Viking design practice: extensive use was made of automatic fault-detection and -correction techniques. The simple switching employed in the earlier Mariner was enhanced by centralized redundancy control that leaned heavily on software. It became apparent that a mission dependent on ground command for response to faults would have required an extensive 24-hour-a-day, seven-day-a-week flight team with only marginal capability of responding to potentially catastrophic events during the long round-trip communication time.

Taking advantage of the spacecraft's computer capability, the designers came up with an autonomous on-board fault-detection and -correction scheme. Several spacecraft functions or assemblies—including power systems, receivers, transmitters, exciters in both X- and S-bands, and command and data systems—were made redundant and were also protected by some combination of hardware and software interaction. These protection routines were used in detecting faults and in deciding what action was

needed to correct them.

There were, of necessity, many areas in the Voyager design where redundancy could not be reasonably employed. These included such items as structural and antenna components and instrument deployment mechanisms. Here steps were taken wherever possible to reduce the risks of failure. Piece-part FMECAs were done on all secondary circuits (temperature, references, and so on) to verify that failures would not cause the loss of the primary function.

Significant portions of the Voyager spacecraft used designs from previous spacecraft, largely the Mariner or Viking orbiters. They included the command computer, data storage, modulation-demodulation, Canopus star tracker, and thermal control. Even so, these components were not accepted in blind faith. They were analyzed and tested, and their use helped lower project risk and cost with no performance loss—the best of all combinations.

Shuttle design stresses redundancy

The Space Shuttle's avionics system, on the other hand, comprises a string of four computers, with one backup, and they control the vehicle, its systems, and its flight [see "Shuttle firsts put to the test," *Spectrum*, August 1981, pp. 34-39]. The use of redundant avionics to improve reliability called for redundancy management on board the craft to achieve the desired fault tolerance. In general, the designs followed two processes:

1. Selection—the process of selecting a reading or value from one component or instrument, or averaging a "best" estimate from the whole set of redundant components or instruments to perform the subsystem task.
2. Fault detection—the process of detecting failures and announcing them to the crew or ground, identifying the failed component, and removing it from the selection-detection process.

These processes were implemented in one of the following four places—in hardware, in software, in combinations of hardware and software, or in hardware and software with crew participation. For example, in the Shuttle's flight control system, the redundancy management for the computers and the multiplexor/demultiplexor resided in hardware-software interactions, whereas that for the 10 rate gyros and four accelerometers resided in software only and that for starting the three main engines resided in the hardware of the engines' electronic controllers. The crew was involved in redundancy management in display units and in switching from the four primary computers to the backup [see table].

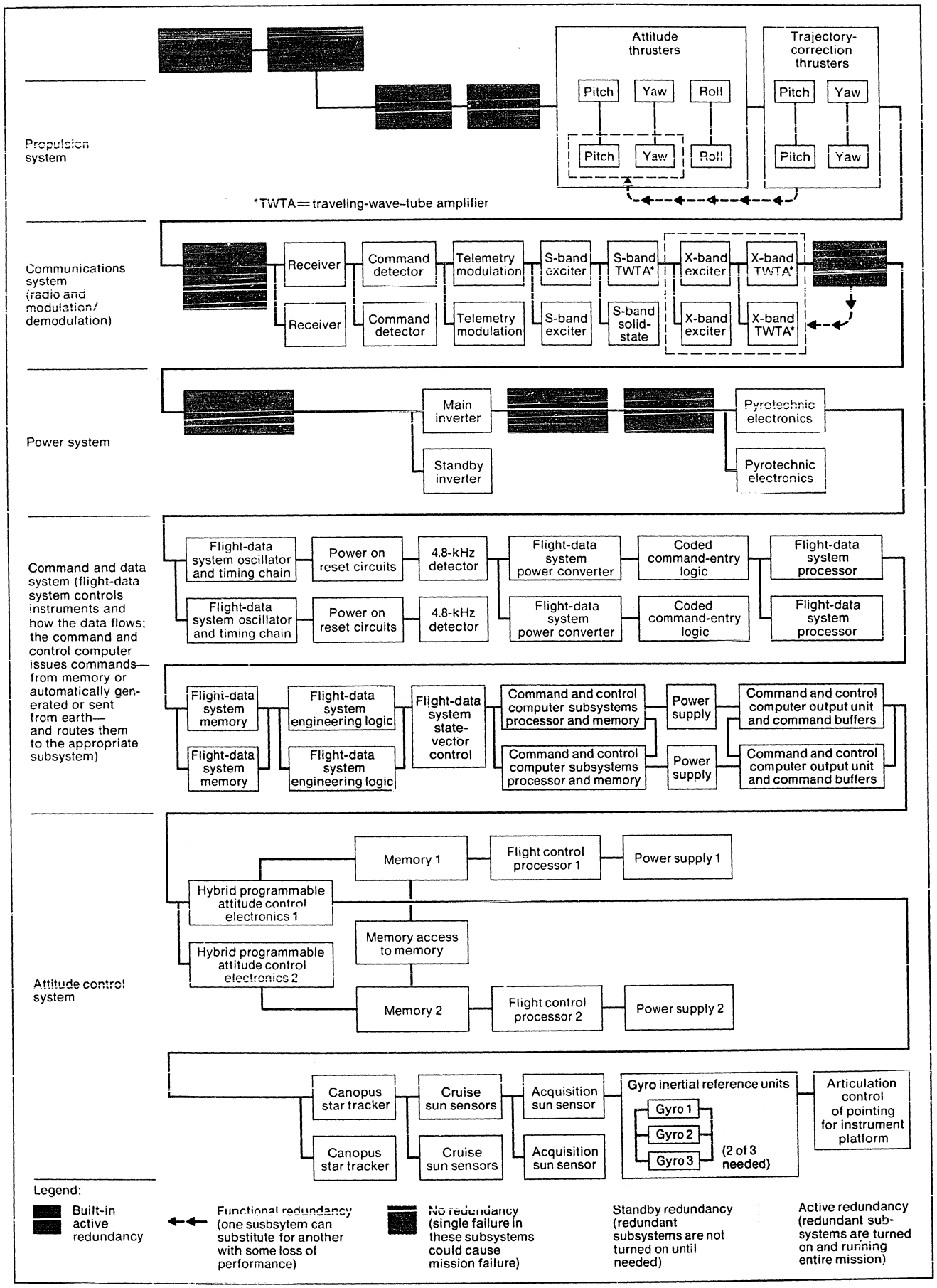
Another example of redundancy in Shuttle design is the avionics software. During critical flight periods (ascent and entry), the data-processing system does parallel processing to discover faults in the data from sensors as well as failures in the data processing itself. This configuration consists of a redundant set of four units performing identical processing.

Each member of the redundant set receives identical data from

Redundant features of representative Space Shuttle avionics systems

System	Number of systems	Redundant features
Flight computer	5 (4 primary, 1 backup)	Avionics software checks computer output words bit for bit with like words from the other computers and checks 500 times each second that computers are synchronized. The hardware itself monitors the bits, spaces, and parity between words. Either the software or the hardware can remove one computer from the set of four primaries. In the event of a second fault, the crew is alerted and may switch manually to the backup. In fact, the crew at any time may switch to the backup.
Instrument multiplexor and demultiplexor	8 (4 for forward instruments, 4 for aft instruments)	Computer software monitors input and output of the multiplexors and demultiplexors and the MDM hardware itself also has self-checking capability for inputs. To get the information necessary for flight, only one of the units forward and one aft are necessary to process the data from instruments.
Main engine electronic interface units	3 (1 for each main engine)	These units give the computers performance information about the orbiter's powerful main engines. If any engine is not performing properly, the computer will turn it off. Using redundant commands from each of the computers, these engine interface units will determine when to turn the engines on. The Shuttle will achieve orbit with two engines running and will abort safely with one engine running.
Rate gyros	10 (4 on the orbiter, 3 on each of the 2 solid-fuel rocket boosters)	The avionics software selects either an average of the gyro readings or just one of them. If a rate gyro is giving a reading the software determines to be faulty, the gyro is not included in the average. If three gyros on the orbiter (or two on each of the boosters) are found to be faulty, the software uses only the one determined to be correct.
Accelerometers	4	As above, the avionics software selects an average of the readings or just one of them, depending on the determination of correctness of the reading.
Orbital engine gimbal driver	4 (2 for each of 2 rockets)	The avionics software determines whether the drivers are operating properly (receiving and responding to commands). However, the software will not remove a faulty driver from operation. Instead the crew is alerted and the switch to the backup must be made manually.
Cathode-ray tubes	4	Hardware has self-checking capability. It alerts crew when performance degrades, and a switch to alternate CRT is made manually.
Rotation control stick	3 sticks and 9 transducers (3 for each axis on each stick)	Avionics software determines selection of transducer readings for each axis of each stick, as well as selection of the stick itself.

Note: The redundancy of the Space Shuttle avionics systems was achieved using multiple pieces of hardware for each one. Systems are monitored by the avionics flight software or by the specific hardware itself. The switch to backups is either automatic or done manually by the orbiter crew upon software or hardware alerts.


Propulsion system
Attitude thrusters
Pitch
Yaw
Roll
Pitch
Yaw
Roll
Trajectory-correction thrusters
Pitch
Yaw
Pitch
Yaw
*TWTA=traveling-wave-tube amplifier
Communications system (radio and modulation/demodulation)
Receiver
Command detector
Telemetry modulation
S-band exciter
S-band TWTA*
X-band exciter
X-band TWTA*
Receiver
Command detector
Telemetry modulation
S-band exciter
S-band solid-state
X-band exciter
X-band TWTA*
Power system
Main inverter
Standby inverter
Pyrotechnic electronics
Pyrotechnic electronics
Command and data system (flight-data system controls instruments and how the data flows; the command and control computer issues commands—from memory or automatically generated or sent from earth—and routes them to the appropriate subsystem)
Flight-data system oscillator and timing chain
Power on reset circuits
4.8-kHz detector
Flight-data system power converter
Coded command-entry logic
Flight-data system processor
Flight-data system oscillator and timing chain
Power on reset circuits
4.8-kHz detector
Flight-data system power converter
Coded command-entry logic
Flight-data system processor
Flight-data system memory
Flight-data system engineering logic
Flight-data system state-vector control
Command and control computer subsystems processor and memory
Power supply
Command and control computer output unit and command buffers
Flight-data system memory
Flight-data system engineering logic
Command and control computer subsystems processor and memory
Power supply
Command and control computer output unit and command buffers
Attitude control system
Memory 1
Flight control processor 1
Power supply 1
Hybrid programmable attitude control electronics 1
Memory access to memory
Hybrid programmable attitude control electronics 2
Memory 2
Flight control processor 2
Power supply 2
Canopus star tracker
Cruise sun sensors
Acquisition sun sensor
Gyro inertial reference units
Gyro 1
Gyro 2
Gyro 3
(2 of 3 needed)
Articulation control of pointing for instrument platform
Canopus star tracker
Cruise sun sensors
Acquisition sun sensor
Legend:
Built-in active redundancy
Functional redundancy (one susbsytem can substitute for another with some loss of performance)
No redundancy (single failure in these subsystems could cause mission failure)
Standby redundancy (redundant subsystems are not turned on until needed)
Active redundancy (redundant subsystems are turned on and running entire mission)

all redundant subsystems and performs identical processing. However, outputs from a given computer are sent only to a subset of the redundant subsystems. This is accomplished by managing buses so that all members of the redundant set and the backup receive data from a sensor, but only one computer sends commands to that sensor. The others only listen to or receive the data being sent by the commanded subsystem.

Weeding out bad hardware

But even the best and most thoroughly reviewed designs must be implemented with reliable hardware. Spacecraft components are of two classes: those that are composed largely of semiconductor electronics and those that are not. Manufactured electronic parts consist of two subpopulations: those that contain inherent defects and those that do not. Since there is no known degradation mechanism for devices that do not contain flaws they may be considered to have lifetimes that are, for practical purposes, infinite at the parts level. Therefore the objective of NASA's assurance program is to weed out the defective components, or "weak sisters," rather than, say, to determine the failure rates of the combined population.

Reliability screening of such combined populations results not in the establishment of a constant MTBF, but in a failure rate that decreases as the test time increases. More than likely, these results are simply illustrative of the fact that "bad" parts (those with inherent defects) are failing and being replaced with "good" parts, resulting in an increasingly strong population.

The components that are not primarily made up of semiconductors do have wearout characteristics, while being subject to the same possibilities of manufacture and assembly defects. These components include batteries, solar arrays, optics, a variety of mechanical and electromechanical devices and mechanisms, momentum wheels, and the valves and plumbing associated with propulsion systems. Included also are one-shot devices, such as separation systems, appendage deployment devices, and protective covers that can be jettisoned. In the vast majority of cases, where premature failure can be avoided, it is the wearout lives or malfunction of these devices and the depletion of nonrenewable consumable materials that tend to affect reliability.

NASA places heavy emphasis on the selection and control of parts, materials, and manufacturing processes. Although the details may vary from project to project, the programs coincide in these major areas:

- Emphasis on the use of controlled parts—that is, parts with a formally controlled specification. The governing agencywide document is the NASA Standard Parts List, usually supplemented by a center's Preferred Parts List and an Approved Parts List for the specific project.
- Assurance for adequate margins in specific circuits.
- Performance of stress analysis and worst-case analysis.
- Inspection and screening to weed out defective parts.

How the approach to parts works can be seen through two NASA projects: the Space Shuttle and Voyager.

Off-the-shelf devices preferred for Shuttle

The Space Shuttle design emphasizes the use of state-of-the-art technology. The use of off-the-shelf equipment is encouraged whenever it can be shown to perform as reliably as and more cheaply than equipment that might be obtained through a development program. For this off-the-shelf equipment the failure history of electrical and electronic parts is closely examined, and sometimes extra testing is required.

Redundancy as implemented in the Voyager space probe. Showing the interdependence of all the elements, subsystems, and systems. In order for the spacecraft to perform its mission, an unbroken path must proceed through all the boxes. Functional relationships—that is, flow of data or commands—are not shown nor are functional interconnections.

For example, the hybrid microcircuits in the Shuttle avionics system were known by manufacturers to have a general problem with particulate contamination. To reduce this potential failure cause, all hybrid microcircuits except those with protective coatings were put through a particulate impact test and a 168-hour burn-in to eliminate units prone to infant mortality. The particulate test from the preliminary lots of hybrid microcircuits had rejects of approximately 15 percent. In six months, rejects were reduced to approximately 2 percent as a result of cleaner fabrication lines and improved inspections.

An interesting case study of the competing factors in parts selection is the use of complementary-MOS technology in the Voyager program.

One of the first decisions in planning the reliability program for Voyager was for narrowing the designs to a few highly reliable part types. Circuit designers tend to squeeze every last ounce of performance from their designs. To a large degree, the system designers force this approach when power, weight, and volume are in short supply, as was the case in Voyager. This represents a hard trade to manage between reliability and system performance.

The flight data system designers proposed use of 4000 series CMOS devices as the baseline of the logic. This was favored by the system designers, since CMOS was a low-power, high-density technology. The science instrument designers were also anxious to use CMOS, but while they were not constrained by the project rules, they were reluctant to do so because of parts availability and procurement questions. The reliability specialists were against it because CMOS was unqualified and had a mixed record on radiation performance. (Pioneer, Voyager's predecessor that had already been launched and was on its way to Jupiter, had not yet discovered the magnitude and nature of the Jovian radiation environment.) The project managers did not want to get into a situation where they approved CMOS for all applications and baselined it for all logic designs, only to see it fall apart in testing—or find a big radiation problem at Jupiter when Pioneer data arrived.

The ultimate decision was to allow the use of CMOS only in the flight data system and to authorize its qualification. In the worst case, a redesign based on bipolar low-power logic was possible. As it turned out, the CMOS was very susceptible to ionizing radiation; Pioneer discovered intense electron belts at Jupiter, and a process-hardening technique was needed by the CMOS supplier that added an additional year to parts acquisition. Since the project management was very conscious of the risk of new technology and parts reliability, it was able to limit CMOS use to one subsystem and the instruments.

The value of this approach was proved when on March 5, 1979, Voyager passed through the heart of the Jovian radiation environment without detectable damage to its engineering subsystems.

Testing—components to system

After steps to ensure good design and reliable parts, NASA verifies the hardware through a series of system tests that fall into two categories: performance and environmental tests.

The performance tests are generally done at all levels of assembly—from subassemblies through components and subsystems. These tests verify that the hardware performs as expected, in all operations, and that it "plays together" well in the

sense of being properly interfaced and integrated. These tests exercise the software as well as the hardware and ultimately embrace ground support operations as well as flight systems.

The environmental tests ensure that the craft can withstand the anticipated launch, flight, and reentry and landing conditions. Tests are normally conducted at levels based on measured or anticipated flight loads including an appropriate safety factor.

Usually the most significant environmental conditions are the vibroacoustic loads during launch, reentry, and landing phases, along with the thermal and vacuum conditions of free flight. The planetary and deep space probes, however, often are called upon to withstand special hazards associated with planetary atmospheres. They therefore require tests not needed for earth-orbiting missions.

Tests at lower levels of assembly, which are usually extensive, are at the option of the project office. They are generally considered screens to determine the acceptability of a component or subsystem for integration into the system.

For Voyager, these tests were done at the Jet Propulsion Laboratory. For example, one set of tests verified the redundancy of the system's design. During spacecraft testing the power was removed from a redundant unit to verify operational independence. Though this did not verify failure independence, it did give good confidence in the design. Redundancy verification testing was also performed. Faults were simulated in the spacecraft, and the response at the system level was monitored.

Most testing done on largest assembly

Emphasis on testing the highest level of assembly—the whole spacecraft—has always been a NASA priority. This is the all-up system level, consisting of the spacecraft and all flight hardware in place including instruments. The most important are the vibroacoustic tests, which simulate the effects of the launch environment, and the thermal-vacuum test, which simulates the major effects of the space environment. It is quite common to discover a number of anomalous conditions during the pre- and post-test functional checks, and these conditions are not necessarily related to the actual environmental exposure. Some are caused simply by unexpected interface problems, others by workmanship errors introduced during integration. The uncovering of those flaws alone justifies the value of total system verification.

These tests are done on either a prototype, which never flies, or a "protoflight" model. Goddard pioneered the protoflight concept in the mid 1960s and all NASA centers have since adopted it for testing their projects. Prior to this, separate prototype and flight spacecraft were built, with the prototype being subjected to levels significantly in excess of flight requirements to test margins. It was found, however, that usually no significant damage was incurred by the prototype that would have precluded its use as flight hardware. Under the protoflight concept, only a single spacecraft is built for the first launch. The first spacecraft is tested at exposure levels as if it were a prototype. This includes time durations appropriate to a flight unit for time-dependent stresses, such as vibroacoustic loads. In addition there is usually a model of the spacecraft containing no flight hardware; it is used for engineering evaluations of structural and thermal loads.

Environmental test programs serve not only to qualify hardware for flight by demonstrating adequate stress margins, but also to screen out defects.

Prototype or protoflight units are tested to levels conservatively set at 50 percent above the mean-plus-two sigma flight level for structural loads (recently modified for static loads to 25 percent above the mean-plus-three sigma value) and for thermal loads at 10°C in excess of the high and low predicted extremes.

For payloads launched by expendable launch vehicles, the test philosophy has remained essentially unchanged over the last 20 years, although test facilities and analytical techniques have improved.

The Space Shuttle Columbia's first flight in April was actually a protoflight test. There had also been several landing exercises with a prototype—the Space Shuttle Enterprise—that was released from atop a Boeing 747 jetliner.

A look ahead—a new reliability era

Throughout the 1960s NASA stressed manned programs as the nation focused on the goal of landing men on the moon. With national prestige at stake, as well as human lives, the need to subjugate all other objectives to reliability was self-evident. As a result, cost was relegated to a secondary role. But to a less dramatic degree, the unmanned programs faced a similar technical challenge to develop hardware that would operate unattended in a harsh environment not fully understood and that could not be accurately simulated on earth.

By the time the Apollo program reached its pinnacle of success, the reliability policies in force had been so successful that near-earth orbiting spacecraft, typically designed for one year of life, were routinely surviving for multiples of their design-goal lifetimes. The result was an embarrassment of riches—more data were being received from space than could be conveniently processed on earth. Although gratifying, this is not necessarily a desirable situation for all projects, since technological advances tend to make older spacecraft obsolete.

At the same time, NASA came under increasing fiscal pressures because of budget cuts and inflation. Certain missions began to be designated as low-cost and high-risk, with some of the elements contributing to reliability to be sacrificed in the interests of reducing costs. This approach, for example, typically calls for eliminating redundancy at the subsystem level—that is, subsystems could not be duplicated on board to ensure redundancy, as had been done, for example, on Voyager. Where no clear-cut cost-risk tradeoffs were imposed, the reliability of each mission was nevertheless implicitly controlled by stringent budget accountability, with the more critical missions being assigned more generous budgets. This trend continued through the 1970s.

The successful flight and landing of the Space Shuttle Columbia marks not only the beginning of a new era in space exploration but also a new era in reliability. With the potential to retrieve and repair spacecraft, the more critical and more costly spacecraft can be put on more cost-effective programs.

To implement Shuttle era cost-risk tradeoffs, NASA has delineated four classes of payloads, graduated in emphasis on reliability depending on the nature and importance of the mission. Each space mission will be assigned a classification at the outset. Then, it will be the responsibility of the field center developing the project to develop the reliability and assurance program for that particular class of mission.

At the engineering level, the rapid advances in technology presented a continuing challenge to devise solutions to new problems. For example, the steady increase in microcircuit packaging density has produced an increasingly difficult screening problem regarding the detection of defects. At the same time components are now being packaged for which it is literally impossible to test all possible circuit functions in a reasonable time. Thus the achievement of high reliability in the space program presents a continuing challenge. The recent success of the Space Shuttle reaffirms our belief that the challenge will continue to be met. ◆